УДК 519.711

ІНФОРМАЦІЙНА БЕЗПЕКА АСУТП ЕНЕРГООБ'ЄКТІВ

Васильченко В. І.[1], Гриб О. Г.[2], Лелека О. В.[1], Гапон Д. А.[2], Ієрусалімова Т. С.[2]

[1]Державне підприємство НЕК "Укренерго",
[2]Національний технічний університет "Харківський політехнічний інститут"

В статті розглянуті сучасні заходи інформаційної безпеки для роботи АСУТП енергооб'єктів.

Постановка проблеми. Подальше проведення реформ і впровадження ринкових відносин в енергетиці вимагають виконання заходів з підвищення ефективності енергооб'єктів і всієї енергетичної системи в цілому. Це може бути досягнуто за допомогою підвищення заходів безпеки проти сучасних інформаційних загроз для роботи АСУТП енергооб'єктів.

Аналіз останніх досліджень і публікацій. Згідно діючої нормативної документації це забезпечується вирішенням таких завдань [1]:

– вимірювання параметрів, приймання, опрацювання й представлення персоналу в зручному для сприйняття й прийняття рішень вигляді достатньої, достовірної і своєчасної інформації про хід технологічного процесу і стан устаткування;

– керування устаткуванням, у тому числі автоматична підтримка параметрів у межах, обумовлених проектом або заданих оперативним персоналом, а також виконання комплексів дискретних керуючих дій регулювальними органами для приведення параметрів в експлуатаційні або задані межі, у нормальних, передаварійних, перехідних і післяаварійних режимах роботи (дистанційне і програмно-логічне керування, а для АЕС, крім того, – управління системами забезпечення безпеки);

– релейний захист і автоматика основного електричного устаткування енергоблоку або агрегату (генератора, блочного трансформатора, робочого і резервного трансформаторів власних потреб і випрямного трансформатора);

– приведення устаткування і його агрегатів у безпечний стан системами технологічного захисту шляхом зниження навантаження або зупину, якщо виникла аварійна ситуація (відхилення параметрів за допустимі межі);

– синхронізація блока генератор-трансформатор або генератора з електромережею;

– реєстрація проходження технологічного процесу, контрольованих параметрів і параметрів, що відхилились від заданого значення;

– розпізнавання і реєстрація передаварійних, аварійних і післяаварійних подій і ситуацій, процесів, а також виявлення першопричин аварій і спрацьовування захистів;

– розрахунок техніко-економічних показників(ТЕП) роботи агрегату;

– діагностика стану устаткування, діагностика і опробування комплексів засобів автоматики (КЗА);

– оповіщення оперативного персоналу за допомогою світлового і, у разі необхідності, звукового сигналів, а також у вигляді повідомлень на терміналах оперативного контуру керування про порушення нормальної експлуатації устаткування (попереджувальна сигналізація), а також про порушення меж і/або умов безпечної експлуатації (аварійна сигналізація);

– оперативне представлення персоналу узагальненої інформації про поточний стан устаткування й інформаційна підтримка персоналу для забезпечення правильності операторської діяльності в аварійних ситуаціях;

– обмін достовірною технологічною і техніко-економічною інформацією про роботу технологічного об'єкта керування із суміжними системами і верхнім рівнем ієрархічного керування.

Отже у підсумку АСУТП вирішує наступні задачі:

– контроль і облік параметрів технологічних процесів;

– забезпечення надійності та безпеки управління технологічними процесами і підвищення на цій основі надійності електропостачання споживачів;

– оптимізація управліннями технологічними процесами;

– збереження та продовження ресурсу технологічного обладнання;

– запобігання аварій та ліквідація їх наслідків з меншими витратами;

– економія експлуатаційних витрат і скорочення чисельності обслуговуючого персоналу;

– зниження економічних втрат, що виникають внаслідок недостатньої інформаційної та загальної безпеки;

– зниження вартості володіння технологічним об'єктом.

Мета статті. Розглянути сучасні заходи інформаційної безпеки для роботи АСУТП енергооб'єктів.

Основні матеріали дослідження. В АСУТП енергооб'єкта нижнім рівнем є АСУТП установок та систем, а верхнім - енергооб'єктовий.

При цьому АСУТП енергооб'єкта забезпечує виконання функцій і вирішення задач, інформаційна база яких формується за рахунок інформації від різних установок та систем (приєднань) і з рівня енергосистеми, а також тих задач, керуючі дії яких реалізуються на декількох установках та системах (приєднаннях) енергооб'єкта або за його межами.

