УДК 004.056.5

АНАЛІЗ ЙМОВІРНОСТІ РЕАЛІЗАЦІЇ ЗАГРОЗ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ

Сергій Гончар

З метою вирішення задач по забезпеченню інформаційної безпеки автоматизованих систем управління технологічними процесами проведено аналіз загроз захисту інформації та детальний опис джерел навмисних загроз. Здійснено аналіз уразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами, класифікація та причини їх виникнення. Дані рекомендації щодо усунення або нівелювання даних уразливостей. Приведено вираз для визначення ймовірності реалізації загроз захисту інформації. Досліджено взаємозв'язки між загрозами, уразливостями і ризиком для автоматизованих систем управління технологічними процесами. Приведено життєвий цикл аналізу ймовірності реалізації загроз інформаційної безпеки автоматизованих систем управління технологічними процесами та сформульовано вихідні дані, які необхідні для цього аналізу.

Ключові слова: *загроза, захист інформації, автоматизовані системи управління, уразливості, ризик, життєвий цикл.*

Вступ. На сьогоднішній день в галузях, які життєво важливі для критичної інфраструктури широко використовуються автоматизовані системи управління технологічними процесами, які включають системи диспетчерського управління і збору даних, системи розподіленого управління та інші конфігурації систем управління.

Ще відносно недавно питання безпеки об'єктів критичної інфраструктури держави вирішувалося по двох основних напрямках: захист від несанкціонованого доступу на об'єкт та забезпечення надійного функціонування автоматизованих систем управління технологічним процесом (АСУ ТП). Однак розвиток та поширення інформаційних технологій, глобалізація інформаційно-телекомунікаційних мереж зумовили появу нового типу загроз безпеки об'єктів - злому і порушення режимів функціонування ключових об'єктів інформатизації, які відповідають за управління та забезпечення безпеки об'єктів критичної інфраструктури.

Враховуючи зазначене та зважаючи на особливості автоматизованих систем управління [1], для вирішення задач по забезпеченню їх інформаційної безпеки необхідні дослідження взаємозв'язків між загрозами, уразливостями і ризиком, а також аналіз ймовірності реалізації загроз інформаційної безпеки АСУ ТП.

Загрози захисту інформації АСУ ТП. Загрози інформації класифікують за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки, тобто – порушення конфіденційності, цілісності доступності інформації і відповідальності [2].

Розрізняють чотири типи загроз безпеки інформації [3]:

- несанкціонований доступ до інформації;
- несанкціонована модифікація або викрадення інформації;
- відмова в обслуговуванні;
- відмова у відповідальності.

Загрози для об'єктів критичної інфраструктури можуть виходити з різних джерел: навмисних (терористичні групи, промислові шпигуни, невдоволені працівники, зловмисники), ненавмисних (складність системи, людські помилки, аварії, відмови обладнання), природні (стихійні лиха, кліматичні умови тощо). Приведемо більш детальний опис груп, що входять в категорію навмисних загроз:

- *Зловмисники.* Найчастіше хакери зламують мережі для гостроти відчуттів в дусі змагань або для хвастощів серед колег. Раніше віддалений злом вимагав неабияких комп'ютерних знань та навичок, а тепер зловмисники можуть завантажити сценарії атаки і протоколи Інтернету. Таким чином, у той час як інструменти атаки стали більш складними, вони також стали більш легкими для використання.
- *Оператори ботнету.* Ботнет – комп'ютерна мережа, що складається з деякої кількості хостів, з запущеними ботами (автономним програмним забезпеченням). Найчастіше бот у складі ботнета є програмою, що потай встановлюється на пристрій жертви і дозволяє зловмиснику виконувати якісь дії з використанням ресурсів зараженого комп'ютера. Зазвичай ботнети використовуються для нелегальної або злочинної діяльності: розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні.
- *Злочинні групи.* Злочинні групи прагнуть атакувати системи для отримання грошової виго-

ди з допомогою спаму, фішингу, шпигунських програм для вчинення крадіжки та шахрайства в Інтернеті.

– *Іноземні спецслужби.* Іноземні спецслужби використовують кіберзасоби, як частину їх шпигунської діяльності, спрямованої на збір інформації або для проведення операцій в рамках інформаційних впливів на супротивника.

