УДК 004.7

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АСУТП

Юшкетова М.О.[1)], Кратінов О.Г.[2)]
Східноукраїнський національний університет імені Володимира Даля
[1)]магістрант; [2)]к т. н, доцент

І. Постановка проблеми

В даний час проблематика інформаційної безпеки АСУТП привертає все більшу увагу фахівців. Думка про те, що оскільки система SCADA не підключена напряму до мережі Internet, то вона володіє значним запасом уразливості по відношенню до зовнішніх кібератак, виявилась не спроможною. Про це свідчить збільшення кількості інцендентів, пов'язаних з інформаційним зломом комп'ютерних систем управління технологічними об'єктами, що призводить до численних аварій, збоїв та зупинок у роботі об'єктів і навіть їх фізичного руйнування. У роботі [1] приведена велика статистика інцендентів (2008 - 2010 р.р.), пов'язаних з відмовами устаткування АСУТП з причин інформаційної уразливості в електроенергетиці, в т.ч., ядерної, авіації, газодобувної промисловості, на транспорті та ін.

Проблема заслуговує серйозної уваги, якщо врахувати те, що, з одного боку, рівень автоматизації сучасних підприємств збільшується, системи управління набувають розподіленого характеру і «долають» великі відстані, використовуючи глобальні телекомунікації і мережеві технології, що, на жаль, збільшує можливость несанкціонованого втручання, а з іншого боку - не можна не відзначити активізацію та «успіхи» хакерних технологій.

Аналіз останніх публікацій показав, що Україна в 2013 р. опинилася на четвертому місці в світі по числу вихідних з країни кібератак [2] після Росії, Тайваню та Німеччини. Провідний німецький оператор зв'язку Deutsche Telekom повідомляє, що число інтернет-загроз постійно зростає - щодня виявляється близько 200 тис. нових зразків шкідників. Тільки в пастках Deutsche Telekom збираються записи про 450 тис. атак на день [3].

Частина з них безумовно адресована великим промисловим об'єктам. На думку багатьох фахівців, виявлений в 2010 р. черв'як Stuxnet, створений спеціально для атаки на сервера АСУТП і ПЛК, черв'як Shamoon і ряд інших проявів є прикладами нової кібер-зброї, здатної не тільки заподіяти непоправної економічної шкоди, але й викликати серйозні техногенні наслідки [4].

В Україні статистика таких інцедентів в літературних джерелах не наводиться, хоча це не позбавляє від проблеми, а ряд наявних публікацій не вичерпують усіх питань, що стосуються практичного забезпечення інформаційної безпеки систем управління промисловими об'єктами. Підходи до вирішення цих проблем повинні спиратися на загальні закономірності і сучасні досягнення в області безпеки інформаційних технологій, а з іншого боку - враховувати характерні особливості АСУТП як об'єкта захисту.

ІІ. Мета роботи

Проаналізувати технічні аспекти організації інформаційного захисту АСУТП, виходячи з особливостей її структури.

ІІІ. Виклад матеріалів дослідження

Як відомо, АСУТП є комп'ютерно-інтегрованої інформаційної системою і може бути поділена на декілька логічних рівнів, наприклад:

- верхній рівень, або рівень клієнтських додатків;
- середній рівень, або інформаційний рівень АСУТП, на якому розташована SCADA-система;
- нижній рівень - рівень контролерів, контрольно-вимірювальних приладів та виконавчого обладнання.

Такий поділ - не єдиний варіант, і в кожному конкретному випадку можуть бути здійснені різні підходи. Наприклад, нижній рівень, крім керуючих контролерів, може містити польову шину, яка є однією з мережевих технологій Field Bus, інтегруючі контрольно-вимірювальні датчики та виконавчі механізми. Вище рівня клієнтських додатків АСУТП може бути виділений рівень бізнесдодатків або рівень АСУ, що відображає інформаційній шар управління підприємства в цілому.

Однак, так чи інакше, можна зробити висновок про те, що АСУТП є мережевою ієрархічною багаторівневою системою. Це створює кращі передумови для реалізації концепції комплексного «багатошарового захисту» [4]. Сучасні мережеві технології дозволяють досить гнучко і надійно

структурувати подібні системи, як логічно, так і фізично, що важливо для забезпечення інформаційної безпеки. Правильно виконане структурування за рівнями і подальша сегментація дають можливість скоротити число інформаційних потоків, забезпечити їх необхідну спрямованість і фізичний поділ. При цьому сегментування, використовуване для ізоляції мережевих пристроїв за функціональним призначенням, може здійснюватися на основі технологій віртуалізації VLAN і забезпечувати певний рівень інформаційного захисту при передачі даних.

