ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ОБМІНУ ТЕХНОЛОГІЧНИМИ ДАНИМИ МІЖ KNX-ПРИСТРОЯМИ»

Виконала студентка 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Семенова І.Д.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2020 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Семеновій Інні Дмитрівні
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія захисту обміну технологічними даними між KNX -пристроями»

керівник магістерської роботи Гайдур Галина Іванівна, проф..
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «13» жовтня 2020 року № 230.

2. Строк подання студентом магістерської роботи 15.12.2020 р.

3. Вихідні дані до магістерської роботи
Система автоматизації KNX;
комплекси управління захистом обладнання KNX;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту обміну технологічними даними між KNX -пристроями
2. Склад та умови функціонування системи автоматизації KNX SCADA.
3. Методи та засоби управління захистом обміну технологічними даними між KNX -пристроями.
4. Варіант технології управління захистом обміну технологічними даними

між KNX -пристроями.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу складу та умов функціонування систем автоматизації KNX.

4. Результати аналізу методів та засобів захисту обміну технологічними даними між KNX -пристроями.

5. Призначення, можливості та функції платформи ETS5.

6. Архітектура та компоненти платформи ETS5.

7. Додатки протоколу KNX.

8. Варіант технології управління захистом обміну технологічними даними між KNX -пристроями

9. Рекомендації щодо застосування технології управління захистом обміну технологічними даними між KNX -пристроями.

10. Висновки за результатами роботи.

6. Дата видачі завдання 01.10.2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту обміну технологічними даними між KNX -пристроями.	09.10.2020 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	30.10.2020 р.	
3.	Аналіз методів та засобів захисту систем KNX.	16.11.2020 р.	
4.	Розроблення варіанту технології управління захистом обміну технологічними даними між KNX -пристроями.	23.11.2020 р.	
5.	Розроблення рекомендацій щодо застосування технології управління захистом обміну технологічними даними між KNX -пристроями.	02.12.2020 р.	
6.	Оформлення результатів дослідження.	09.12.2020 р.	
7.	Підготовка доповіді до захисту.	15.12.2020 р.	

Студент Семенова І.Д.
(підпис) прізвище та ініціали

Керівник магістерської роботи Гайдур Г. І.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Семенової Інни Дмитрівна
на тему: «Технологія захисту обміну технологічними даними між knx-пристроями»

Актуальність:

Забезпечення безпеки технологічного середовища в умовах кібернетичних впливів відноситься до методології захисту підприємства під час організації автоматизованого виробництва. Кожен пристрій з віддаленим підключенням до мережі створює потенційну точку входу для загроз безпеки та некоректної роботи SCADA. Безпека систем автоматизації стає все більш необхідною послугою у зв'язку з широким використанням автоматизації процесів, що прямий результат переходу до інформаційної моделі суспільства. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи від новітніх загроз, визначено мета та завдання управління захистом кінцевих точок корпоративної інформаційної системи.
2. Було досліджено методи та засоби управління захистом обміну технологічними даними між KNX -пристроями.
3. Запропоновано варіант технології захисту обміну технологічними даними між KNX -пристроями та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У магістерській роботі бажано було б провести саме порівняльний аналіз рішень різних виробників.
2. Запропонований варіант технології управління захистом обміну технологічними даними між KNX -пристроями бажано було б детальніше показати на використаному прикладі підприємства.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку **відмінно**, а студент **Семенова І. Д.** – присвоєння кваліфікації 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Якість роботи	
Виконано на замовлення підприємства	√
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує
(_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Семенова І. Д. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія захисту обміну технологічними даними між knx-пристроями».

Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Семенова І. Д.. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Черниш О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерськоїї роботи

Студентка ***Семенова І.Д.*** обрала тему роботи, метою якої було дослідити зміст технології захисту обміну технологічними даними між knx-пристроями та розробити варіант технології управління їх захистом на підприємстві. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Семенова І. Д показала відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студентка Семенової Інни Дмитрівни на оцінку **«відмінно»** та присвоїти їй кваліфікацію 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Керівник магістерської роботи _____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Семенова І.Д.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2021 року

РЕФЕРАТ

Текстова частина магістерської роботи: 72 сторінки, 32 рисунків, 15 джерел.

