основе анализа данных мониторинга с учетом экспертных оценок.

Если нижний уровень допускает выбор решения на основе значений отдельных параметров, то на более высоких уровнях представления знаний рассматриваются стратегии и алгоритмы, основанные на вероятностном описании предметной области. В качестве критериев для принятия решений предлагается рассматривать разные уровни рисков, и в первую очередь риски, связанные со здоровьем населения.

1. *Андерсон Дж.* Когнитивная психология. – СПб.: Питер, 2002. – 496 с.
2. *Дилтс Р.* Моделирование с помощью НЛП. – СПб: Питер, 2001. – 288 с.
3. *Люгер Дж.,* Искусственный интеллект: стратегии и методы решения сложных проблем. – М.: «Вильяме», 2003. – 864 с.
4. *Гаврилова Т.А., Хорошевский В.Ф.* Базы знаний интеллектуальных систем. – СПб. Питер, 2001. – 384 с.
5. *Каменева И.П., Яцишин А.В., Артемчук В.А.* Компьютерные средства оценивания экологических рисков с использованием структурного анализа данных мониторинга // Электронное моделирование. – 2013. Т.35, № 6. – С.99-113.
6. *Кини Р.* Теория принятия решений // Исследование операций: в 2-х томах, Т1, М.: Мир, 1981. – С.481-512.
7. *Каменева И.П.* Вероятностные модели репрезентации знаний в интеллектуальных системах принятия решений // Искусственный интеллект. – Донецк, ИПИИ НАН Украины, 2005. – № 3. – С.399-409.
8. *Гладун В.П.* Процессы формирования новых знаний. – София, 1994. – 192 с.
9. Управление риском: Риск. Устойчивое развитие. Синергетика. – М: Наука, 2000. – 432 с.
10. *Большаков А.М., Крутько В.Н., Пуцилло Е.В.* Оценка и управление рисками влияния окружающей среды на здоровье населения. – М.:Эдиториал УРСС, 1999. – 256 с.

*Поступила 25.09.2017р.*

УДК 004.056.5

С.Ф. Гончар, Київ

## ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

**Abstract.** The features of industrial control systems that distinguish them from automated systems of traditional information technologies are presented. These features should be taken into account when developing and implementing measures to ensure the cybersecurity of industrial control systems that operate on critical infrastructure objects.

**Вступ**

На даний час автоматизовані системи управління технологічним процесом (АСУ ТП) включають в себе системи диспетчерського управління і збору даних, системи розподіленого управління та інші конфігурації систем управління об'єктами критичної інфраструктури. Об'єкти критичної інфраструктури – це підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення [1].

Ще відносно недавно питання безпеки об'єктів критичної інфраструктури вирішувалося по двох основних напрямках: захист від несанкціонованого доступу на об'єкт та забезпечення надійного функціонування автоматизованих систем управління технологічними процесами. Однак, розвиток та поширення інформаційних технологій, глобалізація інформаційно-телекомунікаційних мереж зумовили появу нового типу загроз безпеки об'єктів критичної інфраструктури – кіберзагроз.

Для забезпечення кіберзахисту автоматизованих систем (АС) традиційних інформаційних технологій (ІТ) існують відповідні механізми, методики тощо. Але, автоматизовані системи управління технологічними процесами мають певні відмінності від автоматизованих систем традиційних інформаційних технологій, які необхідно враховувати при розробці та впровадженні заходів забезпечення кібербезпеки об'єктів критичної інфраструктури.

**Основна частина**

Кібербезпека традиційно зосереджена на досягненні конфіденційності, цілісності та доступності.

Однією із відмінностей традиційних систем інформаційних технологій (ІТ) та автоматизованих систем управління технологічними процесами полягає у тому, що стратегія кібербезпеки традиційних інформаційних технологій спрямована, в першу чергу, на досягнення конфіденційності з необхідними засобами керування доступом для досягнення даної мети. При цьому, цілісність інформації займає друге місце по важливості задачі. Доступність у даному випадку буде по пріоритетності займати останнє місце [2].

Так, наприклад щодо автоматизованої системи для обробки інформації з обмеженим доступом основною задачею буде забезпечення конфіденційності інформації, що обробляється у цій АС. Основні зусилля спрямовані на запобігання несанкціонованому доступу до цієї інформації, такому як: розголошення, копіювання, перехоплення, підміна, викрадення інформації, аналіз трафіка тощо. Доступ до інформації у таких системах не має критичного значення, оскільки завжди можна перезавантажити систему тощо.

