УДК 004.05

Д.С. Бірюков, В.М. Бурлаков

ВПЛИВ СУЧАСНИХ КІБЕР-ЗАГРОЗ НА ЕФЕКТИВНІСТЬ СИСТЕМ ФІЗИЧНОГО ЗАХИСТУ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ТА ІНФРАСТРУКТУРИ

Анотація: В роботі розглядається питання про необхідність врахування кібер-загроз при формуванні систем фізичного захисту критично важливих об'єктів та інфраструктури.

Ключові слова: вразливість автоматизованих систем управління, критична інфраструктура, системи фізичного захисту.

Вступ

Проблема забезпечення безпеки функціонування автоматизованих систем управління (АСУ) та АСУ технологічними процесами (АСУ ТП) на виробничих підприємствах критичної інфраструктури є багатоаспектною і включає нормативні, організаційні, технологічні, психологічні складові. В технологічному аспекті безпека АСУ пов'язана переважно з надійністю їх апаратного та програмного забезпечення, в організаційному – з дотриманням вимог фізичного захисту. Психологічний аспект безпеки АСУ стосується здебільшого оцінки та прогнозування поведінки ліцензованого персоналу, а нормативний аспект представлений зводом регулюючих і інструктивних документів.

На кінець 80-х років минулого сторіччя був накопичений значний досвід щодо проектного забезпечення та практичного оцінювання надійності АСУ та АСУ ТП, розроблені нормативні документи з питань надійності та ризик-менеджменту таких систем, включаючи державні і галузеві стандарти, опубліковано значну кількість наукових статей та десятки монографій [1-4].

Характерною особливістю останніх двадцяти років є значне зростання якості, в тому числі і надійності, елементної бази технічних засобів інформатизації поряд з суттєвим підвищенням складності АСУ ТП. Розвиток інформаційних технологій (ІТ), апаратного забезпечення АСУ та комп'ютерних мереж створив умови для віддаленого управління технологічним процесом (ТП) на підприємствах, автоматизованого збору та аналізу необхідних даних, зміни параметрів (перепрограмування) контролерів ТП. Ці можливості розглядаються та активно використовуються керівництвом великих компаній, які є операторами критично важливих об'єктів (КВО) промисловості та критичної інфраструктури (КІ), як способи оптимізації виробничих процесів, збору та підготовки аналітичних матеріалів для прийняття ділових рішень, зменшення витрат при роботі з підрядниками [5]. Компаніями виробниками елементної бази та АСУ можливість віддаленого керування АСУ ТП розглядається як

фактор зменшення витрат на цикл підтримки виробництва продукції. Проте, поряд із можливостями, що відкриваються, і економією коштів новітні технології привносять і значні загрози безпеці [6].

Загальносвітовою тенденцією є посилення тиску несанкціонованих втручань (кібер-атак) на корпоративні інформаційні системи. Так, за даними підрозділу Міністерства внутрішньої безпеки США (Команди готовності до комп'ютерних надзвичайних ситуацій – Computer Emergency Readiness Team) кількість кібер-атак на сервери та мережі, що обслуговують федеральні урядові структури, в 2010 році становила понад 41 тис. випадків, і в порівнянні з попереднім роком зросла майже на 40% [7]. При нападах використовувалися вразливості програмного забезпечення, які не були виявлені і усунені в організаціях, що стали мішенню атаки.

Переломним моментом стало виявлення в 2010 році перших випадків зараження програмного забезпечення контролерів АСУ ТП на промислових підприємствах вірусом Stuxnet, що призвело до суттєвих негативних наслідків на об'єктах атаки [8]. Тому виявлення цього вірусу на фоні його масштабних руйнівних здатностей значно піднесло актуальність завдань забезпечення безпеки, захисту від терористичних і криміногенних загроз, кібер-атак та інших видів зловмисного втручання (проникнення) і викликало необхідність вжити додаткових заходів щодо забезпечення безпеки промислових систем.

2. Новітні кібер-загрози для АСУ ТП КВО та КІ

Відповідно до діючих нормативів промислові мережі, як правило, функціонують ізольовано не тільки від зовнішнього світу, а й від локальних мереж підприємства. Тому проникнення вірусу в системи моніторингу технологічних процесів визнавалося неможливим через, як вважалось, непереборне фізичне розмежування мереж. Проте з різних причин, в основному через недотримання організаційно-технічних регламентів на об'єктах критичної інфраструктури, були допущені випадки проникнення шкідливого програмного коду Stuxnet в АСУ промислових об'єктів [8].

