doi:https://doi.org/10.15407/emodel.41.01.093

УДК 519.7-004.65

М.Ю. Комаров, аспірант
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(Україна, 30164, Київ, вул. Генерала Наумова, 15,
тел. +3809870000344, e-mail: maxkom@i.ua)

Загальні характеристики підприємства електроенергетики і елементи їх вразливості технологічного походження

Наведено відомості щодо способів забезпечення функціонування мереж підприємств електроенергетики. Описано традиційні засоби захисту інформації. Надано результати огляду вразливостей індустріальних мереж. Дано аналіз підходів до захисту від загроз кібербезпеці.

Ключові слова: кібербезпека, підприємство електроенергетики, вразливість, захист периметра, захист мережі, міжмережевий екран.

Забезпечення кіберзахисту інформаційних мереж підприємства електроенергетики при реалізації заходів протидії сучасним кіберзагрозам є невід'ємною частиною політики безпеки інформації підприємств енергетичної галузі. Аналізуючи загальні загрози безпеці інформації при розробці політики безпеки на підприємстві енергетичного сектору, необхідно враховувати специфіку його функціонування, а також брати до уваги технологічну та функціональну специфіку обробки інформації, що циркулює на відповідних об'єктах інформаційної діяльності.

Інформаційні мережі підприємств електроенергетики завжди суттєво відрізнялися від традиційних корпоративних мереж. Незважаючи на те що певна частина ресурсів мережі підприємства електроенергетики фактично використовується для корпоративних комунікацій, велика частина її інфраструктури призначена для обміну даними з промисловим обладнанням за допомогою різних протоколів. Спочатку мережі підприємств електроенергетики були розроблені з метою виконання єдиної задачі: забезпечувати операторів інформацією про стан електромережі. Кібербезпека не розглядалася навіть як віддалена перспектива. Фактично у XX столітті кібератаки були практично невідомі в промисловому середовищі. Навіть в процесі

© Комаров М.Ю., 2019

еволюції в сучасні інтелектуальні мережі оператори, як і раніше, забезпечували мінімальний захист інфраструктури службової мережі.

На початку XXI століття з'явилося нове розуміння потенційних збитків, до яких можуть призвести кібератаки. Це, в свою чергу, спонукало операторів приділяти більше уваги безпеці мереж, що мають критичне значення. Першим кроком став набір вимог NERC CIP, прийнятий у 2008 р. Проте кібербезпека розглядалася переважно в рамках її традиційного IT розуміння, і проблеми розглядалися та оброблялися в рамках такого розуміння усунення загроз.

Традиційні засоби захисту. Традиційно захист мережевих пристроїв засновано на двох базових елементах:

1) антивірусне програмне забезпечення (ПЗ) певного типу, що працює на обчислювальній машині і використовує для аналізу комбінацію евристичних моделей поведінки разом з іншими моделями або сигнатурами та допомагає виявити шкідливе ПЗ, запущене на зараженій машині;

2) міжмережевий екран.

Механізм захисту в ранніх версіях міжмережевих екранів ґрунтувався на заздалегідь налаштованому знанні додатків, мережевих взаємозв'язків між ними і механізму примусової підтримки існуючих взаємозв'язків. В цьому випадку обмінюватися даними можуть тільки підтверджені хости і додатки. У більш пізніх версіях міжмережевих екранів було додано механізм Deep Packet Inspection (DPI), що привело до появи гібрида брандмауера (антивіруса), який має можливість перевіряти характеристики даних, що проходять через міжмережевий екран.

Нові пакетні технології та захист за допомогою секретності. У XX столітті почалась заміна традиційних мереж SONET, SDH, PDH (які використовувалися багато років) мережами на основі пакетних технологій. Існує безліч передумов такої заміни, проте слід зазначити, що такий перехід істотно підвищує ризик появи кіберзагроз для електромереж. Традиційна технологія SONET (SDH) значно менше вразлива для такого роду загроз, в порівнянні з пакетною технологією, через її природню статичність і відсутність рівня сигналізації. Крім того, статична природа мережі не дозволяє зловмисникам міняти своє розташування за бажанням. З іншого боку, пакетні технології дозволяють динамічно прокласти шлях до будь-якої точки мережі за допомогою системи адресації. Зрештою, деякі пакетні протоколи і технології мають рівень сигналізації, який робить їх особливо вразливими для кібератак.

