РОЗДІЛ 6

ІНФОРМАЦІЙНА БЕЗПЕКА

УДК 004.056.53

О.В. Кручінін[1], М.С. Гаржа[1]
[1]Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ТА ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЇ В КАНАЛАХ ЗВ'ЯЗКУ СИСТЕМИ ДИСПЕТЧЕРСЬКОЇ ЦЕНТРАЛІЗАЦІЇ «КАСКАД»

Анотація. Обґрунтована важливість безпеки інформації в автоматизованих системах керування технологічними процесами (АСК ТП), як у рамках світового досвіду так і українського. Визначені загальні вимоги до системи кібербезпеки, розглянута АСК ТП залізної дороги, та визначені її вразливості.

***Ключові слова**: АСК ТП, система диспетчерської централізації, шифрування, вразливість, загроза, кібербезпека , web-сервер.*

Вступ. З розвитком технологій АСК ТП поступово перетворилися із закритих керуючих пристроїв на багаторівневі промислові мережі на базі стандартних мережевих протоколів, які мають безліч подібностей з корпоративними мережами, що активно використовуються. На жаль, це стосується й уразливостей, які тісно пов'язані із загрозами кібербезпеці. Ці мережі схильні до зараження шкідливими програмами, злому, виведення з ладу ПЗ та інших видів зовнішнього впливу. Це істотно впливає на виробничі процеси, і з кожним роком кількість подібних інцидентів збільшується.

Дії кіберпідрозділів силових структур ворожих держав спрямовані на порушення функціонування об'єктів інфраструктури, що може призвести до руйнувань та людських жертв. Даний вид атак є одним з найнебезпечніших при кібервійнах. Фахівці вважають, що найближчими роками він буде найпоширенішим.

Постановка задачі. Для досягнення поставленої мети в роботі сформовані і вирішені такі завдання:

- визначити актуальність необхідності захисту інформації АСК ТП;
- визначити особливості організації та структури АСК ТП Придніпровскої Укрзалізниці;
- визначити вразливості, які є характерними для каналів зв'язку системи диспетчерської централізації «КАСКАД»;
- визначити технічні обмеження для вирішення задач захисту інформації в каналах зв'язку.

Основний зміст роботи.

Промислова система керування (АСК ТП) – це загальний термін, що охоплює окремі типи систем контролю, включаючи системи супервізорного контролю та збору даних (SCADA-системи), розподілені системи керування (РСК) та інші конфігурації систем керування, такі як програмовані логічні контролери (ПЛК), які часто застосовуються в промислових секторах та критичних інфраструктурах.

Зазначеними обставинами АСК ТП якісно відрізняється від традиційних систем автоматичного керування (САК), які представляють технічні засоби для автоматизації дій людини на окремих ділянках технологічного процесу. АСК ТП складається з комбінації елементів контролю (наприклад, електричних, механічних, гідравлічних, пневматичних), що діють спільно для досягнення промислової мети (наприклад, виробництво, транспортування матерії чи енергії).

АСК ТП використовуються для управління географічно розподіленими активами, часто розподіленими на тисячі квадратних кілометрів, включаючи розподільчі системи, такі як розподіл води та системи збору стічних вод, сільсько-господарські системи зрошення, нафтогазові трубопроводи, електроенергетичні мережі та системи залізничного транспорту.

Можна припустити, що цілями таких атак будуть системи постачання держави, такі як електропостачання, водопостачання, системи залізничного транспорту.

За даними Kaspersky ICS CERT, у перші шість місяців 2020 року частка атакованих комп'ютерів зросла порівняно з попереднім півріччям із 38% до майже 40% у системах автоматизації будівель та з 36,3% до 37,8% в АСУ ТП нафтогазової галузі. До останніх відносять сервери управління та збору даних (SCADA), сервери зберігання даних, шлюзи даних, стаціонарні робочі станції інженерів та операторів, мобільні робочі станції інженерів та операторів, комп'ютери, що використовуються для адміністрування технологічних мереж, та комп'ютери, що використовуються для розробки ПЗ для систем промислової автоматизації.

В даній роботі розглядається АСК ТП Придніпровської залізної дороги. Дана АСК ТП є досить розгалуженою та покриває різні сфери життєдіяльності залізничного транспорту (рис. 1). Вона включає у себе збір інформації з різноманітних датчиків, розташованих по всій території залізничних шляхів, агрегація зібраної інформації на спеціальних серверах, що можуть забезпечити цілодобовий доступ до неї, передача забраних даних у різні точки залізниці з метою використання вже обробленої інформації на місцях.