Ціллю реалізованих на даний час атак Stuxnet є системи автоматизованого управління SCADA WinCC/PCS7 виробництва компанії Siemens. Крім того хробак "бачить" в мережі і засоби локального управління (контролери) PLC Simatic виробництва компанії Siemens та здатен їх перепрограмовувати (тобто змінювати параметри режимів ТП), а також накопичувати і передавати данні отримані з них. Зважаючи на розповсюдженість таких контролерів можна оцінити масштаби небезпеки, оскільки вони складають основну частину АСУ ТП багатьох об'єктів критичної інфраструктури, стратегічного та військового призначення, як, наприклад, контролери устаткування АЕС в Бушері (Іран), що вважаються експертами "ціллю" цієї кіберзброї.

Характерною особливістю вірусу Stuxnet є його перенесення всередині підприємства (між комп'ютерами, які не з'єднані мережею) за допомо-

гою зйомних носіїв інформації – заражених вірусом флеш накопичувачів (рис. 1).

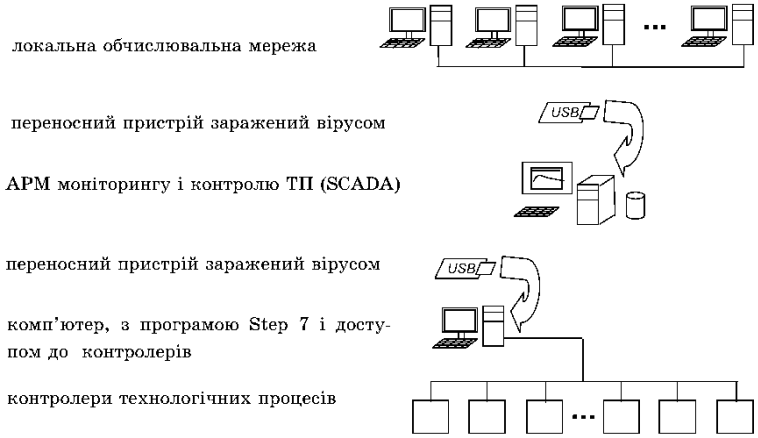

Рис. 1 – Атака Stuxnet

В жовтні 2011 р. фахівці корпорації Symantec повідомили про появу нової кібер-загрози – Duqu, яка може стати передвісником наступної хвилі спрямованих атак на промислові підприємства [9]. На їх думку розробники нового вірусу, як найменш, мали доступ до вихідного коду “хробака” Stuxnet. На відміну від Stuxnet, що був створений для роботи у промислових АСУ ТП, Duqu є класичною шпигунською програмою для збору конфіденційної інформації. Ціль Duqu – дані про устаткування і автоматизовані системи, що використовуються для управління виробничим циклом, які потрібні для здійснення подальшого зловмисного нападу з використанням засобів на зразок Stuxnet.

В березні 2012 р. Команда готовності до комп’ютерних надзвичайних ситуацій Міністерства внутрішньої безпеки США оприлюднила інформацію про виявлені спроби втручання в роботу АСУ об’єктів газотранспортних систем [10]. Розслідування наслідків спроб втручання показало, що ці кібер-атаки належать до однієї групи і пов’язані з фішинговою активністю, яка була спрямована проти персоналу компаній-операторів газотранспортних систем, починаючи з грудня 2011 р.

Аналізуючи наведені випадки здійснення кібер-атак, треба зазначити наступне. Характер і форми комп’ютерних нападів, від яких має бути розроблений захист, можуть істотно розрізнятися. Але, незважаючи на різноманітність типів атак, наслідки від них на найвищому рівні, як правило, включають:

- несанкціонований доступ або перехоплення інформації (втрата конфіденційності);

- несанкціонована зміна інформації, програмного забезпечення, обладнання і т.д. (втрата цілісності);
- блокування транзакцій та/або відключення системи (втрата готовності).

Професійно організована комп'ютерна атака складається з декількох етапів, пов'язаних із визначенням цілей, розвідкою, забезпеченням доступу до системи, безпосередньо реалізацією атаки, знищенням доказів про втручання.

Тому загальний план протидії кібер-нападам повинен включати заходи щодо:

- забезпечення можливості своєчасного виявлення та реагування на кібер-атаки;
- моніторинг та усунення виявлених уразливостей;
- відновлення пошкоджених систем, мереж і устаткування;
- зменшення (мінімізацію) наслідків таких нападів.