Виробники промислового обладнання завжди дотримувалися спільної думки про те, що системи залишаються захищеними від кібератак до того часу, поки їх інтерфейси та комунікаційні структури тримаються в секреті

від сторонніх осіб. Вони впевнено вважали, що, не маючи деталізованих специфікацій, зловмисники не зможуть обмінюватися даними з обладнанням (і, ймовірно, навіть не стануть намагатися це робити). Багато хто погоджувався з тим, що такий підхід приховування інформації заблокує всі можливості для проведення кібератак на окремі пристрої або мережі.

Вразливості індустріальних мереж. Основною відмінною рисою мережі енергосистеми (ЕС) є використання протоколів управління (Industrial Control Protocol, відомі як протоколи SCADA, системи диспетчерського управління та збору даних) на додаток до стандартних корпоративних комунікацій. Системи SCADA використовуються не тільки в енергетиці, але і в мережі підприємств електроенергетики для управління критично важливим обладнанням. Втрата зв'язку з таким обладнанням або будь-які навіть незначні збої в системі зв'язку можуть швидко стати причиною виникнення катастрофічних ситуацій, що супроводжуються відключенням електроенергії на кілька днів, тижнів або навіть місяців. Тому безпека комунікаційної мережі має критичне значення. Враховуючи те, як мало уваги було приділено забезпеченню безпеки в мережах ЕС на початкових етапах їх розробки, не дивний той факт, що в даний час ці мережі мають безліч вразливостей. Розглянемо вразливості, властиві початковим проектам мереж, а також сучасні засоби захисту.

Вразливості обладнання зв'язку з об'єктом (Remote Terminal Unit (RTU)) і SCADA. При розробці промислових пристроїв і протоколів питання їх безпеки практично не враховувалися. В кращому варіанті захист здійснювався за допомогою підвищеної секретності. В даний час жоден з провідних протоколів SCADA (DNP3 в Північній Америці і МЕК-101 в Європі) не має механізмів для виконання аутентифікації або перевірки будь-яких команд, які вони отримують. Цю вразливість було продемонстровано в рамках проекту Аврора в 2007 р. в національних лабораторіях Айдахо, в якому група хакерів мала пошкодити навчальну електростанцію. Хакери успішно проникли на навчальну електростанцію і запустили процес самознищення генератора. Поява вірусу STUXNET у 2010 р. стала черговим болючим нагадуванням про цю вразливість. Вірус STUXNET відправляв помилкові і шкідливі команди на Siemens PLC через множинні лазівки в захисті консолі управління.

Фірмові властивості обладнання RTU і SCADA також створюють проблеми. Через високу чутливість коду ПЗ промислового обладнання операторам мереж підприємств енергетики часто заборонено вносити зміни, такі як оновлення операційної системи або установка латочок в системі безпеки. В результаті існує безліч дірок в системі безпеки, які не покриваються існуючими виправленнями або іншим способом в RTU або промисловому обладнанні, яке працює на стандартних операційних системах.

Зрештою, слабкі сторони підходу, заснованого тільки на секретності, обговорювалися багато разів не тільки в згаданих вище випадках, але і пізніше на конференції Black Hat, включаючи віддалене управління системами командування патрульною службою та дозаторами інсуліну.

Вразливості в мережах підприємств електроенергетики. Одним з питань аналізу вразливостей, яке рідко розглядається, є мережева технологія, що використовується. Оскільки традиційні системи рідко піддавалися атакам, а більш сучасні мережі менше захищені, безпека мережевих технологій, що використовуються, не вивчалася належним чином.

Існують дві великі групи атак, які пов'язані з мережевою технологією:

1. Атаки на рівні управління мережею (control plane) — деякі з сьогоднішніх пакетних мереж мають рівень управління, створений розробниками протоколів для спрощення надання каналів зв'язку. Можливість динамічно задавати пункти призначення за допомогою таких протоколів, як BGP і OSPF, дозволяє руйнування мережі або виведення її з ладу. Простим поширенням шкідливої інформації зловмисник може зробити так, що мережа відправлятиме трафік «в нікуди», створюючи кільця з маршрутів або виконуючи інші шкідливі дії. Фактично це дозволяє вивести з ладу всю мережу, використовуючи один інтерфейс. В протоколах, які використовують IP, MLPS і MPLPS-TP, окремий незахищений вузол може послужити причиною виходу з ладу всієї мережі. Саме це сталося в кінці 2010 р. в Китаї, коли невірна інформація про маршрути від одного провайдера призвела до недоступності Інтернету. Проблему ускладнює той факт, що мережі підприємств електроенергетики зазвичай мають досить велику кількість фізично незахищених місць. Зловмисник може легко проникнути на автоматичну підстанцію, ввести шкідливу інформацію в мережу і повністю деактивувати її.