Об'єкт дослідження – процес забезпечення захисту обміну технологічними даними між knx-пристроями.

Предмет дослідження – технологія організації захисту обміну технологічними даними між knx-пристроями.

Мета роботи – розробити варіант управління захистом обміну технологічними даними між knx-пристроями та рекомендації щодо застосування технології захисту на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом обміну технологічними даними між knx-пристроями.

В роботі зроблено аналіз проблеми забезпечення кібербезпеки обміну технологічними даними між knx-пристроями та визначено мета та завдання організації захисту обміну технологічними даними між knx-пристроями. Проведено аналіз існуючих технологій управління захистом обміну технологічними даними між knx-пристроями.

Досліджено методи та засоби управління захистом корпоративної мережі на базі протоколу KNX, ETS5/6, KNX Secure/ipSecure Визначено призначення, основні функції та склад платформи ETS5.

На основі досліджень проведених в роботі розроблено варіант технології управління захистом обміну технологічними даними між knx-пристроями та рекомендації щодо застосування технології управління захистом на підприємстві.

Галузь використання – кібербезпека систем автоматизації.

СИСТЕМА АВТОМАТИЗАЦІЇ, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ЗАХИСТОМ ТЕХНОЛОГІЧНИХ ДАНИХ KNX, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ЗАХИСТОМ KNX-SCADA, ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ ТЕХНОЛОГІЧНИМИ ДАНИМИ KNX.

ЗМІСТ

Стор.

ВСТУП

Актуальність дослідження. Забезпечення безпеки технологічного середовища в умовах кібернетичних впливів відноситься до методології захисту підприємства під час організації автоматизованого виробництва. Кожен пристрій з віддаленим підключенням до мережі створює потенційну точку входу для загроз безпеки та некоректної роботи SCADA.

Зазвичай безпека забезпечується системою, яка складається з програмного забезпечення безпеки, розташованого на центрально керованому і доступному сервері або шлюзі в мережі, але, у випадку організації автоматизованого робочого процесу виробництва обладнанням на основі протоколу KNXб дане рішення не актуально, оскільки центрального контролера просто не існує. Тому необхідно зупинитися на методах захисту безпосередньо керуючих та сенсорних пристроїв.

Безпека систем автоматизації стає все більш необхідною послугою у зв’язку з широким використанням автоматизації процесів, що прямий результат переходу до інформаційної моделі суспільства.

Це визначає актуальність дослідження щодо організації активного захисту технологічних даних систем KNX.

Об’єкт дослідження – процес забезпечення захисту обміну технологічними даними між knx-пристроями.

Предмет дослідження – технологія організації захисту обміну технологічними даними між knx-пристроями.

Мета роботи – розробити варіант управління захистом обміну технологічними даними між knx-пристроями та рекомендації щодо застосування технології захисту на підприємстві.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту технологічних даних

систем KNX;

встановити сутність завдань управління захистом технологічних даних систем KNX;

проаналізувати існуючі технології захисту технологічних даних систем KNX;

проаналізувати методи та засоби захисту технологічних даних систем KNX

проаналізувати основні функції та принципи реалізації захисту технологічних даних систем KNX.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом обміну технологічними даними між knx-пристроями.

Практичне значення одержаних результатів полягає в розробці варіанта технології захисту технологічних даних систем KNX., а також у розробці рекомендацій щодо застосування систем захисту технологічних даних систем KNX.