До потенційно вразливих складових інформаційної інфраструктури підприємства, що найчастіше використовуються як об'єкти нападу при здійсненні атаки на АСУ ТП, можна віднести:

- сервер організації, що має вихід в "зовнішній світ" (піддається постійним атакам через Інтернет);
- персональні мобільні комп'ютери (ноутбуки, планшетні комп'ютери, смартфони тощо), які функціонують на основі загально розповсюдженої ОС, мають уразливі місця та використовуються співробітниками та керівництвом підприємства спільно з робочими (захищеними) комп'ютерами (іноді здійснюється передача даних між персональним і робочим комп'ютером);
- апаратне забезпечення (комп'ютери) з підключенням до локальної мережі;
- комп'ютери, які мають порти для приєднання зйомних накопичувачів, дисководи для зчитування інформації з оптичних дисків.

Найбільшу загрозу безпеці об'єктів КВО та КІ становлять саме скоординовані атаки з використанням програмних вірусів. Такий вид атаки поєднує підготовчий етап (дії, що створюють на об'єкті нові уразливі місця) та атакуючі дії (використання уразливих місць). При цьому, підготовчі дії можуть здійснюватися значно раніше за часом ніж сама атака, можуть бути задіяні працівники (інсайдери) підприємства, що є об'єктом нападу, та здійснені різноманітні відволікаючі маневри.

 ISSN 1560-8956

3. Роль фізичного захисту при забезпеченні безпеки АСУ на об'єктах ядерної промисловості

Особливе значення має надійність АСУ ТП на АЕС, де законодавчо визначена необхідність практичного виключення аварійних ситуацій, які можуть призвести до радіаційного зараження і викиду радіаційних речовин у навколишнє середовище. Складовими частинами АСУ ТП є комплекс технічних засобів, оперативний персонал, програмне та інформаційне забезпечення. АСУ ТП мають складну структуру, і , як правило, будуються за технологічним (окремій ділянці об'єкту управління відповідає своя підсистема, наприклад, підсистема управління турбіною енергоблоку) та функціональним принципами (наприклад, підсистема збору та обробки інформації) [11].

Функції запобігання проникненню на критично важливі об'єкти покладено на систему фізичного захисту (СФЗ). Згідно рекомендацій МАГАТЕ фізичний захист формується на основі створення і вивчення проектної загрози, яка є описом ознак і характеристик потенційних інсайдерів і/або зовнішніх противників, які могли б здійснити спробу несанкціонованого вилучення ядерного матеріалу або диверсії, і проти яких розробляється і оцінюється система фізичного у захисту [12]. СФЗ об'єкту являє собою сукупність організаційних, адміністративних і правових заходів, інженерно-технічних засобів, а також дій підрозділів охорони, що мають в своєму розпорядженні спеціальні засоби, спрямовані на запобігання незаконному втручанню. До інженерно-технічних засобів СФЗ відносять фізичні бар'єри, сегментацію і допуски, технічні засоби і пристрої, програмне і апаратне забезпечення протидії мережевим кібер-атакам тощо.

Таким чином, захист АСУ ТП є елементом загальної конфігурації СФЗ, що визначається як сукупність підсистем СФЗ, функціонально пов'язаних між собою, що обумовлено основними технічними характеристиками цих підсистем і вимогами фізичного захисту, що задовольняються виконуються СФЗ.

Розробляючи проектну загрозу необхідно враховувати наступні характеристики загроз та особливості об'єктів, що захищаються [13]:

- можлива присутність на об'єкті внутрішніх правопорушників (інсайдерів), знання та навички, якими можуть вони можуть володіти;
- розуміння цілей зловмисників (диверсія, саботаж, крадіжка інформації тощо);
- національні нормативні документи, що регулюють питання безпеки на об'єктах ядерної інфраструктури, правила, норми тощо.

Ці характеристики допомагають визначити параметри та критерії виявлення, затримки і реагування при розробці СФЗ та оцінці її ефективності.

Серед можливих намірів (цілей) зловмисників можна назвати:

- порушення параметрів технологічного процесу (ТП), що призведе до важкої аварії;
- порушення параметрів ТП або керівний вплив, який призведе до зупинки реактору;
- крадіжка даних, технологічний шпіонаж;
- “таємне” проникнення для здійснення в подальшому координованої атаки.