2. Атаки на рівні передачі даних (data plane) — атаки Denial of Service (DoS) є класичним прикладом атак при передачі даних. Зазвичай DoS атаки бомбардують ціль безліччю фальшивих запитів на з'єднання, що призводить до виснаження ресурсів приймаючої сторони настільки, що вона ледве встигає обробляти дійсні запити. Іноді всі ресурси виснажуються і система стає повністю недоступною. DoS атаки є простими у виконанні, вони націлені на саму чутливу частину мережі — здатність до активного з'єднання. Для підприємства електроенергетики втрата зв'язку з RTU або обладнанням релейного захисту може дуже швидко привести до втрати контролю над електромережею і відключення електроенергії на значній території. Тому DoS атаки особливо небезпечні для внутрішніх службових мереж. Однак DoS атаки не є єдиним серйозним типом атак на рівні передачі даних. Інші атаки включають перехоплення мережевих ресурсів і напад на станції управління.

Поєднання атак 1 і 2 становить значну загрозу, яка неминуче присутня в мережі. Вразливість залежить від архітектури і реалізації мережі і її можна виправити або звести до мінімуму в результаті перегляду мережевої архітектури.

Підходи до захисту від загроз кібербезпеці. Для усунення вразливостей операційних мереж може бути застосовано кілька тактик. Сучасні підходи до забезпечення безпеки є дуже різними, однак існує тенденція до використання IT технологій.

Захист периметра. Перший набір захисних засобів, націлений на заборону будь-яких контактів мережі з вузлами, що лежать за її межами. До засобів захисту периметра мережі належать:

Міжмережеві екрани, розроблені для управління обміном інформацією. Вони дозволяють створювати з'єднання тільки між заданими об'єктами і можуть дозволити або відхилити запити на з'єднання, а також перевірити ім'я користувача і пароль віддалених користувачів. Проте їх ефективність обмежена, оскільки після надання дозволу на з'єднання вони не володіють інформацією про дані, що передаються. Таким чином, шкідливий код або помилкові дані потенційно можуть потрапити в мережу.

Зашифровані VPN мережі, які зазвичай використовуються в поєднанні з міжмережевими екранами. Цей засіб дозволяє виконати безпечний обмін даними між різними елементами периметра безпеки ESP (Electronic Security Perimeter). По суті, це є захистом від атак «людина посередині», націлених на отримання доступу до інформації управління.

Більшість заходів щодо забезпечення безпеки випливають з концепції захисту периметра мережі. Обмеження таких заходів зазвичай пов'язані з тим, що фізично здійснити впровадження в мережу підприємства енергетики відносно просто. Якщо інші мережі (наприклад, операторські) розміщують своє устаткування в добре захищених приміщеннях, таких як вузли та центральні офіси, комунікаційне обладнання підприємств електроенергетики розташоване в безлюдних, погано захищених місцях, куди досить просто проникнути фізично і уникнути захисту периметра мережі. Тому критично важливо звести до мінімуму можливість проникнення в мережу. Саме тут потрібно застосовувати додаткові заходи захисту.

Захист мережі. Архітектура і протоколи зв'язку, що використовуються для мережі підприємства енергетики, містять безліч потенційних вразливостей. Обрана мережева технологія може значним чином вплинути на стабільність і чутливість мережі до кібератаки. Існує кілька способів уникнути захисту системи безпеки мережі, до яких належать атаки на рівнях управління і передачі даних. Відповідно існують методи зведення до мінімуму або придушення загроз, які дозволяють підвищити безпеку і стійкість мережі, не впливаючи на її продуктивність.

