УДК 004. 056
DOI: 10.31673/2409-7292.2021.021112

Довгуша І.М., Луценко І.М., Деркаченко Я.А.

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АСУ ТП ЕНЕРГЕТИЧНОЇ КОМПАНІЇ НА ОСНОВІ ПОБУДОВИ ЗАХИЩЕНИХ АНКЛАВІВ

В роботі приведено основні відомості про системи та мережі автоматизованих систем управління технологічними процесами та виявлено тенденції їх сучасного розвитку. Сформульовано нові задачі підвищення їх безпеки, як на етапі аналізу окремих функціональних вузлів, так і створення системи та мережі в цілому за технічними вимогами. Досліджено різні види побудов захищених анклавів та вироблено рекомендації з їх вибору в залежності від заданих технічних вимог до системи та з врахуванням критичності систем. Досліджено технологію захисту анклавів з урахуванням критичності активів.

Ключові слова: Кібербезпека, SCADA, енергетика, АСУ ТП, автоматизовані системи управління, анклави.

Вступ

В наші дні практично в будь-якому виробництві використовуються автоматизовані системи управління технологічними процесами (АСУ ТП). Однак автоматизація без виконання вимог інформаційної безпеки може бути критично небезпечною. Необхідно розуміти, чому захист АСУ ТП став особливо важливим, які загрози зараз найбільш реальні, і як захистити промислові інфраструктури від зловмисників. На сьогоднішній день підприємства все серйозніше підходять до інформаційної безпеки свого бізнесу. Однак для захисту складних промислових процесів на підприємствах критичної важливості необхідні спеціалізовані засоби та підходи.

Компанією Positive Technologies провели аналіз опитування, в якому вони оцінили готовність компаній до атак типу APT. При підготовці дослідження було зібрано інформацію про те, які кошти використовуються в різних організаціях для захисту від кібератак та проведено оцінку чи зможуть організації впоратися зі складними загрозами. Опитування в ряді галузевих спільнот, в які входять експерти з IT та ІБ з різних сфер вітчизняного бізнесу. На думку 60% респондентів, що представляють ПЕК і промисловість, ризик успішної кібератаки є критично небезпечним для їх компаній, але при цьому всього 11% учасників опитування впевнені, що компанія зможе протистояти APT. Більшість вважає, що цілями APT-угруповання при атаці на їх компанії будуть порушення технологічних процесів і виведення з ладу інфраструктури. Більше половини респондентів (55%) повідомили, що організації, в яких вони працюють, вже ставали жертвами кібератак. Кожен четвертий учасник зазначив, що одним з наслідків таких атак ставали простої інфраструктури (рис. 1).

Для того, щоб побудувати ефективну стратегію захисту, необхідно розуміти, як діють APT-угруповання і які мотиви лежать в основі їх поведінки. Далі буде розглянуто, як саме APT-угруповання атакують компанії з паливно-енергетичного комплексу: які техніки використовують, щоб проникнути в інфраструктуру, як діють всередині, а також на яких етапах можна виявити атаку.

В цілому атаки розвиваються за одним сценарієм і схожі між собою. Але у кожного злочинного угруповання формується власний шаблон поведінки. Він залежить від складу учасників, їх навичок, попереднього досвіду, наявності доступу до конкретних інструментів. У міру розвитку угруповання удосконалює свої методи, відбираючи найбільш підходящі і відмовляючись від безперспективних стратегій.

Поведінка APT-угруповань описано відповідно до матриць MITRE ATT&CK. В кінці розділу буде показано теплові карти (heat maps), які засновані на матриці MITRE ATT&CK, де відображені найбільш часто використовувані техніки атак на паливно-енергетичні компанії.

Дані для аналізу отримані в ході розслідувань кіберінцідентов і робіт по ретроспективному аналізу подій безпеки в інфраструктурі різних компаній, а також в ході постійного відстеження активності діючих сьогодні APT-угруповань експертами PT Expert

Security Center. Додатково використовувалася інформація з загальнодоступних звітів про діяльність APT-угруповань, підготовлених провідними компаніями в області ІБ.