1. АНАЛІЗ ПРОБЛЕМИ ЗАББЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ KNX-МЕРЕЖ ТА SCADA СИСТЕМ НА ОСНОВІ KNX

Building Management Systems (BMS) - автоматизований комплекс управління всіма інженерними системами будівлі, що включає ряд архітектурних та інженерних рішень, набір апаратних і програмних засобів, що дозволяють мінімізувати витрати енергоресурсів, скоротити кількість персоналу, що управляє будівлею, збільшити термін служби устаткування, запобігти аварії, забезпечити оптимальне реагування на зміни, що протікають і можливість гнучкого внесення різних змін з мінімальними витратами, а також забезпечити найбільш комфортні та безпечні умови для людей.

На європейських ринках об'єкти нерухомості, оснащені універсальною системою управління, часто називають «інтелектуальними».[6] Говорячи про BMS мова їде про цілі, як правило, багатоповерхові будівлі - торгові центри, готелі, розважальні комплекси, багатоквартирні будинки.

Система автоматизації також допомагає заощадити фінансові ресурси власника і, глобально, ресурси планети.

- Впровадження в проект автоматизації більш сучасних джерел освітлення, з можливістю регулювання потужності світла в поєднанні з датчиками освітленості, дозволять автоматично змінювати рівень освітленості в приміщенні, в залежності від часу доби і природної освітленості;
- Використання датчиків присутності і руху забезпечить автоматичне вимикання джерел світла, через декілька хвилин після того, як люди залишать приміщення, що особливо актуально в прохідних приміщеннях, санвузлах, на сходах і в громадських будівлях;
- Цікаві можливості економії досягаються при автоматизації роботи різних кліматичних систем - якщо в приміщенні використовується кілька різних систем, досить задати необхідний температурний режим для окремих приміщень або

всього будинку цілком та автоматика сама вирішить за допомогою яких систем можна досягти заданих умов найбільш економічно. Додатково, це виключить можливі конфлікти між кількома системами, наприклад, між кондиціонерами і теплими підлогами, що значно подовжить термін служби обладнання і заощадить власникові гроші.

Якщо підвести підсумок під описаними шляхами економії електроенергії, то, на думку фахівців, можлива економія, за умови коректного проектування системи може скласти від 10 до 40 відсотків.

Часто, в сучасному будинку крім освітлення і кліматичного обладнання, використовуються складні інженерні системи: вентиляції, кондиціонування, котельне обладнання, обладнання для басейнів і саун та багато іншого. Використання систем домашньої автоматизації в симбіозі з такими системами дозволить продовжити термін їх служби за рахунок своєчасного інформування про можливі неполадки і систем звітності про роботу обладнання.[5]

Також подібний функціонал системі дозволяє будувати складні керуючі структурі алгоритмізації, відомі як SCADA, у загальному розумінні це наглядове керування та збір даних (Supervisory control and data acquisition – англ.) — це архітектура системи керування, що складається з комп’ютерів, мережевих засобів передачі даних та графічних інтерфейсів користувача для високорівневого нагляду за машинами та процесами. Він також охоплює датчики та інші пристрої, такі як програмовані логічні контролери, які взаємодіють з технологічним заводом або обладнанням. У випадку з побудови SCADA на основі технології KNX, можна повністю виключити атаки та збої у роботі, що притаманні класичнім комп’ютерам з їх ОС та мережевому обладнанню.

1.1. ПРИЗНАЧЕННЯ, СТУРКТУРА, ФУНКЦІЇ ТА УМОВИ ФУНКЦІОНУВАННЯ KNX СТРУКТУР

Чим більше систем, тим необхідніше використовувати систему автоматизації. Існує безліч виробників, вендорів та інтеграторів які працюють з різними системами і, безумовно, у кожної з них є свої переваги і недоліки. Розглянемо різні типи АСК СА.

Перелік систем за основними ознаками (Рис. 2.1):

- Провідні (дротові);
- Бездротові;
- Централізовані;
- Децентралізовані;
- З відкритим протоколом;
- Із закритим протоколом.