– *Інсайдери.* Незадоволені інсайдери є основним джерелом комп'ютерної злочинності. Інсайдерам не потрібно мати багато спеціальних знань про кібератаки, тому що можливості якими вони володіють, перебуваючи усередині системи, часто дозволяють їм отримати необмежений доступ до системи, а також здійснити її пошкодження або крадіжку даних. Також інсайдерські загрози становлять сторонні постачальники обладнання та програм, а також співробітники, які ненавмисно впроваджують шкідливі програми в системі. Інсайдерами можуть бути працівники, підрядники, партнери по бізнесу.

– *Фішери.* Фішинг – вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів - логінів і паролів. Дана загроза реалізується шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень всередині різних сервісів. У листі міститься пряме посилання на сайт, зовні відрізнити від справжнього, або на сайт з переадресацією. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленої сторінці свої логін і пароль.

– *Сніфінг.* Сніфінг – поширений вид атаки, коли всі пакети, отримані мережевою картою, пересилаються на обробку спеціальною програмою, званому сніфером. У результаті зловмисник може отримати велику кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці пакети проходили. Найбільшою небезпекою такої атаки є отримання самої інформації, наприклад логінів і паролів співробітників, які можна використовувати для незаконного проникнення в систему під виглядом звичайного співробітника компанії.

– *Спамери.* Спам – розсилка реклами або інших видів повідомлень особам, які не висловлювали бажання їх отримувати.

– *Автори шпигунських і шкідливих програм.* Особи або організації, які зі злим умислом проводять атаки на користувачів шляхом написання і поширення шпигунського і шкідливого програмного забезпечення.

– *Терористи.* Терористи ставлять перед собою мету знищити, вивести з експлуатації критично важливі об'єкти інфраструктури, створити загрозу національній безпеці, викликати масові жертви, послабити економіку країни, завдати шкоди суспільній моралі. Терористи можуть атакувати одну мету, щоб відвернути увагу та ресурси від інших цілей.

– *Промислові шпигуни.* Метою шпигунства може стати компрометація інформації або її крадіжка з подальшим деструктивним використанням, до повної зупинки і банкрутства промислового об'єкта.

Уразливості АСУ ТП. Уразливістю є недолік або слабке місце інформаційної системи, системи безпеки, процедур внутрішнього контролю, які можуть бути використані для порушення цілісності або доступності системи та її коректної роботи.

Класифікація уразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами показана на рис. 1.

Розглянемо більш докладно уразливості автоматизованих систем управління [4].

1. Уразливості політик і процедур. До цієї категорії можна віднести:

– невідповідність або відсутність політики безпеки;

– невідповідність або відсутність процедур безпеки (повинні бути розроблені конкретні процедури безпеки і навчений відповідний персонал);

– відсутність підвищення кваліфікації персоналу у сфері безпеки;

– невідповідність архітектури безпеки;

– невідповідність або відсутність керівництва по впровадженню обладнання;

– відсутність відповідальності за документальне адміністрування політик і процедур безпеки;

– відсутність або недолік аудитів в області безпеки;

– відсутність конкретного плану аварійного відновлення системи у випадку збою або аварії (план повинен бути готовий, апробований та доступний у разі виникнення апаратного або програмного збою, щоб уникнути простою і втрати виробництва);

– відсутність змін конфігурації управління (повинно здійснюватися управління модифікаціями апаратних засобів, програмованого облад-

нання, програмного забезпечення, щоб гарантовано захистити систему від невідповідних або неправомірних модифікацій до, під час, і після впровадження системи).

Рис. 1. Класифікація уразливостей інформаційної безпеки АСУ ТП

Аналіз показує, що уразливості політик і процедур в промислових автоматизованих системах управління виникають через відсутність або неповну, неадекватну документацію в галузі безпеки, у тому числі політик і керівництва (процедур), адміністрування аудиту, відновлення.