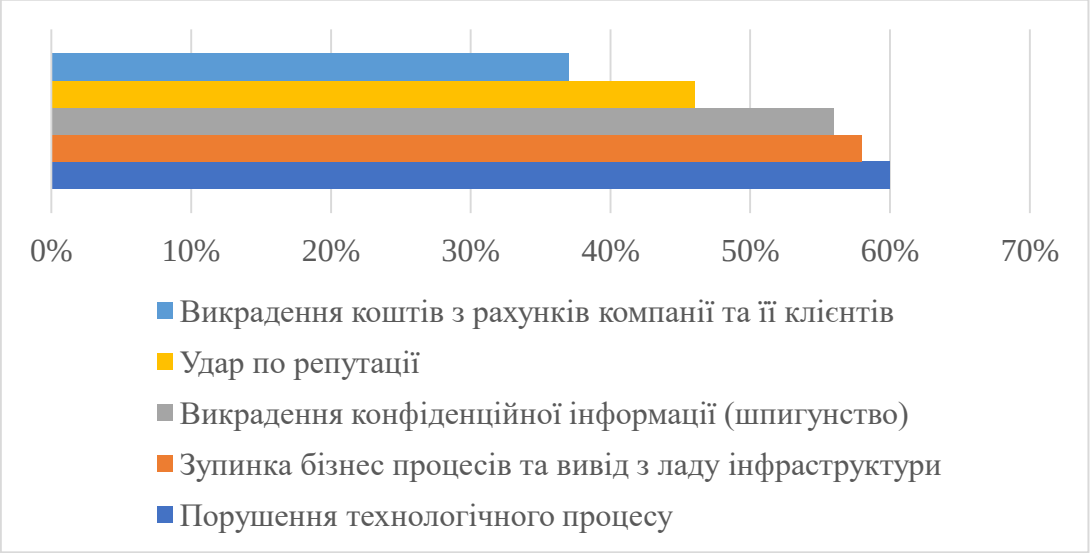

Рис. 1. Основні цілі, які сталять хакери при атаках на енергетичні компанії

Технологія забезпечення кібербезпеки АСУ ТП енергетичної компанії на основі побудови захищених анклавів

Раніше поняття про кібербезпеку зосереджувались на поділі пристроїв, портів, служб і навіть користувачів на функціональні групи. Логіка проста: при використання такого підходу поверхня будь-якої атаки зводиться до мінімуму. Сама функціональна група може бути захищена за допомогою різноманітних програмних та апаратних продуктів, перетворюючи групу в захищений анклав. Потрапити за межі периметру анклаву буде набагато складніше, оскільки ізоляція його служб стримуватиме спроби сканування та отримання інформації про мережеві пристрої.

Але на жаль, при створенні анклавів компанії, як правило, визначають занадто великі периметри, розділяючи промислову мережу на лише два-три анклави: система управління, ділова локальна мережа, а в деяких випадках і наглядова демілітаризована зона між ними. У деяких випадках, наприклад, на ядерних установках, застосовується п'ятирівнева анклавна система. Анклави можна - і потрібно розподіляти на менші одиниці. Однак для цього потрібно визначити самі функціональні групи. Формування анклаву повинно починатись з групування мереж, активів, операцій, які вони виконують, і навіть користувачів, які несуть відповідальність за ці операції. Потім ці групи вивчаються та виявляються спільні функції між системами. Результатом цих досліджень стане анклав, який містить лише ті системи, які необхідні для виконання певної функції на підприємстві.

Після визначення меж анклаву його необхідно захистити. В ідеалі – в кожному анклаві безпека має бути реалізована на якомога вищому рівні, але в реальності ціна на засоби інформаційної безпеки та сукупність інших факторів робить такий підхід неможливим. Тому також необхідно визначити анклави, які представляють найбільший ризик для безпеки та надійності, для того щоб реалізувати найкращий захист саме на периметрі критичних анклавів. Захист периметра може складатися з брандмауерів, мережевих IDS та IPS-пристроїв (NIDS та NIPS), списків контролю доступу маршрутизатора (ACL), програм для моніторингу та/або подібних продуктів безпеки - всі вони можуть і повинні бути налаштовані для ізоляції визначених меж анклаву.