Логічно вважати, що найбільш критичні рівні з точки зору захисту - це верхній і середній рівні АСУТП. Перший є рівнем, який має вихід до зовнішніх комунікацій для підключення до мережі Internet, а другий - є центром управління та моніторингу АСУТП. До того ж тут також не виключаються зовнішні підключення. Нижній рівень, як правило, краще ізольований логічно і використовує ізольоване середовище на фізичному рівні (RS-232, RS-485, Field Bus та ін). Виходячи з цього, при організації системи захисту АСУТП необхідно обмежити число точок доступу у «зовнішнє середовище », а для кожної такої точки необхідно створювати демілітаризовану зону, що забезпечує поділ сегментів корпоративної та промислової мережі, а також захист зовнішнього периметру АСУТП ефективними засобами міжмережевого екранування.

Для виключення несанкціонованого доступу з корпоративного сегменту в сегмент АСУТП відомі рішення на основі систем односторонньої мережевої взаємодії, таких, як достатньо відома Fox-IT Data Diode. А длля передачі даних в межах сегмента АСУТП можна використовувати протоколи, які реалізують односпрямовану передачу.

Подальше поглиблення безпеки пов'язане із захистом внутрішнього периметру АСУТП – ретельним налаштуванням маршрутизаторів і комутаторів, в т.ч. з використанням механізмів ACL, підвищенням безпеки робочих станцій і серверів за рахунок використання прогресивного антивірусного програмного забезпечення і управління його оновленням, підвищенням рівня безпеки додатків, які забезпечують аутентифікацію, авторизацію і аудит при доступі до додатків, а також своєчасним видаленням невикористовуваних додатків, протоколів і сервісів.

На середньому та нижньому рівні все частіше використовуються спеціалізовані промислові польові міжмережеві екрани (Field Firewalls, Industrial Firewalls). У цій області пропонується ряд ефективних апаратних рішень у вигляді «модулів безпеки», що включаються безпосередньо перед захищуваним пристроєм, наприклад, керуючим контролером або кластером таких пристроїв (Tofino-security, Siemens, Modcon та ін). Зрозуміло, модулі безпеки повинні підтримувати відповідні протоколи АСУТП - Modbus TCP, Profibus, DNP3, OPC, CIP, CAN та ін., тобто, в даному випадку здійснювати інспекцію на прикладному рівні – контролювати функції читання та запису в протоколі та забороняти передачу кодових комбінацій, що призводять до некоректної чи аварійної роботи виконавчих механізмів.

Висновок

У роботі відзначається зростаюча актуалізація проблеми інформаційної безпеки АСУТП. Виявлено, що структурізація інформаційних потоків в АСУТП є об'єктивною базою для побудови ефективної системи безпеки. Показано, що вищі рівні АСУТП можуть бути захищені традиційними методами і засобами інформаційних технологій, а нижні рівні вимагають застосування спеціалізованих програмно-апаратних пристроїв.

Список використаних джерел

1. Гарбук С. В., Комаров А. А., Салов Є. І., НТЦ Станкоінформзаціта. В этой статье опубликованы аналитические данные по уязвимостям в АСУ ТП. По материалам Интернет-изданий за 2008-2010г. г.- Електроні дані 2008-2010. - Режим доступу: http://itdefence.ru, - Назва з домашньої сторінки інтернету.
2. ПАТ "Сегодня.ua ": Украина лидирует по количеству кибератак в мире - Електроні дані 2013. - Режим доступу: http://www.segodnya.ua/ukraine/Ukraina-lidiruet-po-kolichestvu-kiberatak-v-mire.htm. - Назва з домашньої сторінки інтернету.
3. Ярова Г. Украина на 4 месте в мире по количеству исходящих кибератак - Електроні дані 2013. - Режим доступу: http://ain.ua/2013/03/07/115754 # more-115 754. - Назва з домашньої сторінки інтернету.
4. Гречин А., Решение задач информационной безопасности в сфере АСУ ТП - Електроні дані 2008-2010. - Режим доступу: http://www.remmag.ru/admin/upload_data/remmag/10-6/Cisco.pdf, - Назва з домашньої сторінки інтернету.