2. Уразливості платформ. До даної категорії можна віднести:

2.1. Конфігурація:

– програмне забезпечення не оновлюється для виявлення вразливостей (через складність програмного забезпечення АСУ зміни повинні пройти комплексне тестування, що займає певний час і забезпечує уразливість до загроз);

– операційна система та програми безпеки впроваджуються і оновлюються без ретельних випробувань (повинні бути розроблені документовані процедури для тестування нових програм безпеки);

– параметри конфігурації використовуються за замовчуванням (це часто призводить до небезпечного відкриття портів інших служб і виконання небажаних програм);

– не зберігаються критичні конфігурації системи (для підтримки доступності системи і запобігання втрати даних повинні бути розроблені документовані процедури для відновлення параметрів конфігурації у разі випадкової або зловмисної зміни в конфігурації);

– зберігання незахищених конфіденційних даних (наприклад, паролі) на портативних пристроях (ці пристрої будуть втрачені або вкрадені і безпека системи може бути порушена);

– відсутність адекватної політики паролів (коли паролі повинні бути використані, наскільки стійкими вони повинні бути і як вони повинні зберігатися);

– відсутність пароля (паролі повинні бути реалізовані для запобігання несанкціонованого доступу – для входу в систему (якщо в системі є облікові записи користувачів), при включенні живлення (якщо в системі немає облікових записів користувачів), при виході та режиму заставки);

– розкриття паролів (прикладами можуть бути спільне використання паролів для різних облікових записів користувачів, повідомлення паролів стороннім, передача паролів в незашифрованому вигляді через незахищені підключення);

– підбір пароля (погано підібраний пароль може бути легко розгаданий зловмисником або комп'ютерною програмою для отримання несанкціонованого доступу);

– неадекватність контролю доступу (неправильно налаштований контроль доступу може дозволити оператору дії адміністратора або заборонити оператору коригувальні дії в аварійній ситуації).

2.2. Обладнання:

– невідповідне тестування змін системи безпеки;

– недостатній рівень фізичного захисту критично важливих систем;

– несанкціонований фізичний доступ сторонніх осіб до обладнання;

– незахищений віддалений доступ до компонентів АСУ;

– подвійні мережеві карти для з'єднання мереж (при підключенні до різних мереж можливий несанкціонований доступ з однієї мережі в іншу);

– відсутність документування активів (відсутність точного списку активів в системі може залишити несанкціоновані точки доступу);

– радіочастотний і електромагнітний імпульс (наслідки впливу можуть бути від тимчасового порушення управління до пошкодження плат);

– відсутність резервного електроживлення;

– втрата контролю навколишнього середовища системи (втрата контролю навколишнього середовища процесорів може привести до перегріву і пошкодження або роботі з помилками);

– відсутність резервування критично-важливих компонентів.

2.3. Програмне забезпечення:

– переповнення буфера (може викликати аварійне завершення або зависання програми, що веде до відмови обслуговування. Окремі види переповнення, наприклад переповнення в стековому кадрі, дозволяють зловмиснику завантажити та виконати довільний машинний код від імені програми і з правами облікового запису, від якої вона виконується);

– не включені або ідентифікуються як відключені можливості безпеки, які були встановлені з програмним продуктом;

– відмова в обслуговуванні;

– неправильна обробка невизначених, погано визначених, або "неприпустимих" умов (деякі реалізації систем уразливі для пакетів, які спотворені або містять "неприпустимі" значення полів);

– використання незахищених галузевих протоколів передачі даних;

– передача повідомлень в незахищеному вигляді;

– запуск надлишкових сервісів, тобто тих служб, які не використовуються для вирішення поставлених завдань;

– використання пропрієтарного програмного забезпечення, яке було предметом обговорення на конференціях і в періодичних друкованих виданнях;

– недостатня перевірка справжності та контролю доступу для конфігурування та програмування;

– не встановлено програмне забезпечення виявлення/запобігання несанкціонованого проникнення;

– не підтримується протоколювання роботи всіх служб і сервісів;

– не реєструються інциденти.

2.4. Шкідливе програмне забезпечення:

– не встановлено захист від шкідливого програмного забезпечення;

– захист від шкідливого програмного забезпечення не актуальна, тобто не оновлюється або оновлюється рідко;

– захист від шкідливого програмного забезпечення впроваджена без проведення ретельних випробувань.

Як бачимо, уразливості платформ в АСУ ТП можуть виникати через недоліки, помилки, або неякісне обслуговування своїх платформ, у тому числі обладнання (апаратні засоби, операційні системи і додатки, відсутність контролю фізичного доступу.

3. Уразливості мережі. До даної категорії можна віднести:

3.1. Конфігурація мережі:

– невідповідність архітектури мережевої безпеки;

– відсутність контролю потоку даних;

– неякісно налаштовані параметри безпеки обладнання;

– відсутність резервування конфігурації мережевого пристрою;

– передача паролів в незахищеному вигляді;

– недостатньо часта зміна паролів доступу до мережевих пристроїв;

– неадекватність контролю доступу до мережевих пристроїв.