Перший досвід експлуатації МСДЦ «КАСКАД» показав, що система в достатній мірі технологічна і повністю задовольняє потреби робітників господарства перевезень. Крім цього, за свідченнями персоналу дистанцій сигналізації та зв’язку, система надійна і практично не потребує обслуговування. У наш час системі «КАСКАД» немає альтернативи по впровадженню на Укрзалізниці.

Ключові фактори, що керують проектними рішеннями щодо властивостей керування, зв'язку, надійності та резервування АСК ТП. Оскільки ці фактори значно впливають на структуру АСК ТП, вони також допоможуть визначити вимоги до системи безпеки.

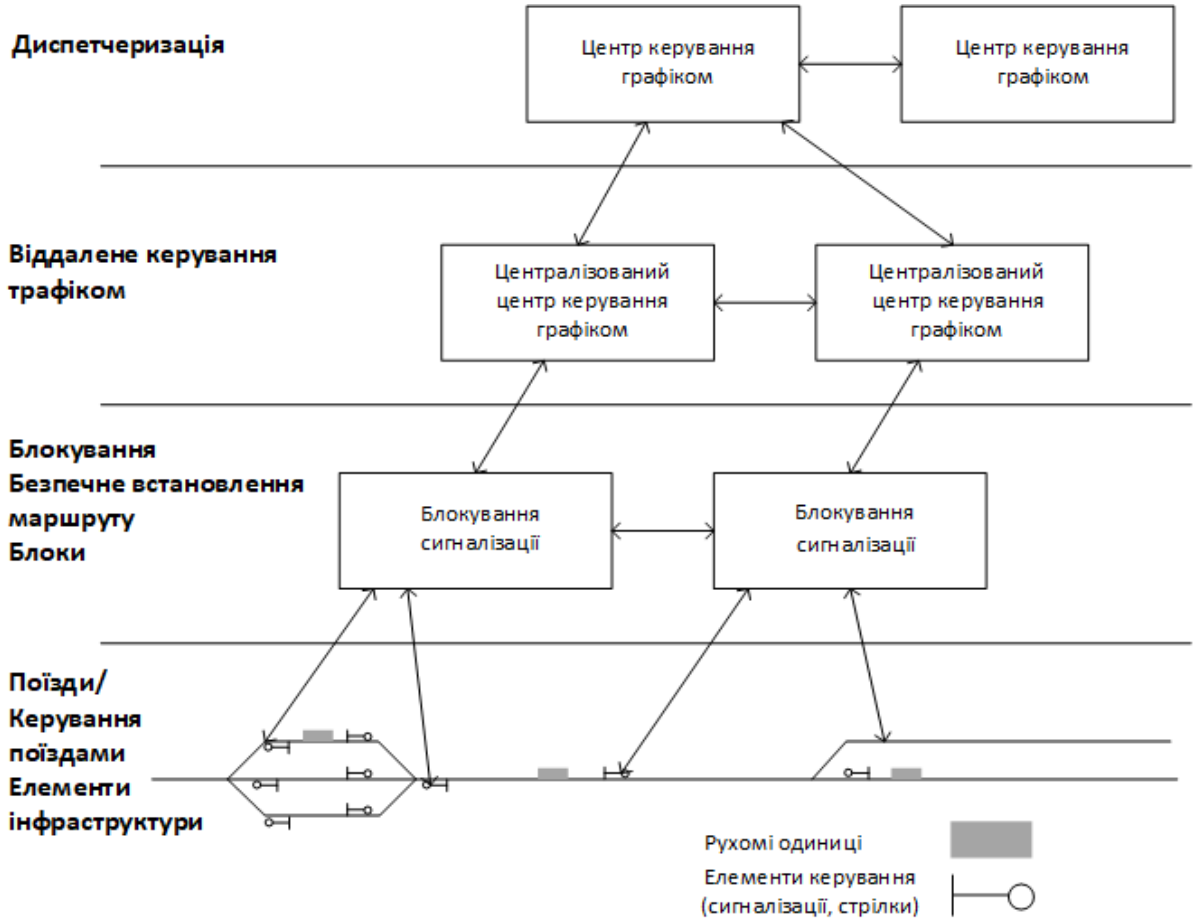

Рис. 1. Ієрархічна структура системи диспетчерського керування рухом поїздів

Часові вимоги до керування. Процеси АСК ТП мають широкий спектр вимог до часу, включаючи дуже високу швидкість, узгодженість, регулярність та синхронізацію.