АСУТП установок та систем забезпечує функціонування цих структурних одиниць енергооб'єкта у відповідності з завданнями (критеріями, уставками) верхнього рівня АСУТП енергооб'єкта в нормальних і аварійних режимах роботи.

У випадку відсутності зв'язку АСУТП установок та систем з верхнім рівнем, вона, а також та частина АСУТП енергооб'єкта, що зберегла зв'язки з іншими АСУТП установок та систем, забезпечує виконання тих функцій і задач, для яких існує необхідна інформаційна база і виконавчі механізми для реалізації керуючих дій. У підсистемах (системі) електричної частини АСУТП енергооб'єкта нижній рівень утворюють мікропроцесорні пристрої керування, релейного захисту і автоматики (РЗА), що забезпечують контроль, керування і захист кожного з елементів основного електричного устаткування і кожного приєднання, об'єднаних системоутворюючою мережею (магістраллю).

АСУТП на підстанціях є низовим рівнем системи управління, який безпосередньо пов'язаний з технологічним обладнанням. В рамках АСУТП збирається первинна інформація по всіх параметрах технологічних процесів, вирішуються завдання метрологічного забезпечення, виконуються процедури прямого регулювання та дистанційного управління обладнанням, виконуються роботи по збереженню ресурсів. З цього випливає, що ефективність технологічних процесів, по суті забезпечується на рівні АСУТП.

Крім того, цей рівень є джерелом інформації для верхніх рівнів управлінської структури. І багато в чому визначає ефективність управління всією енергетичною системою. Тому завдання створення АСУТП на підстанціях є досить актуальною в рамках комплексу робіт з удосконалення та модернізації системи управління енергетичної компанії.

У зв'язку з цим цілісність і вірність інформації є першочерговим завданням. У минулому захист АСУТП був побудований на принципах закритості і невідомості,тобтосистеми були повністю незалежними і не обмінювалися інформацією між собою, мережеві протоколи були закритими і пропрієтарними. Проте, існуючі АСУТП широко поширені і мають доступ до мережі.

Оскільки системи побудовані на базі загальновідомих протоколів, вони уразливі для внутрішніх і зовнішніх кіберзагроз [2]. Через особливості функціонування АСУТП, вони сильно відрізняються від загальних інформаційних систем з точки зору забезпечення безпеки. Так як аналіз ризиків і безпеки йде не тільки на підставі базового програмно-апаратного комплексу, але і з точки зору керованих і експлуатованих об'єктів.

АСУТП були спочатку розроблені для управління і контролю промислових процесів з використанням власних закритих протоколів. Вони звичайно знаходилися в ізольованих мережах. Тим не менш, в останні роки, АСУТП системи були підключені до корпоративних мереж та Інтернету. Це дозволило компаніям контролювати процеси, і допомагало приймати правильні і вигідні рішення.

Однак недоліком цього є те, що АСУТП ніколи не розроблялися з урахуванням безпеки. З комунікаціями на основі Інтернет-протоколу (IP), з'явилися несподівані загрози, яких не було в попередніх системах, які можуть з'явитися в будь-якому місці в будь-який час.

Однією з головних причин, чому IP є надзвичайно успішним у тому, що він може бути використаний практично скрізь як на віртуальних, так і на фізичних пристроях.

У складних АСУТП, є безліч як дротових, так і бездротових засобів зв'язку та протоколів, що беруть участь в отриманні даних в центральну систему моніторингу. Це дозволяє реалізувати сильні сторони IP мереж АСУТП на змішаних системах стільникового, супутникового, і фіксованого зв'язку.

Для передачі даних, можна використовувати різні діапазони дротових (телефонних ліній, оптичні волокна, ADSL, кабелі) і бездротової комунікацій (радіо, стільниковий зв'язок, WLAN, або супутниковий зв'язок). Вибір того чи іншого типу зв'язку залежить від ряду факторів, які характеризують існуючу інфраструктуру.

Такі фактори, як існуючого обладнання, з'єднань, доступних комунікацій в ізольованих ділянках, швидкості передачі даних і частоту опитування, віддаленості обладнання, бюджет установки і можливістю розміщення для покриття майбутніх потреб. Все це впливає на остаточне рішення для архітектури побудови зв'язку.