Хоча захист периметра є важливим, внутрішня частина анклаву також повинна бути захищена для запобігання можливості внутрішніх атак або атак, які якимось чином обходять встановлені на периметрі захисні елементи (наприклад, введення зловмисного програмного забезпечення в систему управління, яка використовує фізичний пристрій, або шкідливе

програмне забезпечення, яке використовує поки невідому точку входу або вразливість нульового дня, яка не виявляється системами безпеки). Внутрішній захист складається в першу чергу з систем безпеки робочих станцій, таких як антивірус, система виявлення вторгнень IDS (HIDS) та застосування систем білих списків для програмного забезпечення. Як і у випадку із захистом периметру, внутрішній захист має бути налаштований згідно з дозволеними параметрами створених та задокументованих анклавів.

Мета статті – запропонувати варіант технології захисту автоматизованих систем управління технологічними процесами на основі захищених анклавів.

Побудова захищених анклавів. Ідентифікація функціональних груп

Першим кроком побудови захищеного анклаву є виявлення будь-яких функціональних можливостей групи, для того щоб визначити, з чого складається кожен анклав та межі його периметру. Під "функціональною групою" мається на увазі все, що безпосередньо бере участь у функціонування даного анклаву. Визначаючи функціональні групи, необхідно провести оцінку всіх активів (фізичні пристрої), систем (програмне забезпечення та додатки), користувачів, протоколів тощо. Необхідно відокремлювати один елемент від іншого де це можливо, наприклад протокол від активу. Якщо два елементи можна розділити і це не вплине на роботу основної функції будь-якого елемента, то вони належать до двох різних функціональних груп. Наприклад, якщо деякі системи HMI використовують протокол DNP3, необхідно створити список усіх пристроїв, які в даний час спілкуються через DNP3. Провести оцінку кожного пристрою щоб перевірити, чи потрібен DNP3 для його функціонування чи ні (він може підтримувати кілька протоколів і може без проблем використовувати інший протокол для виконання своїх функцій). Якщо даний протокол не потрібен для його нормального функціонування, то даний елемент слід виключити з функціональної групи та, якщо можливо, також необхідно вимкнути протокол, який не використовується на HMI. Результатом цих дій буде список усіх активів, які можуть нормально функціонувати лише при ввімкненому протоколі DNP3.

Подібним чином слід розглядати всі активи, які підключені один до одного в мережі, як фізично, так і логічно. Кожен представляє функціональну групу на основі мережі.

Функціональна група може базуватися майже на чому завгодно. Спільний функціонал групи, які слід враховувати при побудові анклавів у промислових мережах, включають контроль циклами, наглядові елементи управління, процеси управління, управління збереженням даних, промислові комунікації, віддалений доступ та менш чутливі групи, такі як групи користувачів та групи промислових протоколів.

Мережеві підключення. Функціональні групи, засновані на підключенні до мережі, легко зрозуміти, оскільки мережі за своєю природою з'єднують пристрої разом: різні пристрої з'єднані в мережі, чітко показують ті елементи, які належать до взаємопов'язаних групи та ті, що виключаються периметром. Мережі слід розглядати як фізично (які пристрої підключені до інших пристроїв через мережу кабелі або бездротові з'єднання) і логічно (які пристрої мають один і той же маршрутизатор, мережевий простір або підмережу).

Межі фізичної мережі легко визначити за допомогою карти мережі. В ідеалі всі мережі систем управління повинні мати жорсткі фізичні межі. Зв’язок між мережами має бути тільки через одну точку, яка захищена брандмауером або іншим пристроєм безпеки.

Межі логічної мережі визначаються маршрутизаторами, які в них використовуються а фізичні межі адресними просторами. Маршрутизатор забезпечує логічне розмежування між кожною мережею. Це робить можливим створення комунікацій між двома логічними підмережами, зв’язок між якими буде можливий лише через один маршрутизатор, що дає змогу використовувати ACL та інші захисні заходи.

Слід звернути увагу, що VLAN є типом логічної межі, але таким, що застосовується на другому рівні, а не третьому. В VLAN-х використовуються стандартизовані теги в заголовку пакета Ethernet. Однак мережі VLAN не рекомендуються використовувати при створенні анклавів, оскільки можливий сценарій при якому відбудеться зміна заголовку пакета для переходу в інший VLAN, минаючи маршрутизатор.

