УДК 004:056

КЛАСИФІКАЦІЯ КІБЕРЗАГРОЗ СИСТЕМ КЕРУВАННЯ ПРОМИСЛОВОГО ОБЛАДНАННЯ

Сорокін М. С. к.т.н., доц., e-mail: sorokin.ekt@btu.kharkov.ua
Державний біотехнологічний університет

Актуальність дослідження. Мережевісистеми управління (МСУ) все частіше застосовуються для полегшення моніторингу та контролю під час автоматизації виробничого процесу. В останні роки назміну електромеханічним пристроям з жорстким підключеннямза допомогою провідників у так званих системах диспетчерського контролю і збору даних приходять підключені до інтернету за допомогою бездротових пристроїв до вбудованих мікроконтролерів датчиків та систем керування. Ці технології дозволяють модернізувати сучасніМСУ, досягнувши більш високої швидкості та менших експлуатаційних витрат. Тим не менш, останні події свідчать про значні проблеми з безпекою МСУ.

Метою досліджень є розглянути та запропоновати класифікацію кіберзагроз мережевих систем управління з технологічними процесами виробництва відповідно до міжнародних норм.

Основні матеріали досліджень. Безпека МСУ принципово відрізняється від IT-безпеки, оскільки МСУмають взаємодіяти з базовою фізичною інфраструктурою в режимі реального часу контролюючи або змінюючи параметри виробничого процесу. Відповідно там де є контроль або зміна параметру функції є потенційно небезпечним місцем для втручання. Незважаючи на те, що останні зусилля спрямованіна застосування рішень IT-безпеки до МСУ, ці рішення безпосередньо не усувають ризиків, пов'язаних зі зростаючою кількістю кібератак, які здатні поставити під загрозу дані датчиків управління [1], [2]. В результаті, незважаючи на значні досягнення в розробці відмово стійких МСУ, в кращому випадку мало розуміння їх стійкості до кіберінцидентів. Безперечно, питання кібербезпеки не розглядалися при проектуванні застарілих SCADA-систем.

Кібератаки з МСУ можна в широкому сенсі класифікувати як комп'ютерні аварії, нецільові атаки та цілеспрямовані атаки. Результатом кібератак може бути вплив на економічну діяльність підприємства, тобто погіршення технологічного процесу із метою недоотримання запланованого рівня прибутку. Отже втручання на такому рівні можна кваліфікувати як кібертероризм, що є суттєвим злочином.[3]Комп'ютерні аварії трапляються у вигляді повторноговиявлення ненавмисних збоїв IT. Нецільові атаки на МСУ схожі на інциденти, від яких може постраждати будь-який комп'ютер, підключений до мережі. Цілеспрямовані атаки на МСУ є найсерйознішим класом атак, оскільки зловмисники адаптують свої стратегії до компонентів автоматизованої системи керування технологічним процесом [4]. Найбільш яскравим прикладом можна вважати випадок коли черв'як Stuxnet [5] продемонстрував серйозні загрози для МСУ. Stuxnet має можливість інфікувати і перепрограмувати програмовані логічні контролери (ПЛК) і приховувати зміни за допомогою руткіта ПЛК. Кібератаки , націлені на системи МСУ, можуть бути класифіковані як атаки обману та атаки типу «відмова в обслуговуванні» (Denial of Service, DoS), які, відповідно, призводять до втрати цілісності та доступності даних систем контролю та управління. Працездатність для SCADA-систем можна визначити як їх здатність підтримувати виконання операцій шляхом запобігання, виявлення або стійкостідо атак обману. Атаки обману можуть включати неправильне вимірювання датчиків або введення над ними контролю, неправильну позначку часу або неправильну ідентичність пристрою, що посилає сигнал керування. Зловмисник може розпочати ці атаки, отримавши секретні ключі, що використовуються пристроями, що підключені до мережі, або імітуючи режим невідповідності певних датчиків та виконавчих механізми. Стійкість до кіберзагроз для SCADA-систем можна визначити як здатність підтримувати виробничий процес, запобігаючи або під дією DoS-атаки на датчики вимірювання та управління входами-виходами програмованих логічних мікроконтролерів. Щоб розпочати DoS-атаку, зловмисник може глушити канали зв'язку, перешкоджаючи виробничому обладнанню та пристроям

надсилати дані або наповнювати мережу зв'язку даними не пов’язаними із технологічним процесом.