Протидія атакам на рівні управління. Одним з найнебезпечніших типів атак є атака на рівні управління, коли атакуючий пошкоджує управління мережею, у результаті чого мережа стає повністю недоступною. Такий тип атаки викликає особливе занепокоєння, оскільки отримання доступу принаймні до одного вузла потенційно може привести до виведення з ладу всієї мережі. По суті, вся мережа захищена рівно в тій мірі, наскільки захищений найслабкіший канал. Отже, безпека мережі електроенергетичного підприємства залежить від доступу до найменше захищеної підстанції.

Мережі, які включають рівень управління або протокол сигналізації, дуже чутливі до атак такого типу. До них належать мережі типу MPLS і IP. Вразливості на рівні управління були продемонстровані безліч разів як організаціями стандартизації (IETF RFC 4272, 5920 і 6941), так і на конференціях, присвячених хакерським атакам. Фактично техніку виведення з ладу мережі MPLS через рівень управління було продемонстровано в реальному часі на конференції Black Hat в 2011 р.

Оскільки пригнічення атак можливо тільки до певної міри, загроза небезпеки залишається до тих пір, поки існує площина управління. Мережі, засновані на технології без рівня управління, завжди будуть надійнішими. До них належать мережі SONET і SDH і Carrier Ethernet. Засобів для проведення атаки на рівні сигналізації мереж SONET і SDH або Carrier Ethernet не існує. Обидві технології вимагають наявності керуючої станції для функціонування мережі. При забезпеченні безпеки керуючої станції атаки на площину управління стають неможливими.

Протидія атакам на рівні передачі даних. Атаки на рівні передачі даних є потенційним джерелом загроз. Хоча такі атаки мають тенденцію до збільшення вузьконаправленості (наприклад, DoS атаки направляються на певний хост), потенційні втрати зв'язку між станцією оператора і RTU можуть перешкодити управлінню мережею. Як і у випадку атак, спрямованих на рівень управління, атаки на рівні передачі даних можуть бути пригнічені внаслідок зміни схеми мережі.

У сценаріях, де з'єднання зв'язку задані жорстко (як у SONET і SDH або Carrier Ethernet), атакуючому набагато складніше вивчити мережеві елементи без встановлення з ними прямого з'єднання. Така жорсткість при передачі даних відкриває доступ до мінімальної кількості частин кожного хоста в мережі та закриває інші частини, які можуть бути більш вразливими. У випадках, коли існує маршрутизація мережі (така як MPLS і IP), зловмисник може зібрати інформацію через перехоплення і шпигунство в мережі з незахищеного вузла, після чого використовувати помилкові адреси для підготовки атаки.

Іншим способом підвищення безпеки і захисту від нелегального проникнення або навмисного спотворення інформації є використання протоколів аутентифікації джерела. Найбільш важливим з них є 802.1X на основі Ethernet, який перевіряє кожен доданий пристрій в централізовано керованій базі даних. Він використовує шифрування для того, щоб перевірити справжність нового пристрою і упевнитися, що він не маскується під існуюче мережеве обладнання. Це гарантує, що всі підключені до мережі пристрої дійсно є справжніми аутентифікованими мережевими пристроями, а не пристроями, доданими хакерами.

Внутрішній захист додатків (захист від шкідливого ПЗ). Найскладнішими для виявлення є атаки зсередини, які надходять з елементів, розташованих в мережі. Вони є загрозою з різних точок зору.

По-перше, вкрай складно прийняти рішення відносно того, чи є певна команда дійсною або шкідливою. Деякі команди (наприклад, команда на виведення з експлуатації старого блоку RTU) можуть бути коректно використані у випадках, коли їх відправляє авторизований персонал, однак вони можуть завдати шкоди, якщо були відправлені іншими особами без належних повноважень.

По-друге, оскільки атаки проводяться за різними напрямками, для забезпечення безпеки всієї мережі потрібна система, яка є у всіх елементах і площинах, і відстежує всі можливі напрямки атаки. Деякі утиліти використовують міжмережевий екран для уникнення ризику того, що один вузол буде контролювати інший, а також для стримування кіберзагроз на місці їх виникнення. Проте це може викликати більш широке блокування або відключення мережі. Чим більша підстанція залучена в цей процес, тим вище ризик ураження мережі.

Нарешті, стандартному міжмережевому екрану важко контролювати команди. Попри те, що стандартні міжмережеві екрани з активною функцією DPI здатні перевіряти корисне навантаження програмного забезпечення з метою визначити, чи присутня там виділена раніше сигнатура, і відзначити потенційні збіги, вони не мають можливості оцінити, чи є певна команда істинною або шкідливою.