Головною особливістю нових АСУТП є використання протоколів глобальної комп'ютерної мережі (WAN), такі як TCP/IP, SONET/SDH, MPLS, ATM таFramerelay. Завдяки можливості розподілу функцій і процесів через WAN можна домогтися високої живучості системи, так розподіляючи обробку інформації на фізично розподілених системах стає можливим побудувати систему АСУТП яка зможе пережити повну втрату устаткування в будь-якому місці. Є два типи різних загроз, які можуть вплинути на сучасні АСУТП:

- Перший тип загроз є несанкціонований доступ до програмного забезпечення управління, будь то доступ людини, вірусні атаки або інші втручання, при

яких відбувається навмисні або ненавмисні зміни деяких параметрів.

- Другим типом загроз є загроза пакетного доступу до сегментів мережі, де знаходиться компоненти АСУТП.

Для розуміння потенційних загроз у галузі безпеки необхідно займатися відтворенням існуючих мереж АСУТП.

При цьому слід брати до уваги:

- наявність фізичного доступу в Інтернет;
- використаними протоколами безпеки і аутентифікації;
- використання спеціалізованих протоколів і закритих інтерфейсів для приховування проломів в безпеці.

Наступний список показує способи підвищення захисту мереж АСУТП в поєднанні з корпоративною мережею, як описано в [3]. Заходи безпеки через АСУТП з точки зору технології можуть бути подані наступним чином:

- суворі обмеження та контроль для зовнішніх підключень;
- впровадження розмежувань і нейтральних зон (DMZ);
- підвищення безпеки за допомогою віртуальних приватних мереж (VPN) на додаток до інструментів цілісності серверів;
- мінімізація шляхів доступу до внутрішньої мережі і підвищений рівень спостереження;
- шифрування листів і блокування файлів і каталогів;
- регулярна і ретельна перевірка безпеки і уразливості розвиток контролю та методів контролю, щоб впоратися з будь-якими випадковостями в обладнанні АСУТП.

Більш детально ці заходи описуються в [4].

Висновки. З наведеного матеріалу можна зробити слідуючи висновки.

Мережа АСУТП повинна бути фізично відділена від корпоративної мережі та інших ненадійних мереж. Коли фізичний поділ неможливий, можна розділити мережу логічно.

Логічний поділ може виявитися більш складним у реалізації і ризикує бути неефективно сконфігурованим.

Уникати використання технології віртуальної локальної мережі (VLAN) для логічного поділу мережі АСУТП від корпоративної мережі, так як технологія VLAN не призначена в якості міри безпеки, а є інструментом для обмеження пропускної здатності.

Зв’язки, які походять від зовнішніх ненадійних мереж до мережі АСУТП, повинні бути обмежені буферної мережею.

Повинні бути заборонені прямі з’єднання з компонентами АСУТП; пристрої всередині мереж АСУТП не повинні спілкуватися з незахищеними мережами.

Якщо потрібно використовувати компоненти існуючої корпоративної мережевої інфраструктури, такі як комутатори, маршрутизатори і канали глобальної мережі передачі даних то необхідно організовувати захищений канал передачі даних.

Потрібно уникати пристроїв АСУТП, які підключаються до двох або більше мереж з різними рівнями безпеки. Для надійного захисту необхідно використовувати активний захист, наприклад:

- брандмауери (Firewall);
- системи запобігання вторгнень (IPS);
- антивірусне програмне забезпечення.

На етапі проектування необхідно забезпечити виконання вимог безпеки і на етапі реалізації повинні проводитися випробування системи. Крім того, слід розглянути питання про використання груп стандартів з безпеки (IEC 62443) в якості моделі при побудові АСУТП.

Список використаних джерел

1. ГКД 34.20.507-2003 "Технічна експлуатація електричних станцій і мереж. Правила", 2003.
2. D. H. Ryu, H. Kim, and K. Um, "Reducing security vulnerabilities for critical infrastructure", Journal of Loss Prevention in the Process Industries, 2009.
3. "Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress", CRC Report RL32114, 2008.
4. Centre for the Protection and National Infrastructure, Good Practice Guide: Securing the Move to IP-Based SCADA/PLC Networks, 2011.

Аннотация

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУТП ЕНЕРГООБЪЕКТОВ

Васильченко В. И., Гриб О. Г.,
Лелека А. В., Гапон Д. А.,
Иерусалимова Т. С.

Рассмотрены современные средства информационной безопасности для работы АСУТП энер-гообъектов.

Abstract

INFORMATION SAFETY IN POWER UTILITIES AUTOMATED PROCESS CONTROL SYSTEMS

V. Vasilchenko, O. Gryb, A. Leleka,
D. Gapon, T. Ierusalimova

The modern means of information security for power utilities process control systems are described.