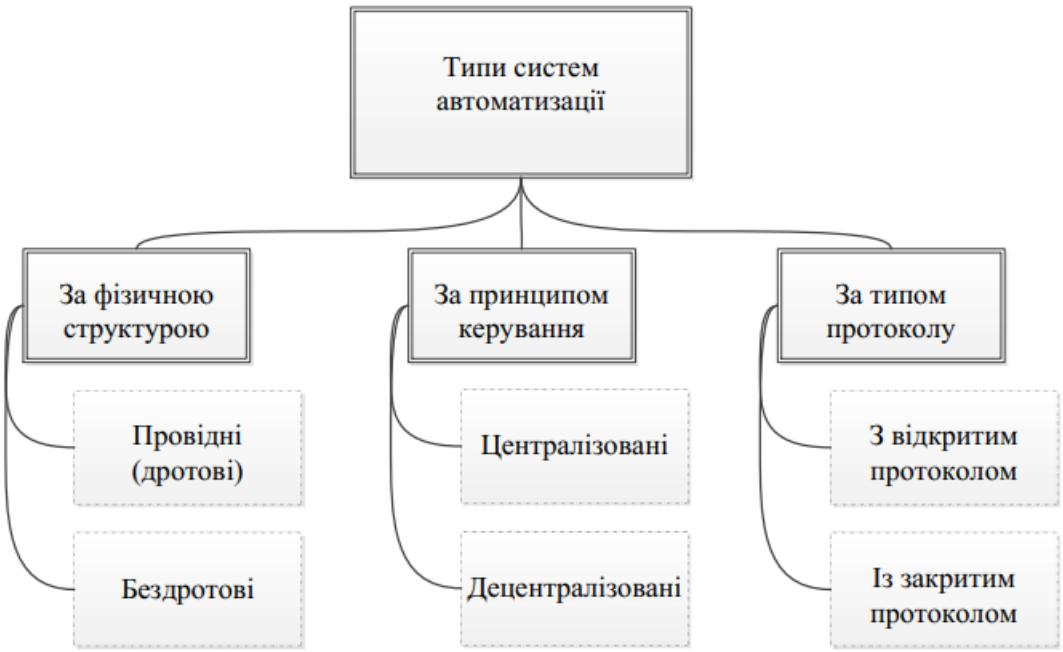

Рис. 1.1 – Типи систем автоматизації

Розглянемо провідні системи автоматизації. Суть провідної системи автоматизації полягає в тому, що всі керуючі пристрої - датчики, вимикачі, пристрої управління кліматом, різноманітні керуючі панелі, контролери обладнання та програмовані ліній виробництва - зв'язуються єдиною провідною інформаційною шиною, по якій йдуть сигнал та телеграми до виконавчих

пристроїв, що розташовані в щитовій кімнаті, що дозволяє набагато ефективніше побудувати систему фізичного захисту. Як середовище передачі інформації у провідній (шинній) системі використовуються спеціальні кабелі сертифіковані міжнародною асоціацією KNX відповідно до вимог обладнання, зазвичай це кабель EIB BUS 2x2x0.8. У провідної системи є свої переваги і недоліки, розглянемо їх.

Переваги:

- Надійність. Сигнал, що йде за спеціальними проводам - це надійно. Низька ймовірність перешкод і наведень та пошкодження середовища передач (кабелю), так як він фізично замурований у стіні (стелі, підлозі);
- Швидкість відгуку. Система автоматизації - це зручність та ефективність, тому якщо після натискання на клавішу запуску сценарію (комбінації дій які виконуються після натискання однієї кнопки та мають на меті створити той чи інший настрій, наприклад сценарій «ЗМІНА 1» - певне освітлення х урахуванням робочих місць, та часу доби, налаштований контроль якості повітря, певна температура, яка необхідна для даного виробничого процесу) у вас відбувається значна затримка, то це викликає дискомфорт і бажання натиснути на кнопку ще і ще, тим самим інформаційна шина перевантажується командами і перестає відповідати на запити. Якщо середовище передачі сигналу дротове, то швидкість відгуку висока, так як ця система (правильно спроектована) є перешкодозахищенною та надійною;
- Дизайн керуючих елементів. У таких систем в більшості випадків пропонується великий вибір керуючих елементів (розумних вимикачів), в порівнянні з бездротовою системою. Вони забезпечені великою кількістю функцій і можливостей;
- Різноманітність інтегрованих систем. У провідних системах легше зробити інтеграцію з кліматичними системами, аудіо- та відео-мультірумом, ніж в бездротових;