Всі ці обмеження обумовлюють, здавалося б, нездоланні труднощі, пов’язані з внутрішніми загрозами. При цьому відповідно до NERC CIP очікується, що електроенергетичні підприємства будуть вирішувати такі проблеми. Зокрема, вони повинні виявляти і блокувати ситуації, коли якесь обладнання, RTU або консоль управління, захоплено шкідливим ПЗ, та мати змогу зупинити виконання шкідливих дій. Для того щоб мережа змогла впоратися з усіма обмеженнями, пов’язаними з існуванням внутрішніх загроз, потрібно врахувати кілька факторів. Розподілений характер

можливих атак не дозволяє застосовувати централізоване або перехідне вирішення таких проблем. Крім того, рішення повинні бути зрозумілими для систем управління виробничим процесом (ICS) і інтелектуально розпізнавати команди, щоб визначити, чи дійсною є певна команда чи шкідливою.

Отже, ідеальне рішення являє собою розподілений міжмережевий екран з перевіркою команд ICS. Рішення такого типу може бути присутнім у всіх елементах, оскільки воно інтегровано в структуру мережі (будучи частиною мережевого комутуючого обладнання). При цьому здатність брандмауера з підтримкою ICS визначати достовірність різних команд систем SCADA використовується для того, щоб виявити внутрішні атаки або загрози, які виникають в результаті попадання шкідливого ПЗ в мережу.

Два основних елементи ідеального рішення — присутність у всіх частинах мережі і розпізнавання додатків — випливають з характеристик атак. Розподілений характер мереж підприємств електроенергетики, а також той факт, що більшість елементів мережі можуть бути не захищені належним чином, змушує віддати перевагу розподіленому підходу перед централізованим. Єдиним способом впровадження такого рішення без перенаправлення всього трафіку в центр, викликаючи перевантаження, є розподілене використання інтелектуального аналізу команд. При цьому у зв'язку зі складністю виявлення шкідливих атак виникає вимога розпізнавання трафіку додатків.

Шкідливі програми зазвичай розміщуються на діючих станціях управління і хостах, що перевіряються. Змінам піддається тільки зміст керуючих повідомлень. Щоб виявити спотворення інформації такого типу, повідомлення повинен перевірити зовнішній елемент, вільний від атаки. Для цього потрібно проводити інтелектуальний аналіз і перевірку кожної команди, що зумовлює необхідність використання засобів розпізнавання додатків.

Багаторівневий мережевий захист ICS. Службові мережі електроенергетичних підприємств стикаються з великою кількістю потенційних кіберзагроз, які охоплюють кілька векторів атак, а кожна вразливість має власну стратегію захисту. Отже, мережа може бути реально захищена тільки за умови застосування безлічі засобів захисту на різних рівнях. Тільки таким способом можна захистити систему від кожного вектора атак і покрити всі вразливості, які з'являються в разі використання окремої захисної стратегії.

Застосування захисних засобів на різних рівнях називається глибоким захистом (Defense-In-Depth). Стратегія глибокого захисту спрямована не на побудову непроникної єдиної стіни, а на побудову різних рівнів захисту. Такі захисні засоби поєднують різні тактики для того, щоб виявити і заблокувати

атаку. У службових мережах підприємств електроенергетики такий підхід слід застосовувати на всіх рівнях і векторах потенційних атак.

Стратегія глибокого захисту в ICS системах на підприємствах електроенергетики. У мережах електроенергетики застосування стандартних міжмережевих екранів і антивірусного ПЗ є недостатнім для того, щоб забезпечити глибокий захист. Такий підхід націлено тільки на один вектор захисту, але він виявиться марним, якщо атакуючий проникне в мережу або скористається шкідливим ПЗ для відправки шкідливих команд. З цієї причини застосовується стратегія багаторівневого захисту за всіма векторами атак, особливо в критично важливій службовій мережі або мережі автоматизації.