Топологія локальної мережі кільцевого типу використовується в системі МСДЦ “КАСКАД”. Комплекси “ЛП КАСКАД”, які розташовані на постах ЕЦ залізничних станцій, є клієнтами локальної мережі кільцевого типу “LPnet”.На фізичному рівні локальної мережі “LPnet” використовуються дві пари магістрального кабелю (1,05 мм) при відстані між сусідніми клієнтами мережі до 40-45 км.

Для реальних умов експлуатації локальних мереж зв’язку наведений у прикладі термін затримки транспортування інформації необхідно помножити на коефіцієнт надійності (Кн=1,5-2,0). Згідно до вимог транспортування інформації, що прописана у нормативних документах залізної дороги, термін транспортування не повинен перевищувати 6 с.

Географічний розподіл. Системи мають різний ступінь розподілу, починаючи від невеликої системи до великих, розподілених систем (наприклад, нафтопроводів, електромереж). Більший розподіл зазвичай передбачає потребу в широкій області та мобільного зв'язку.

Дільниця диспетчерського управління, у залежності від географічного розміщення станцій та перегонів, кількості об’єктів управління, системи організації зв’язку, може складатися з одного або декількох сегментів.

Ієрархія. Супервізорне керування використовується для забезпечення центрального розташування, яке може об'єднувати дані з кількох місць, щоб підтримувати керуючі рішення на основі поточного стану системи.

Комплекс «ЦП КАСКАД» розташовується безпосередньо в центрі управління перевезеннями залізниці і складається з робочих станцій, автоматизованих робочих місць диспетчерського персоналу, об’єднаних локальною мережею, сервера, комунікаційного обладнання.

Керуюча складність. Складні системи (наприклад, управління рухом поїздів) вимагають від операторів людини забезпечення того, щоб всі контрольні дії відповідали більшим цілям системи.

Система потребує роботи кваліфікованого персоналу при управлінні перевезеннями, при чому, направленість їх дій повинна бути різною за для забезпечення максимально ефективного управління перевезеннями та безпеки руху поїздів. Таким чином потрібна злагоджена робота усіх робітників пункту, оперативна реакція на будь-які стандартні та нестандартні події, що можуть скластися у процесі контролю за перевезеннями.

Доступність. Потреби системи (тобто надійність) є важливим фак-тором проектування. Системи із сильними вимогами щодо доступності та часу роботи можуть вимагати додаткової резервної або альтернативної реалізації у всіх комунікаціях та керуванні.

Для забезпечення високої надійності та функціонування системи в різних режимах резервування в складі «ЛП КАСКАД» передбачено дві локальних міжмодульних мережі. Основний та резервний комплекти мають свою незалежну шину, джерело живлення, основну і резервну мережу. У свою чергу доступ до модулів (основного і резервного) може відбуватись з обох мереж. У разі пошкодження однієї з мереж або модуля, система продовжує функціонувати, при цьому діагностика стану пристроїв реєструє відповідну несправність.

Вплив збоїв. Невиконання керуючої функції може призвести до суттєво різного впливу для доменів. Системи, що мають більший вплив, часто потребують можливості продовжувати роботу за допомогою надмірного керування або здатності працювати в деградованому стані. Проектування має відповідати цим вимогам.

Для забезпечення роботи під час збоїв система має декілька різних варіантів розвитку подій. Перш за все слід відзначити, що система має резервні сервера для всіх своїх компонентів, а саме Web-сервер, сервер бази даних, резервні системи живлення та системи безперебійного живлення.

Безпека. Область вимог безпеки системи також є важливим чинником проектування. Системи повинні мати можливість виявляти небезпечні умови та викликати дії, спрямовані на зменшення небезпечних умов до безпечних.

Вимоги до безпеки інформації в системі диспетчерської централізації та в системах такого типу в цілому, ставляться до властивостей інформації, які стосуються її доступності та частково цілісності. Усі вимоги, що ставляться до таких систем в Україні, стосуються забезпечення безпеки руху поїздів, створення та використання систем, які б могли забезпечувати ці вимоги є найголовнішим пріоритетом.

Таким чином, проаналізувавши усе згадане вище, можна зробити висновок, що системи такого типу в Україні створюються та використовуються з урахуванням норм безпеки пересування поїздів, але ніяким чином не йде мова про забезпечення безпеки інформації, що передається в системах диспетчерської централізації.

Модулі системи «КАСКАД» поділяються на 3 категорії: модулі взаємодії з пристроями СЦБ, загальносистемні модулі, модулі живлення та електронного крейту. Кожен з модулів першої категорії взаємодіє з мікропроцесорним контролером через міжмодульну послідовну локальну мережу. Локальна міжмодульна мережа забезпечує зв'язок між модулями взаємодії з пристроями СЦБ та модулем контролера міжмодульної мережі, який у свою чергу через системну шину (ISA96) взаємодіє з мікропроцесорним контролером.