Цикли управління. Цикл управління складається з пристроїв, відповідальних за певний автоматизований процес. Відношення пристроїв до цієї функціональної групи відносно просте. У більшості випадків контур управління буде складатися з PLC та будь-яких відповідних входів та виходів, як показано на Рис. 2. Якщо IED це прямий вхід або вихід управління логікою, ці пристрої мають спільну функціональну групу з контролером.

В даному випадку функціональні групи на основі підключення до мережі не є дуже зручним підходом, оскільки цей метод не дозволить чітко поділити активи, побудова функціональних груп, на основі циклів управління дозволить більш точно визначити межі в даному випадку. Створених функціональних груп може буде багато, і кожна міститиме відносно невелику кількість пристроїв (конкретний PLC або RTU та колекція реле та IED).

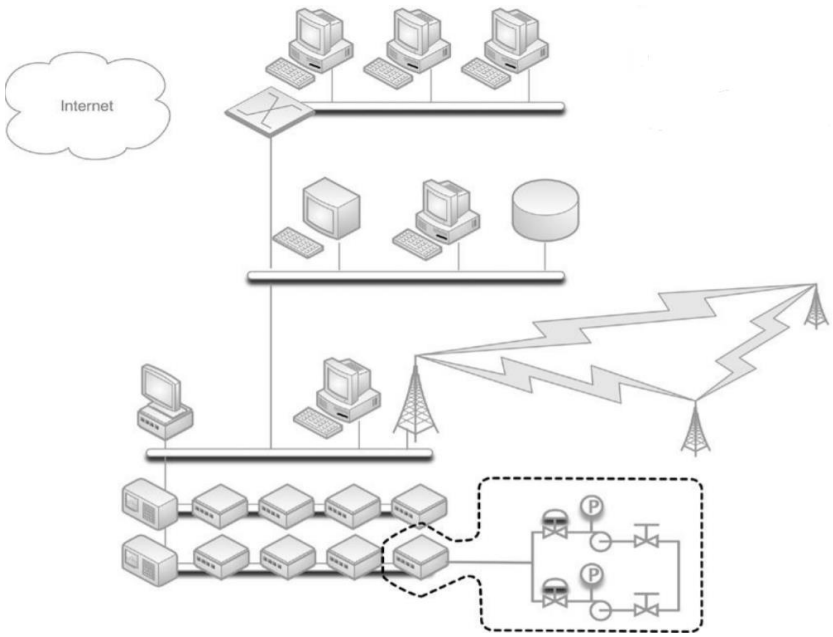

Рис. 2. Функціональна група, заснована на контурі управління

Операторський контроль. Кожен цикл управління також підключений до якогось операторського контролю - як правило HMI – який відповідає за конфігурацію, моніторинг та управління автоматизованим процесом. Оскільки HMI відповідає за PLC, ці два пристрої належать до загальної функціональної групи. Однак HMI безпосередньо не впливає на IED, які підключені до PLC, ці елементи не обов'язково входять до загальної функціональної групи, на відміну від HMI (вони належать до загальної функціональної групи, заснованої на деяких інших загальних критеріях, таких як використання протоколу).

До функціональної групи мають відноситись всі PLC, які контролюються за допомогою HMI, а також будь-який "головний" HMI або системи управління, яка керувати початковим HMI. Інші HMI не мають відноситись до даної групи, оскільки вони не несуть відповідальність за початковий. В ідеалі кожен HMI має представляти власну функціональну групу. Якщо використовується загальний головний контролер для управління декількома HMI, кожна окрема функціональна група HMI міститиме однаковий головний контролер, створюючи перекриття між кількома функціональними групами.

Процеси управління. Якщо головний контролер або головний термінал (MTU) використовується для управління декількома HMI, кожен з яких відповідає за певну частину більшого процесу управління, цей пристрій представляє корінь ще однієї функціональної групи - на цей раз тієї, що містить усі відповідні HMI.