Для кожної цілі можна побудувати множину ймовірних сценаріїв реалізації атаки, оцінка наслідків якої, як правило, здійснюється у вигляді комплексного (векторного) показника, що включає як компоненти кількість людських жертв, економічні втрати, час на відновлення системи, екологічні наслідки тощо.

4. Моделювання сценаріїв загроз та оцінка ефективності СФЗ

Побудова ефективної СФЗ для КВО та КІ пов’язана з вирішенням завдання щодо визначення параметрів заходів та засобів, що входять до структури СФЗ. Пошук рішення поставленого завдання параметричного синтезу здійснюється, як правило, шляхом використання спеціалізованого програмного забезпечення (ПЗ), що дозволяє моделювати множину можливих атак на об’єкт [14]. Важливою складовою таких програмних комплексів є модулі оцінки ефективності СФЗ, в яких реалізовані математичні методи моделювання сценаріїв загроз [15]. В той же час, складність взаємодії програмних та апаратних складових СФЗ, необхідність врахування засобів забезпечення інформаційної безпеки спричиняють певні труднощі для оцінки ефективності СФЗ. Тому існуючі методи моделювання загроз КВО і КІ та оцінки їх захищеності від зловмисного втручання потребують вдосконалення, розширення описових можливостей математичних методів, що застосовуються.

Розглянемо формальну модель опису сценарію загроз КВО та КІ. Нехай визначені елементи сценаріїв загроз (засоби виявлення, оснащення та озброєння порушників, бар’єри, засоби оповіщення та зв’язку, датчики та всі інші пристрої, які є суттєвими з точки зору реалізації загрози). Позначимо множину елементів сценарію $I = \{1, 2, \ldots, n\}$. Нехай задано скінчені множини станів для кожного елементу сценарію $S_i = \{s_i^{(1)}, s_i^{(2)}, \ldots, s_i^{(m_i)}\} \subset Z_+^{\cdot}\ i \in I$. Тобто станам елементів надані індекси (невід’ємні цілі значення), наприклад, множиною станів пристрою ідентифікації фізичної особи на контрольно-пропускному пункті може бути множина {1,2,3}, де 1 відповідає безвідмовному спрацюванню пристрою, 2 – відмові (особа, яка має право доступу ідентифікована як порушник), 3 – відмові (порушнику надано допуск).

Позначимо $x = (x_1^{\cdot} x_2^{\cdot} \ldots, x_m)$ – варіант реалізації СФЗ, який обирається з деякої множини можливих варіантів реалізації $X = \prod_{i \in I} X_i$. Варіанти реалізації СФЗ можна будувати за принципом “конструктора” з заданих альтернативних варіантів. Кожен з варіантів реалізації

СФЗ характеризується техніко-економічними показниками (вартість, надійність, енерговитратність, час реагування на загрозу). Нехай задана вектор-функція $C(x)$, за допомогою якої варіанти реалізації СФЗ оцінюються за техніко-економічними характеристиками, обмеженими вектором значень C_0.

Стан елементу сценарію $y_i(x,t) \in S_i$ залежить від реалізації СФЗ $x \in X$ та моменту часу $t \in T \subset R_+$. Нехай можна виділити m різних станів СФЗ, що визначають захищеність (реалізацію чи нейтралізацію певних загроз) об'єкту. Позначимо $S = \{s_1, s_2, \ldots, s_m\} \subset Z_+$ – множина станів СФЗ та $y(x,t)$ – стан СФЗ реалізованого варіантом $x \in X$ на момент часу $t \in T$.

Модель опису сценарію M встановлює зв'язок між станом елементів сценарію $y_1(x,t),\ y_2(x,t), \ldots, y_n(x,t)$ та станом СФЗ $y(x,t)$, тобто:

$$M : \prod\nolimits_{i \in I} S_i \to S.$$

Функціонування елементів сценарію характеризується ймовірностями перебування елементів у відповідних станах $p_i^{(s)}(x,t) = P\{y_i(x,t) = s\}$, $s \in S_i$, $t \in T$, $i \in I$. На основі моделі опису сценарію M, ймовірнісних характеристик елементів сценарію та із застосуванням логіко-ймовірнісного методу визначається $p^{(s)}(x,t) = P\{y(x,t) = s\}$, $s \in S$ – ймовірність перебування СФЗ в певних станах [16].