В АСУ ТП загальний пріоритет цих цілей, як правило, відрізняється. Безпека в цих системах, перш за все, стосується підтримки доступності

компонентів усіх систем. Забезпечення цілісності для АСУ ТП являється, як правило, другою по пріоритетності задачею. Забезпечення конфіденційності для АСУ ТП має найменше значення, оскільки та технологічна інформація, що циркулює в АСУ ТП не відноситься до інформації з обмеженим доступом.

Важливість цілісності інформації, яка циркулює в АСУ ТП можна спостерігати на прикладі застосування зловмисниками спеціалізованого комп'ютерного вірусу «Stuxnet», який був виявлений на комп'ютерах співробітників іранської АЕС у Бушері і став першою з шкідливих програм, здатних інфікувати автоматизовані системи управління промислових підприємств.

Той факт, що цей вірус може збирати різні відомості про нову "середовище проживання" і обмінюватися інформацією з віддаленим сервером, раніше приводив експертів до висновку про те, що його головна мета – промислове шпигунство. Однак для здійснення основної місії «Stuxnet» не потрібен був вихід в Інтернет, тим більше що в закритих внутрішніх мережах більшості підприємств, де існують вимоги підвищеної безпеки, доступ у всесвітню мережу просто відсутній. Вірус міг діяти автономно – поширюватися по внутрішній мережі і заражати знімні носії інформації. Потрапивши на комп'ютер, «Stuxnet» не стирав файлів, не крав номерів кредитних карт, тобто не було загрози втрати конфіденційності інформації. Вірус активізувався лише у випадку, якщо на машині працювала SCADA-система. Такі системи регулюють технологічні процеси електростанцій, нафто- та газопроводів, військових заводів, підприємств цивільної інфраструктури тощо, тобто об’єктів критичної інфраструктури країни. В даному випадку в якості об’єкта впливу виступали центрифуги для збагачення урану, пошкодити які (шляхом зміни швидкості обертання) і намагався «Stuxnet», а саме: на центрифуги поступала команда збільшувати що призводило до виходу їх з ладу. При цьому, до центру керування надходила інформація про функціонування центрифуг у штатному режимі. В результаті такої кібератаки раптово вийшли з ладу 1368 із 5000 центрифуг IR-1 по збагаченню урану [3].

У випадку виникнення будь-якої аварійної ситуації оператор повинен мати можливість у найкоротший термін здійснити відповідне реагування на процес. Для цього надзвичайно важливим фактором являється забезпечення доступності компонентів системи.

Таким чином, пріоритетність задач щодо кіберзахисту в АСУ ТП і в IT-системах, в багатьох ситуаціях можуть бути повністю інвертовані.

В той же час, певні вимоги до функціонування, які висувають окремі компоненти або система в цілому, мають різні пріоритети для цілей. Тобто, в залежності від обставин, задача забезпечення цілісності системи може мати найвищий пріоритет, а задача забезпечення доступності можуть переважити задачу забезпечення конфіденційності.

Враховуючи зазначене, для визначення пріоритетності задач при

забезпеченні кібербезпеки кожної конкретної АСУ ТП окрім традиційних факторів (модель загроз, модель порушника тощо) необхідно враховувати особливості функціонування даної системи.

Ще однією істотною відмінністю традиційних систем інформаційних технологій та автоматизованих систем управління технологічними процесами являється досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями [4]. 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.

У випадку реалізації кіберзагроз в автоматизованих системах управління технологічними процесами, які працюють на об'єктах критичної інфраструктури, можуть бути наступні наслідки:

- 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.

Як відомо [5, 6], кожна загроза характеризується ймовірністю її реалізації і нанесеними нею збитками, тобто, наслідками її реалізації. Тобто, показник актуальності загрози в АСУ ТП буде пропорційний ймовірності реалізації даної загрози та коефіцієнту її небезпеки.

Тому, враховуючи зазначене, визначення коефіцієнта небезпеки загроз безпеці інформації та їх актуальності в АСУ ТП може мати інший підхід, ніж в ІТ-системах.

Наступною відмінністю традиційних систем інформаційних технологій та автоматизованих систем управління технологічними процесами є те, що задачі забезпечення основних виробничих функцій індустріальних систем управління іноді суперечать задачам забезпечення їх кібербезпеки. Розглянемо найбільш критичні особливості даних систем [4]:

1. Системи ІТ, як правило, не критичні до затримок у часі (наприклад перезавантаження компонента), в той час, як АСУ ТП працюють у режимі реального часу із жорстко заданими часовими параметрами. Крім того, в АСУ ТП надзвичайно критичним є час реагування системи на дії оператора.