3.2. Мережеве обладнання:

– недостатній рівень фізичного захисту мережевого обладнання;

– несанкціонований доступ до портів мережевого обладнання;

– відсутність надлишковості для критично важливих сегментів мережі.

3.3. Периметр мережі:

– не визначений периметр безпеки;

– відсутня або неправильно налаштовано міжмережевий екран;

– мережі управління використовуються для трафіку інших типів;

– управління мережевими сервісами мережі АСУ реалізується в мережі ІТ (мережа АСУ стає залежною від мережі ІТ, у якої немає необхідного пріоритету надійності і доступності).

3.4. Моніторинг мережі:

– неадекватні журнали міжмережевого екрану (кількість контрольованих параметрів не достатньо для проведення аналізу інцидентів);

– відсутність регулярного моніторингу безпеки в мережі.

3.5. З'єднання:

– не ідентифікуються критичні шляхи контролю та управління;

– використання стандартних протоколів зв'язку;

– відсутня або недостатня аутентифікація користувачів, даних або пристроїв;

– відсутність перевірки цілісності з'єднань.

3.6. Бездротові мережі:

– невідповідність аутентифікації між бездротовими клієнтами і точками доступу;

– невідповідний захист даних між бездротовими клієнтами і точками доступу.

Аналіз показує, що уразливості мережі в промислових автоматизованих системах управління можуть виникати через недоліки, помилки, погане адміністрування мереж. Ці уразливості можуть бути усунені або нівельовані за допомогою правильного проектування мережі, шифрування мережевих з'єднань, забезпечення контролю фізичного доступу до мережевих компонентів.

Взаємозв'язок між загрозами, уразливостями і ризиком. Причинами виникнення загроз інформації являються дестабілізуючі фактори – явища чи події, які можуть з'являтися на будь-якому етапі життєвого циклу системи. Наслідком виникнення дестабілізуючих факторів може бути ризик інформаційної безпеки – ймовірність того, що певна загроза використає уразливість системи, в результаті чого буде нанесено шкоду компонентам системи [5]. Отже, порушення інформаційної безпеки – це виникнення і реалізація загроз.

Разом з тим, слід відмітити, що загроза, яка не має відповідної уразливості, може не призводити до ризику. І навпаки, наявність уразливості не завдає шкоди сама по собі, так як необхідна наявність загрози, яка скористається нею.

Взаємозв'язок між загрозами, уразливостями і ризиком приведений на рис. 2 [6].

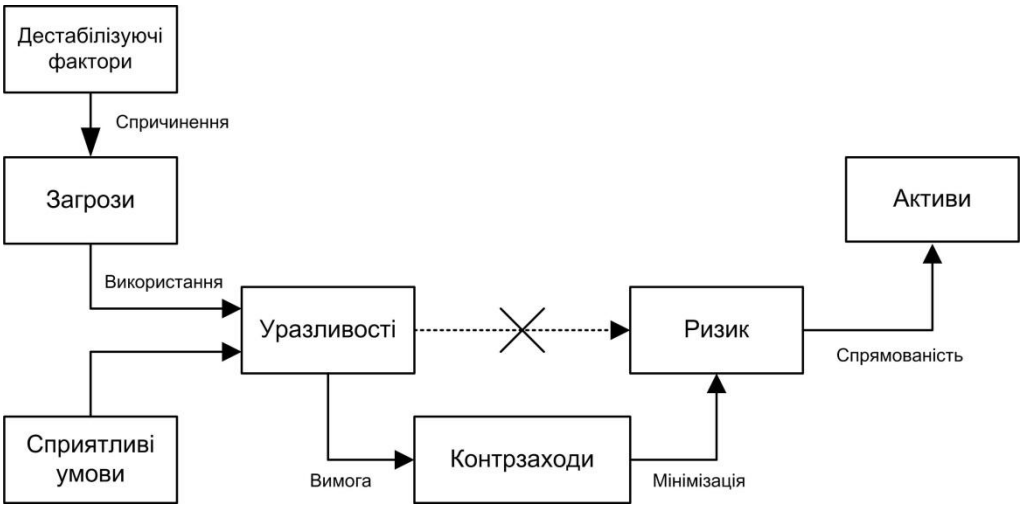

Рис. 2. Взаємозв'язок між загрозами, уразливостями і ризиком

Уразливість, яка не має відповідної загрози, може не вимагати впровадження засобу контролю, але повинна усвідомлюватися і піддаватися постійному моніторингу.