У ICS мережі кожен рівень глибокого захисту має свої переваги і недоліки. Працюючи на кожному рівні, комбіноване рішення успішно забезпечує захист від таких атак:

віддалені атаки, які здійснюються з іншого місця, — захист забезпечується з використанням брандмауера і міжсайтового шифрування, що не дозволяє хакерам отримати доступ до внутрішніх мереж на логічному рівні;

атаки «зловмисник посередині» — для захисту застосовується міжсайтове шифрування, що запобігає пошкодженню або фальсифікації даних;

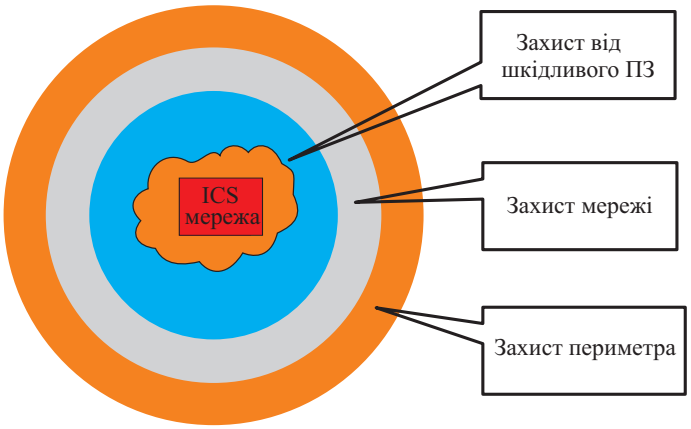
атаки на рівні управління мережі — захист за допомогою певної архітектури мережі, наприклад вибір інфраструктури з високим степенем захисту, такий як Carrier Ethernet або SONET , SDH замість MPLS або MPLS-TP;

атаки з маскуванням — усуваються за допомогою протоколів аутентифікації джерел, таких як IEEE802.1X, що перевіряють, чи не замінений певний хост іншою машиною, яка відправляє шкідливі дані;

перехоплення даних і шпигунство — захист з використанням мережевих технологій з жорстким визначенням шляху і універсальним адресним простором (таких як Carrier Ethernet);

атаки з RTU, керуючих станцій або HMI — усуваються з використанням розподілених мережевих екранів з розпізнаванням додатків; такі брандмауери можуть поглиблено перевіряти трафік SCADA щоб переконатися в тому, що команди стосуються додатка управління або автоматизації (крім перевірки, що пристрої є елементами мережі автоматизації).

Множинні рівні захисту. Належним чином розроблена ICS мережа оточена безліччю захисних шарів, де кожен шар націлений на захист від певного типу атаки (див. рисунок). Коли один рівень захищає від одного типу атаки, наступний рівень покриває його вразливості. ICS мережа, яка лежить в основі, може бути повністю захищена тільки в тому випадку, коли всі рівні працюють одночасно. В іншому випадку кожен окремий рівень може бути атакований і виведений з ладу відносно просто. ICS



мережі надзвичайно уразливі не тільки для традиційних загроз, які часто відбуваються в корпоративних мережах, але до атак, для яких не існує розповсюджених засобів захисту. До них відносяться атаки, націлені на рівень управління ICS. Незахищена фізична частина службової мережі підприємства електроенергетики (разом з існуючими необслуговуваними підстанціями) також може піддаватися атакам на вразливість мережевої технології, що лежить в основі мережі підприємства.

Всі ці атаки можуть бути знешкоджені і утримані на початкових векторах за допомогою стратегії глибокого захисту, який являє собою широкий набір засобів для захисту різних вразливостей мережі підприємства електроенергетики. До засобів глибокого захисту належать захисні засоби периметра разом з мережевим захистом і захистом від шкідливих програм.

Архітектура мережі відіграє критичну роль у рівні вразливості мережі. Такі технології, як Carrier Ethernet, які за визначенням є безпечнішими, можуть значно зменшити вразливість. І навпаки, такі технології, як MPLS, можуть посилити рівень вразливості мережі і потенційно дозволяють зловмисникам заволодіти мережею цілком, використовуючи простий пролом у фізичному захисті. Захист від шкідливих програм повинен входити до функцій постійно активного розподіленого брандмауера з розпізнаванням додатків, який здатний блокувати внутрішні атаки. Такий екран може захистити в ситуаціях, коли зловмисник не робить атаку ззовні, а проникає крізь периметр мережі.

Безпеку мережі підприємств електроенергетики необхідно серйозно розглядати на кожному етапі розробки архітектури мережі, а не тільки як завершальну процедуру її створення. Таке ретельне планування може значно поліпшити відмовостійкість мережі і скоротити витрати на забезпечення безпеки.