2. В системі ІТ першочерговою задачею являється забезпечення конфіденційність, цілісність та доступність інформації, що обробляється в АС. Для АСУ ТП, поряд із кібербезпекою, важливими є задачі забезпечення безпеки обслуговуючого персоналу, збереження обладнання, запобігання виробничих втрат.

3. В АСУ ТП, на відміну від ІТ-систем, існує достатньо тісний взаємозв'язок процесів у самій автоматизованій системі з фізичними процесами і наслідками в промисловому секторі. Тому, при реалізації заходів кіберзахисту всі функції безпеки, інтегровані в АСУ ТП, повинні бути протестовані на предмет відсутності загрози штатному функціонуванню АСУ ТП.

4. Системи ІТ створюються з достатнім запасом ресурсів для підтримки додатків по забезпеченню кібербезпеки. В той же час, АСУ ТП створюються для забезпечення виробничих процесів і, часто, не вистачає ресурсів для підтримки додатків по забезпеченню кібербезпеки.

5. Оновлення програмного забезпечення в системах ІТ здійснюється, як правило, своєчасно та, досить часто, автоматично. Оновлення ж програмного забезпечення АСУ ТП не можуть бути реалізовані завчасно, оскільки додатки повинні бути ретельно перевірені та протестовані кінцевим користувачем перед впровадженням, а відключення таких систем повинні плануватися завчасно, з урахуванням технологічних особливостей.

**Висновки**

Приведено особливості автоматизованих систем управління технологічними процесами, які відрізняють їх від автоматизованих систем традиційних інформаційних технологій, а саме:

- пріоритетність задач щодо кіберзахисту в автоматизованих системах управління технологічними процесами і в ІТ-системах, в багатьох ситуаціях можуть бути повністю інвертовані;
- на відміну від традиційних систем інформаційних технологій автоматизовані систем управління технологічними процесами мають досить тісний взаємозв'язок з фізичними процесами і виконавчими пристроями, що необхідно враховувати особливо при впровадженні заходів кіберзахисту;
- відмінність наслідків реалізації загроз в автоматизованих системах управління технологічними процесами та системами ІТ;

- неможливість уніфікації методик щодо кіберзахисту АСУ ТП, оскільки кожна конкретна система має свої особливості функціонування і свої вимоги до забезпечення кібербезпеки, які висуваються окремими компонентами або системою в цілому.

Зазначені особливості необхідно враховувати при розробці та впровадженні заходів забезпечення кібербезпеки автоматизованих систем управління технологічними процесами, які працюють на об'єктах критичної інфраструктури.

1. *Постанова* Кабінету Міністрів України від 23.08.16р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави». [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/ 563-2016-%D0%BF.
2. *Industrial* communication networks – Network and system security: IEC 62443. – Part 1-1: terminology, concepts and models.
3. *Кибератаки:* вирус – диверсант Stuxnet в ядерной энергетической программе Ирана. [Електронний ресурс]. Режим доступу: http://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html.
4. *Guide* to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.
5. *Домарев В.В.* "Безопасность информационных технологий. Методология создания систем защиты" – К.: ООО "ТИД "ДС", 2002. – 688 с.
6. *Гончар С.Ф.* Визначення актуальних загроз безпеці інформації в автоматизованих системах управління технологічними процесами / Гончар С.Ф. // Захист інформації. – 2015. – Том 17, № 3. – С.225-230.

*Поступила 18.09.2017р.*

УДК 004.932.2:616-006.6

Г.М. Мельник, Ю.М. Батько, Тернопіль

## ОБ'ЄКТНА МОДЕЛЬ ГІБРИДНИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ АНАЛІЗУ БІОМЕДИЧНИХ ЗОБРАЖЕНЬ

**Abstract.** Oncology diagnostic systems are complex systems that combine computer vision and artificial intelligence methods. A large number of use cases are the cause of the complexity of developing a system. To develop the object model of the system, we used the Model-View-Presenter methodology. The object model of the software is evaluated.

### 1. Актуальність

При діагностуванні злоякісних новоутворень використовуються системи онкологічної діагностики. Системи онкологічної діагностики є складними системами, що поєднують методи комп'ютерного зору та методи штучного

 