Виходячи із зазначеного, можна зауважити, що ймовірність реалізації загрози буде залежати від наявності сприятливих умов для використання уразливостей, пов'язаних з цими загрозами.

Нехай R_{nm} – подія, яка відображає реалізацію n-ї загрози з використанням m-ї уразливості, де $n=\overline{1,N}$ – множина загроз; $m=\overline{1,M}$ – множина уразливостей, а Q_k – подія, яка відображає наявність сприятливих умов із множини $k=\overline{1,K}$, для реалізації n-ї загрози з використанням m-ї уразливості. Крім того, події R_{nm} незалежні і складають повну групу несумісних подій.

Тоді, ймовірність реалізації n-ї загрози з використанням m-ї уразливості буде визначатися наступним чином:

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

де $P(R_{nm}\,|\,Q_k)$ – ймовірність реалізації n-ї загрози з використанням m-ї уразливості при умові наявності сприятливих умов Q_k;

$P(Q_k)$ – ймовірність наявності сприятливих умов.

Таким чином, ймовірність реалізації загроз з використанням уразливостей за умови наявності сприятливих умов можливо представити у вигляді матриці:

$$P(R)=\left[P(R_{nm})\right]. \qquad (2)$$

Елементи матриці у виразі (2) визначаються з виразу (1).

Очевидно, що захист інформації буде забезпечено у випадку, якщо:

$$\sum_{n=1}^{N}\sum_{m=1}^{M}\sum_{k=1}^{K} P(R_{nm} \mid Q_k) P(Q_k) = 0 . \qquad (3)$$

В протилежному випадку буде ймовірність реалізації загрози і ймовірність нанесення шкоди компонентам системи.

Життєвий цикл процесу аналізу ймовірності реалізації загроз. Життєвий цикл процесу відображає послідовність стадій та фаз, що визначають динаміку реалізації і розвитку процесу.

Як випливає з виразу (2) та взаємозв'язку між загрозами, уразливостями і ризиком (рис. 2), для аналізу ймовірності реалізації загроз необхідні наступні вихідні дані:

- перелік джерел загроз;
- перелік загроз безпеки інформації;
- перелік уразливостей, через які можлива реалізація загроз;
- перелік сприятливих умов для реалізації загроз.

Життєвий цикл процесу аналізу ймовірності реалізації загроз представлений на рис. 3.

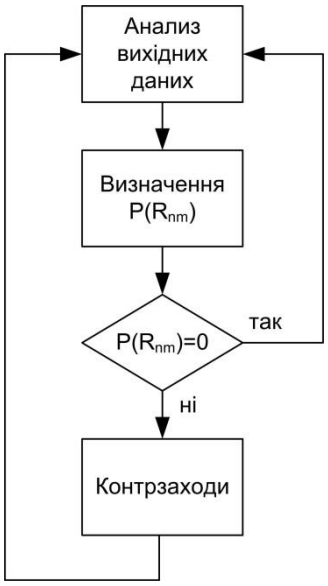

Рис. 3. Життєвий цикл процесу аналізу ймовірності реалізації загроз

Висновки. Проведено аналіз джерел загроз та уразливостей інформаційної безпеки автоматизованих систем управління технологічними процесами, досліджено взаємозв'язки між загрозами, уразливостями і ризиком для автоматизованих систем управління технологічними процесами.

Приведено життєвий цикл аналізу ймовірності реалізації загроз інформаційної безпеки автоматизованих систем управління технологічними процесами та сформульовано вихідні дані, які необхідні для цього аналізу.

ЛИТЕРАТУРА

[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]. 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.

[3]. 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.

[4]. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.

[5]. Information technology – Security techniques – Information security risk management: BS ISO/IEC 27005:2008.

[6]. Industrial communication networks – Network and system security: IEC 62443, Part 3.

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]. Mokhor V.V. Guidelines for cybersecurity (ISO/IEC 27032:2012), 2013, 129 p.

[3]. 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.

[4]. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.

[5]. Information technology – Security techniques – Information security risk management: BS ISO/IEC 27005:2008.