Нехай ефективність СФЗ можна оцінити деяким заданим критерієм $F(\cdot)$, що залежить від ймовірнісних характеристик стану, в якому СФЗ перебуває протягом інтервалу часу T. Тоді загальна постановка задачі підвищення ефективності СФЗ для КВО та КІ має наступний вигляд:

$$F(p(x,t), T) \to extr,$$

з врахуванням обмежень на використання ресурсів та вибору варіанту реалізації елементів СФЗ:

$$C(x) \leqslant C_0,$$
$$x \in X.$$

Представлена постановка задачі є узагальненою, а її розв'язування потребує застосування як спеціальних методів логіко-ймовірнісного аналізу, так і оптимізаційних процедур, побудованих з урахуванням сформованого (формалізованого) критерію ефективності СФЗ, який співвідноситься з конкретним КВО та КІ, або певною ситуацією, що склалася чи може скластися на цих об'єктах.

Висновки

Останнім десятиліттям все частіше при створенні АСУ та АСУ ТП використовуються мережеві технології обміну інформацією, що дозволяє здійснювати відділений доступ до елементів накопичення і обробки інформації (адміністрація веб-серверів, СУБД тощо). Це призвело до зростання ризику можливого здійснення терористичних атак на АСУ ТП

для КВО та КІ. Про ступінь загрози свідчать непоодинокі випадки зараження контролерів АСУ ТП на промислових підприємствах вірусом Stuxnet з тяжкими наслідками.

На сьогодні серед показників ефективності СФЗ треба розглядати спроможність протистояти спробам зараження внутрішніх програмних і апаратних засобів, що здійснюються з метою подальшого зловмисного впливу на АСУ ТП. В нормативному плані доцільно здійснити перегляд стандартів, норм, практики застосування стандартів безпеки на КВО та КІ. В якості зразку, що може бути поширений на КВО та КІ, доцільно використовувати вітчизняний та міжнародний досвід запровадження СФЗ на об'єктах ядерної промисловості.

Література

1. Ястребенецкий М.А., Иванова Г.М. Надежность автоматизированных систем управлення технологическими процессами. - М.: Энергоатомиздат, 1989. - 264 с.
2. Основы теории надежности автоматических систем управления / Л.П.Глазунов, В.П.Грабовский, О.В.Щербаков. – Л.: Энергоатомиздат, Ленингр.отд-ние, 1984. – 208 с.
3. ГОСТ 24.701-86 - Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения.
4. Черкесов Г.Н. Надежность аппаратно-программных комплексов. Спб.: Надежность аппаратно-программных комплексов. Учебное пособие. — СПб.: Питер, 2005. — 479 с:
5. Erbschloe M. Physical security for IT. – Elsevier Inc., 2005. – 231 p.
6. Критически важные объекты и кибертерроризм. – М.: Изд-во МЦНМО, 2008. – Ч.2: Аспекты программной реализации средств противодействия. – 607 с.
7. US Computer Emergency Readiness Team [Електронний ресурс] / Режим доступу [Веб-сайт]: http://www.us-cert.gov
8. Stuxnet Dossier // Symantec Security Response. – February. – 2011. – 68 p.
9. The precursor to the next Stuxnet // Symantec Security Response. – November. – 2011. – 46 p.
10. ICS-CERT Monthly Monitor [Електронний ресурс]. – April. – 2012. – Режим доступу: http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf
11. Безопасность атомных станций. Информационные и управляющие системы / М.А. Ястребенецкий (ред.). - К.: Техника, 2004. - 471 с.
12. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev.5) [Текст]. – Vienna: IAEA, 2011. – 57 p.

13. Оцінка загрози ядерного тероризму: проектна загроза [Текст] / СІ. Кондратов, Ю.М. Скалецький, В.І. Кравцов та ін.; за заг. ред. акад. НАН України В.П. Горбуліна - К.: ДП "НВЦ"Євроатлантикінформ 2006. - 76 с.

14. Бояринцев А.В. Проблемы антитеррористма: угрозы и модели нарушителей / А.В. Бояринцев, А.Г. Зуев., А.В. Ничиков - СПб.: ЗАО “НПП “ИСТА-Системс”, 2008. - 220 с.

15. Боровский А.С., Тарасов А.Д. Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов // Труды ИСА РАН. – Том 61 (1). – 2011. – С. 3 – 13.

16. Моделювання та оцінка сценаріїв загроз для об’єктів критичної інфраструктури [Текст] / Д.С.Бірюков, В.А.Заславський, В.В.Євгієнко, О.В.Франчук // Наукові записки НаУКМА. - 2009. - Том 99: Комп’ютерні науки. - С. 97 - 102.

Отримано 26.11.2012 р.