Цей приклад також вводить поняття комунікації процесів та зберігання істрої. Якщо MTU взаємодіє з сервером ICCP, наприклад, для передачі великого електричного навантаження іншому електричному об'єкту, сервер ICCP також повинен бути включеними

до функціональної групи MTU. Аналогічним чином, якщо інформація з MTU подається в базу даних то ця система також повинна бути включена.

Контроль зберігання даних. Багато пристроїв промислової автоматизації та управління генерують дані, що відображають поточні конфігурації, стан процесу, тривоги та іншу інформацію. Ця інформація, як правило, збирається та зберігається в базі даних. Система зберігання інформації про стан промислових пристроїв може підключатися до багатьох, а потенційно всіх пристроїв по всій мережі систем управління, контролю мережі, а в деяких випадках і офісної мережі.

Торгівельні комунікації. Потреби комунікації між центрами управління достатньо критичні для того щоб виправдати використання спеціалізованого промислового протоколу, розробленого спеціально для цих цілей: Inter Control Center Communication Protocol або ICCP. Для комунікацій з використанням протоколу ICCP вимагається чітке визначення всіх з'єднань між клієнтами та серверами. Це перший приклад функціональної групи, яка виходить за межі периметру мережі компанії.

Одне, що слід пам’ятати при оцінці цієї функціональної групи, це те, що клієнтські пристрої, навіть якщо вони належать іншій компанії та розміщений в середовищі цієї компанії, повинні бути включені до функціональної групи, оскільки вони мають пряме відношення до будь-яких локальних серверів ICCP, які можуть ними використовуватись.

Віддалений доступ. ICCP - це лише один, спеціалізований метод віддаленого доступу до системи. Багато систем контролю та промислових пристроїв - включаючи HMI, PLC, RTU і навіть IED – мають можливість надання віддаленого доступу для технічної підтримки та діагностики. Цей доступ може надаватись через комутоване з'єднання або через маршрутизоване мережеве з'єднання. Віддаленим доступом до систем управління промисловими пристроями, якщо такий надається, слід керувати за допомогою спеціалізованої приватної віртуальної мережі (VPN) або серверів віддаленого доступу (RAS), і повинні дозволятись лише явно визначені з'єднання "точка-точка" від відомих об'єктів, по захищеним та зашифрованим каналам. Чітко визначені користувачі, пристрої, до яких вони отримують доступ, і будь-яка VPN або RAS система, яка використовується при підключенні, мають входити до єдиної функціональної групи віддаленого доступу.

Завдяки функціональній ізоляції віддалених з'єднань може бути забезпечений додатковий рівень безпеки.

Користувачі та ролі. Зрештою, до кожної системи отримує доступ або користувач, або інша система. До цього моменту обговорювалась побудова функціональних груп лише на основі систем: чітко визначаються пристрої, які можуть легітимно з’єднуватись з іншими пристроями. Для операцій людини з системами, наприклад, оператор, який звертається до HMI для проведення налаштувань, так само важливо визначити, до яких саме систем користувач повинен мати доступ. Для цього використовується система IAM, яка визначає користувачів та їх ролі. Найвідоміший приклад IAM - це Microsoft Active Directory, хоча існує багато інших комерційних систем IAM.

Складання ролей та надання доступів до пристроїв є дуже важливою, оскільки отримана функціональна група може використовуватися для моніторингу та виявлення несанкціонованого доступу до системи.

Протоколи. Протоколи, які використовуються в промисловій мережі мають бути чітко визначені для отримання можливості створення функціональних груп на основі протоколів. Наприклад, тільки пристрої які, належать до відповідної функціональної групи можуть використовувати протокол DNP3, а у випадку виявлення використання даного протоколу будь-яким іншим пристроєм за межами даної функціональної групи може розцінюватись як потенційне проникнення зловмисника до мережі. Саме тому пристрої, які використовують конкретні промислові протоколи, повинні бути ідентифіковані для створення ще однієї дуже важливої функціональної групи, як показано на Рис. 4.