[6]. Industrial communication networks – Network and system security: IEC 62443, Part 3.

АНАЛИЗ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

С целью решения задач, связанных с обеспечением информационной безопасности автоматизированных систем управления технологическим процессом про-

веден анализ угроз информационной безопасности и подробное описание источников преднамеренных угроз. Выполнен анализ уязвимостей информационной безопасности автоматизированных систем управления технологическим процессом, классификация и причины их возникновения. Даны рекомендации по устранению или нивелированию этих уязвимостей. Приведено выражение для определения вероятности реализации угроз информации. Исследованы взаимосвязи между угрозами, уязвимостями и риском для автоматизированных систем управления технологическим процессом. Приведен жизненный цикл вероятности реализации угроз информационной безопасности автоматизированных систем управления и сформулированы исходные данные, необходимые для данного анализа.
Ключевые слова: угроза, защита информации, автоматизированные системы управления технологическим процессом, уязвимости, риск, жизненный цикл.

ANALYSIS OF THE PROBABILITY IMPLEMENTATION OF THREATS PROTECTION OF INFORMATION IN INDUSTRIAL CONTROL SYSTEMS

For the purpose of the decision of the tasks connected to support of information security of industrial control systems the analysis of threats of information security and the detailed description of sources of deliberate threats is carried out. The analysis of vulnerabilities information security of the industrial control systems, classification and the reasons of their origin is made. Recommendations about elimination or leveling of these vulnerabilities are made. Expression for determination of probability of implementation of threats of the information is resulted. Correlations between threats, vulnerabilities and risk for the industrial control systems are researched. Lifecycle of probability of implementation of threats of information security of the industrial control systems is resulted and the initial data necessary for the given analysis is formulated.
Keywords: threat, information protection, industrial control systems, vulnerability, risk, lifecycle.

Гончар Сергій Феодосійович, кандидат технічних наук, заступник начальника державного науково-дослідного інституту спеціального зв'язку та захисту інформації.
E-mail: sfgonchar@yandex.ru
Гончар Сергей Феодосьевич, кандидат технических наук, заместитель начальника государственного научно-исследовательского института специальной связи и защиты информации.
Gonchar Sergii, PhD in Eng., Deputy Chief of State Research Institute for Special Telecommunication and Information Protection (Kyiv, Ukraine).

УДК 004.056.5: 004.738.5

ЗАХИЩЕНИЙ МЕРЕЖНИЙ ІНФОРМАЦІЙНИЙ РЕСУРС ЯК СИНЕРГЕТИЧНА СИСТЕМА

Володимир Блінцов, Денис Самойленко

Ускладнення сучасних мережних інформаційних ресурсів, впровадження у них інтелектуальних рішень з нелінійними зв'язками між елементами вимагає використання для їх опису адекватного математичного апарату. Наявні підходи, в основному, грунтуються на засобах системного аналізу, кібернетики, теорії ігор – детерміністичних математичних методах. Це обмежує можливості опису систем з великою кількістю елементів та принципово нелінійними зв'язками між ними, особливо у нерівноважних станах, які можуть виникати при спробі атак на інформаційні ресурси. Запропоновано структурну модель захищеного інформаційного ресурсу з архітектурою, що відповідає вимогам нормативної документації України та стандартів. У складеній моделі виявлено основні ознаки, типові для синергетичної системи. Використання математичного апарату синергетики дозволить більш якісно описати процеси, що супроводжуються виведенням системи з рівноваги, виділити ознаки наближення системи до точок біфуркації та розвинути засоби реалізації виведення системи з нерівноважних станів.
Ключові слова: *інформаційний ресурс, захист інформаційного ресурсу, захист сайту, модель інформаційного ресурсу, синергетика, синергетична модель.*

Постановка проблеми. Стрімка еволюція мережі Інтернет призводить до того, що ресурси цієї мережі, - сайти, - набувають усе більшої кількості функцій та обтяжуються усе більшою кількістю задач. Окрім функцій «візитної картки» чи довідника сучасні мережні інформаційні ресурси (МІР) виконують роль магазинів, банків та платіжних систем, відео- та телефонів, кінотеатрів, телебачення, радіостанцій, газет, журналів тощо. Додаткові завдання, пов'язані з управлінням іміджем власника МІР, маркетингом та соціальною спрямованістю, надають ресурсу «соціальних»