Як провідний процесорний модуль у складі системи використовується модуль контролера «КАСКАД-МП.2616». Він забезпечує функції взаємодії з модулями комплексу, підтримує протоколи мереж зв'язку лінійних пунктів, забезпечує синхронізацію процесів з сусіднім каналом системи, перевіряє достовірність інформації в каналах обміну, підтримує протоколи локальної міжмодульної мережі, протоколи інформаційного обміну по послідовних портах та обміну з пристроями на перегоні (контроль перегріву букс, диспетчерський контроль та інше). Крім цього, модуль контролера забезпечує внутрішню діагностику та резервування.

Модуль контролера побудовано на процесорі ZFx86, що має тактову частоту 66 мГц. Пам'ять модуля складається з SDRAM на 16 Мбайт, Flash EPROM – 0,512Мбайт. Модуль комплектується твердотільним диском (DiskOnChip) об'ємом від 2 до 64Мбайт.

Таким чином, проаналізувавши особливості структури АСК ТП Придніпровської залізниці, можна побачити, що система має канали зв'язку великої протяжності, і зважаючи на те, що ці канали передачі не захищені і є критичними з точки зору впливу на них, можна зробити висновок, що канали передачі схильні до типових атак, таких як прослуховування, підміна, дублювання даних.

Основним методом вирішення подібних вразливостей є використання криптографічного захисту інформації при передачі незахищеними каналами зв'язку. Зважаючи на технічні характеристики модуля системи, можна побачити, що обчислювальна можливість окремих модулів системи(модулів лінійних пунктів) є досить обмеженою. Таким чином, запропоновані рішення

мають відповідати можливостям обладнання, що встановлене в системі диспетчерської централізації.

Проаналізувавши особливості системи, її особливості щодо обчислювальних можливостей, вимоги для реалізації різних криптографічних алгоритмів, можна припустити, що вибір буде зроблений на користь шифру «Калина». Як такого, що може забезпечити достатній рівень захисту інформації, що передається, та такий, що має вимоги до системного обладнання порівняні з тими, якими обладнана система диспетчерської централізації, що розглядається.

Реалізація даного алгоритму шифрування в каналах передачі інформації зможе не тільки забезпечити необхідний рівень безпеки інформації, але й дає можливість реалізації без необхідності зміни існуючого обладнання, що істотно зменшить матеріальні затрати та час на упровадження такого алгоритму шифрування

Наукова новизна полягає в аналізі структури АСК ТП Придніпровської залізниці та аналізі актуальних вразливостей що стосується конфіденційності при передачі та впровадження запропонованого рішення в існуючу систему з недоліками, що були розглянуті.

Висновки. В результаті роботи був проведений аналіз необхідності захисту інформації АСК ТП. Була розглянута АСК ТП Придніпровської залізниці, що відповідає за керування залізничним транспортом. Особлива увага приділена вразливостям, що виникають в каналах зв'язку АСК ТП. Таким чином є необхідність впровадження криптографічних методів захисту, але з урахуванням технічних характеристик встановленого обладнання.

ПЕРЕЛІК ПОСИЛАНЬ

1. NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security – Mineola, 200 – 171 с.

2. Мікропроцесорна диспетчерська централізація "КАСКАД" /М.І. Данько, В.І.Мойсеєнко, В.З. Рахматов, В.І. Троценко, М.М. Чепцов: Навч. посібник. – Харків, 2005. – 176 с. Neil Rosenberg Designing 3D Printers: Essential Knowledge / 3D Hubs – Amsterdam, 2020 – 197 с.

3. Диспетчерське керування рухом поїздів на швидкісних та високошвидкісних магістралях: Навч. посібник /С. В. Панченко, Т. В. Бутько, А. В. Прохорченко та ін. - Харків: УкрДУЗТ, 2019. – 153 с.,

4. ЕФЕКТИВНА РЕАЛІЗАЦІЯ АЛГОРИТМУ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУВАННЯ ДСТУ 7624:2014 («КАЛИНА») ДЛЯ 8/16/32-БІТОВИХ ВБУДОВАНИХ СИСТЕМ: Стаття /Я.Р. Совин, В.І. Отенко, Є.Ф. Штефанюк – 16 с.

5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К.: Мінекономрозвитку України, 2015.

6. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України / [Р. Олійников, І. Горбенко, О. Казимиров та ін.] // Захист інформації. – 2015. – № 2(17). – С. 142-157.