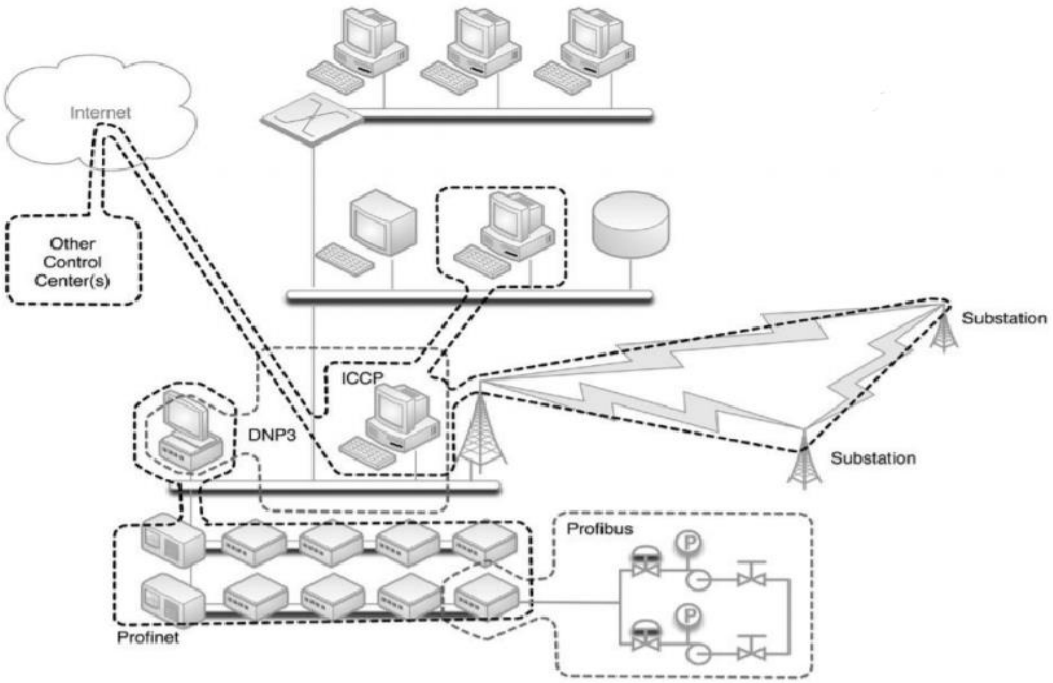

Рис. 4. Функціональна група на основі протоколів

Рекомендації щодо налаштувань систем кібербезпеки в мережах автоматизованих систем управління технологічними процесами

Налаштування мережі. Жоден пристрій, який не належить до певного анклаву, не повинен бути безпосередньо підключеним до анклаву або до будь-якого іншого пристрою у цьому анклаві.

Однак у багатьох випадках будуть існувати пристрої, які мають доступ або підключені до анклаву, навіть якщо вони не належать до жодної з функціональних груп в межах цього анклаву. Наприклад, принтери або робочі станції, які не належать до анклаву можуть бути підключені до локального інтерфейсу комутатора, маршрутизатора, або бездротової точки доступу. Дана аберація може бути наслідком неправильного проектування мережі або неправильної адресації в мережі - незалежно від причини, ці недоліки слід усунути до моменту остаточного формування анклаву.

В деяких випадках може бути неможливо чітко визначити периметр зони анклаву. Наприклад, якщо всі корпоративні системи та системи моніторингу і контролю взаємопов'язані плоскою мережею (мережею, яка комутується суто на другому рівні, без мережевої маршрутизації чи іншого розділення пристроїв) або бездротової мережі, що робить неможливим провести ізоляцію одних груп від інших. У цих випадках може знадобитись повне переналаштування та реконфігурація мережі.

Анклави та конфігурації пристроїв безпеки. Брандмауери, IDS і IPS-системи, системи захисту інформації та управління подіями (SIEM), можуть використовуватись лише в тих випадках коли в організації визначені та впроваджені жорсткі політики безпеки, які мають зіставлятись з конфігураціями систем безпеки. Тому для кожного анклаву слід задокументувати як мінімум наступну інформацію:

- Пристрої, що належать до анклаву (IP-адреси всіх систем).
- Користувачі, які мають доступ до анклаву (облікові записи користувачів та їх унікальні ідентифікатори).
- Протоколи, порти та служби, які використовуються в анклаві.