Мережеві вразливості виникають в МСУ через чотири фактори. По-перше, завдяки широкому використаннюстандартних пристроїв комунікації.МСУ успадковують вразливості цих пристроїв, та таким чином, є об’єктомкіберзагроз відповідних програмних і апаратних засобів, що виходять з ладу. По-друге, власні мережеві протоколи традиційних SCADA-систем модернізуються до відкритих протоколів, щополегшує зловмисникам дізнаватися про операції МСУ. По-третє, дані датчиків керування стаютьдоступними для авторизованих віддалених користувачів через корпоративні мережі та Інтернет. Це робить МСУ об'єктом «інсайдерських» атак. По-четверте, існування організованих кіберзлочинних угруповань підвищує можливості зловмисників щодо здійснення вторгнень в МСУ.

Сучасні SCADA-системи мають ієрархічну структуру з регулюючими контрольно-наглядовими мережами. Атака **A0** позначає атаки на фізичну інфраструктуру або технологічні пристрої (датчики і виконавчі механізми). Оскільки такі атаки вимагають фізичного доступу, зловмисник, який не схильний до ризику, частіше здійснює кібератаки (**A1-A6**).Атаки **A1** і **A2** позначають атаки на систему мережі регулювання, яка взаємодіє з фізичною мережею каналів через технологічні пристрої. Атака **A1** позначає DoS-атаки на мережу зв’язків між ПЛК і технологічними пристроями, або атаку обману на датчик вимірювань або виконавчий пристрій. Атака **A2** позначає аналогічні DoS або атаки обману на мережу зав’язків між ПЛК. Під **A3** ми маємо на увазі кібератаки на мережу керування, яка забезпечує зв'язок між виробничим та наглядовим рівнями управління. Загроза керуючої мережі може вплинути на продуктивність як регулюючого, так і наглядовогорівнівкерування.Атаки **A4** та **A5** позначають атаки на наглядовий контрольний рівень, який реалізує державні оцінювачі для аналізу даних та спостерігачів для діагностики атаки/несправностей. Як правило, оцінки стану та діагностична інформація використовуються для формування заданих точок та параметрів контролера за допомогою процедури оптимізації або людського досвіду. Можливими атаками тут можуть бутиманіпулювання параметрами стану та давачів за схемою діагностики атаки/несправності. Звичайно, атаки **A1-A3** на регуляторну ланку також можуть вплинути на стан наглядовоїланки, оскільки останній може бути забезпечений неправильними даними, коли першізнаходяться під атакою та впливом зловмисників. Нарешті, **A6** позначає атаки на загальну мережу, наприклад, при злочиннихутручаннях, яким вдається взяти на себе роль оператора каналу і тим самим безпосередньо впливати на технологічний процес підприємства. При втручанні рівня А6 точка входу зловмисника може бути не тільки на рівні системи АСУ ТП, а й від будь якого відділу підприємства пов’язаного внутрішньою мережею із системою керування технологічним процесом [5].

Висновок.Таким чином, створивши систематизацію кіберзагроз, відповідно до наведеної класифікації можна виділити основні напрямки впровадження систем кіберзахисту промислового підприємства, а також планувати заходи безпеки на основі результатів оцінювання ризиків із метою оптимізації витрат на запровадження безпечної АСУ ТП.

ПЕРЕЛІК ПОСИЛАНЬ

1. A. Cardenas, S. Amin, and S. Sastry, «Research challenges for the security of control systems» in Proc. 3rd Conf. Hot Topics Security, Jul. 2008, pp. 1-6.

2. Y. Liu, M. K. Reiter, and P. Ning, “False data injection attacks against state estimation in electric power grids,” in Proc. 16th ACM Conf. Comput. Commun. Security, 2009, pp. 21-32.

3. Діордіца І. В. Поняття та зміст кіберзагроз на сучасному етапі / І. В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/

4. N. Falliere, L. Murchu, and E. Chien, W32.Stuxnet Dossier. Mountain View, CA: Symantec, Sep. 2010.

5. X. Litrico, P.-O. Malaterre, J.-P. Baume, P.-Y. Vion and J. Ribot-Bruno, "Automatic tuning of PI controllers for an irrigation canal pool",*J. Irrigat. Drainage Eng.*, vol. 133, no. 1, pp. 27-37, 2007.