Висновки

Незважаючи на те, що інформаційні мережі підприємств електроенергетики завжди значно відрізнялися від традиційних корпоративних мереж, підходи до забезпечення їх кіберзахищеності в основному співпадають з класичними. Індустріальні мережі взагалі та мережі підприємств енергетики зокрема мають низку специфічних вразливостей, які властиві саме цим типам мереж. Як і для будь-яких мереж передачі даних, для мереж підприємств енергетики існують дві великі групи атак: атаки на рівні управління мережею та атаки на рівні передачі даних.

Щодо захисту від загроз кібербезпеці можна використовувати наступні механізми та заходи:

захист периметра;
захист мережі;
протидія атакам на рівні управління;
протидія атакам на рівні передачі даних;
внутрішній захист додатків (захист від шкідливого ПЗ);
багаторівневий мережевий захист ICS.

Лише комплексний підхід до забезпечення безпеки інформації, що циркулює у мережах передачі даних підприємств енергетики, спроможний забезпечити необхідний рівень захищеності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Шаньгін В.Ф.* Информационная безопасность и защита информации. М.: ДМК-Пресс, 2017, 702 с.
2. *Гуреев В.А., Сулейманова О.В.* Разработка архитектуры мини базы знаний противоаварийных тренировок // Энергетика и электрификация, 1987, № 1, с. 44—46.
3. *Гуреев В.А., Редковский Н.Н., Суманенков В.Г.* Информационная технология управления сложными распределенными техническими системами // Тез. докл. 1-й Украинской конф. «Информационные технологии и новейшее применение теории управления» (Автоматика-94) Ч. 1. Киев, 1994, с. 230—231.

Отримано 10.12.18

REFERENCES

1. Shangin, V.F. (2017), *Informatsionnaya bezopasnost i zaschita informatsii* [Information security and protection of information], DMK-Press, Moscow, Russia.
2. Gureev, V.A. and Suleymanova, O.V. (1987), “Development of the architecture of the mini knowledge base of emergency training”, *Energy and electrification*, no. 1, pp. 44-46.
3. Gureev, V.A., Redkovsky, N.N. and Sumanenkov, V.G. (1994), “Information technology management of complex distributed technical systems”, *Informatsionnyye tekhnologii i noveysheye primeneniye teorii upravleniya. Tez. dokl. 1-y Ukrainskoy konf.* [Information technology and the latest application of control theory (Automation-94). Conference proceeding of the 1 st Ukrainian Conf], Part 1, Kiev, pp. 230-231.

Received 10.12.18

М.Ю. Комаров

ОБЩИЕ ХАРАКТЕРИСТИКИ ПРЕДПРИЯТИЯ
ЭЛЕКТРОЭНЕРГЕТИКИ И ЭЛЕМЕНТЫ ИХ УЯЗВИМОСТИ
ТЕХНОЛОГИЧЕСКОГО ПРОИСХОЖДЕНИЯ

Приведены сведения о способах обеспечения функционирования сетей предприятий электроэнергетики. Описаны традиционные средства защиты информации. Представлены результаты обзора уязвимостей индустриальных сетей. Дан анализ подходов к защите от угроз кибербезопасности.

К л ю ч е в ы е с л о в а: кибербезопасность, предприятие электроэнергетики, уязвимость, защита периметра, защита сети, межсетевой экран.

M.Y. Komarov

INVESTIGATION OF GENERAL CHARACTERISTICS
OF UES OF UKRAINE AND ELEMENTS OF TECHNOLOGICAL
VULNERABILITY IN THERMS OF CYBERSECURITY

The information on ways to ensure functioning of the networks of electric power companies is given. The traditional means of information protection are described. The results of the review of the vulnerabilities of industrial networks are presented. The analysis of approaches to protection from threats to cybersecurity is given.

K e y w o r d s: cybersecurity, power company, vulnerability, perimeter protection, network protection, firewall.

КОМАРОВ Максим Юрійович, аспірант, наук. співроб. Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 2002 р. закінчив Національний технічний університет України «Київський політехнічний ін-т». Область наукових досліджень — кібербезпека об'єктів критичної інфраструктури, розробка методів та засобів забезпечення захисту інформації, що циркулює в інформаційно-телекомунікаційних системах підприємств енергетичної галузі.