За можливості необхідно створювати нові списки, які міститимуть, наприклад, список зовнішніх IP-адрес, що можуть підключатись до даного анклаву, та доповнювати та

розширювати вже існуючі. Однак, якщо в організації не використовується централізована система автентифікації, ведення використання таких списків може бути ускладненим.

Забезпечення безпеки периметру анклаву. Створення електронного периметра безпеки (ESP) навколо певного анклаву являється прямим захистом від несанкціонованого доступу до закритих систем, а також а також не дозволяє системам, які розташовані в межах закритого анклаву отримати доступ до зовнішнього середовища.

Висновки

В результаті досліджень запропоновано модель, яка орієнтована на створення захищеної мережі автоматизованих систем управління в енергетичних компаніях, з урахуванням найкращих світових практик та нормативно-правової бази в сфері захисту інформації та кібербезпеки. Модель відображає найкращі, на думку авторів, принципи та варіанти забезпечення кібербезпеки автоматизованих систем управління технологічними процесами енергетичної компанії від несанкціонованого доступу до інформації.

Дану модель можна масштабувати, оскільки побудова мережі відбувається на основі анклавів, які легко можуть бути розширені або створені. Завдяки ідентифікації та ізоляції функціональних груп можна підвищити загальний рівень безпеки в декілька разів, не впливаючи на бізнес-процеси та роботу мережі в цілому. Ці анклави можуть і повинні бути захищені як на периметрі так і всередині, використовуючи різноманітні інструменти, зокрема такі як мережеві та хостові брандмауери, мережеві та хостові системи виявлення та запобігання вторгненню (IDS/IPS), моніторинг додатків в анклаві та антивірус або білий список додатків (AWL).

На додаток до прямих переваг, які надає кожен з наведених пристроїв безпеки, вони також можуть бути корисні при формуванні звітів та попереджень для аналітиків інформаційної безпеки. Інформація, зібрана з цих пристроїв може бути використана для ідентифікації та встановлення базової поведінки, а потім і для виявлення винятків та аномалій в будь-якому анклаві.

Перелік посилань

1. Kim Zetter. Countdown to Zero Day. Stuxnet and the Launch of the World`s First Digital Weapon - Published in the United States by Crown Publishers, an imprint of the Crown Publishing Group, a division of Random House LLC, a Penguin Random House Company, New York. – 2016. – 319p.
2. Gabrielle Desarnaud. Cyber Attacks and Energy Infrastractures. Anticipating Risks - Etudes de l'Ifri – 2017.-60p.
3. Eric D. Knapp Industrial Network Security - 225 Wyman Street, Waltham, MA 02451, USA – 2015.- 360p.
4. APT-атаки на топливно-энергетический комплекс: обзор тактик и техник [Электронный ресурс] – Режим доступа: World Wide Web. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-energy-2019/
5. Почему защита АСУ ТП сегодня стала критически важной? [Электронный ресурс] – Режим доступа: World Wide Web. – URL: https://www.securitylab.ru/analytics/484730.php
6. Безопасность от кибератак и аварий в АСУ ТП [Электронный ресурс] – Режим доступа: World Wide Web. – URL: https://automation-system.ru/main/11-asutp/asu-tp/468-security-asutp.html
7. NERC Critical Infrastructure Protection (CIP), NERC CIP [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.nerc.com/pa/Stand/Pages/CIPStandards. aspx
8. NIST SP 800-82 [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://csrc.nist.gov/publications/detail/sp/800-82/archive/2011-06-09#:~:text=NIST%20Special%20Publication%20(SP)%20800,control%20system%20configurations%20such%20as
9. Nuclear Regulatory Commission Regulation 5.71 [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.nrc.gov/docs/ML0903/ML090340159.pdf
10. Довгуша І.М., Кітура О.В. Безпека автоматизованих систем управління технологічними процесами / Довгуша І.М., Кітура О.В. // Актуальні проблеми кібербезпки: всеукраїнська наукова конференція, тези доп. – К., 2020. – С.91-92.

Надійшла: 13.04.2021 Рецензент: д.т.н., професор Вишнівський В.В.