- Довгий термін служби. Система не має пристроїв на батарейках, які вимагали б регулярної заміни, що виключає можливість несвоєчасної відмові керування;
- Пожежна безпека. Всі вимикачі є слабкострумовими і електро- та пожежебезпечними, у разі необхідності можна підібрати обладнання з параметрами вологостійкості та широким температурним оптимумом.

Особливості та недоліки:

- Місця розташування керуючих панелей/датчиків необхідно вибирати заздалегідь та виводити туди кабель;
- Якісний монтаж. Необхідно користуватися послугами кваліфікованих електромонтажників і будівельників. У разі, якщо інформаційний провід буде перебито, система працювати не зможе і доведеться шукати і відновлювати з'єднання;
- У більшості випадків потрібно розробляти проект - на нього необхідно виділити час і ресурси;
- Особлива топологія прокладки кабелів. Для реалізації проекту необхідно прокладати кабелі від всіх керованих приладів до щита. У підсумку в районі щита утворюється велика кількість дротів яка може здивувати, однак після того як щит змонтовано - щитова набуває закінченого і охайного вигляду, звісно, в разі кваліфікованого монтажу;
- Встановити таку систему можна лише на початку ремонту, поки не зроблена основна електропроводка за класичною схемою. У готовому ремонті зробити провідну систему автоматизації не вийде.
- Потрібен щит великих розмірів (ширина близько 60 см і висота від 80см до 150 см, в залежності від розміру об'єкта, що автоматизується)

Розглянемо бездротові системи автоматизації. У цих системах, на відміну від дротових, сигнал від керуючих пристроїв до виконавчих «іде» по радіоканалу, а не по дротах. Це дозволяє скоротити кількість проводів, а також час на інсталяцію системи. Ці системи можна монтувати на об'єкти з готовим ремонтом з

класичною проводкою. Кожна бездротова панель керування є ще і радіопередавачем, який зв'язується з усіма іншими панелями.

Переваги:

- Можна встановлювати в простір з уже готовим ремонтом з класичною проводкою. Якщо використовувати повністю бездротову панель керування, яка працює на батарейках і посилає сигнал виконавчому пристрою (наприклад радіореле, розташоване близько світильника або світловий групи), то такий вимикач можна розташувати де завгодно. Вони можуть бути як накладного так і вбудованого монтажу;
- Зменшення кількості проводів, в порівнянні з провідний системою.
- Не потрібно розробляти проект. У більшості випадків проектування системи автоматизації не потрібно;
- Вартість. На ринку є багато систем з невисокою вартістю.

Особливості та недоліки;

- Радіоканал. Система, що працює по радіоканалу залежить від якості радіозв'язку. Перешкоди від СВЧ печей, будівельної техніки, DECT телефонів можуть мати негативний вплив на проходження сигналу. Знову ж, матеріал стін або розташована на стіні електрогірлянда можуть мати критичне значення для потужності сигналу, що робіть використання таких систем майже неможливим на виробництві;
- Батарейки. Якщо система працює на батарейках, то їх, очевидно, необхідно міняти, причому регулярно. Якщо цього не зробити, то в найвідповідальніший момент СА не спрацює;
- Необхідність нульового проводу. Є системи, в яких використовуються радіопередавачі, що живляться від мережі змінного струму. Для них необхідний нульовий провід. У класичній проводці до вимикача підходить одна живляча фаза і вона ж йде до групи світла. Тому краще відразу закласти додатковий нульовий провід в коробку під вимикач.

- Обмеженість функціоналу. Дуже складно створити на радіоканалі стабільну повнофункціональну систему, яка управляла б усім, а не тільки світлом і теплими підлогами.
- Безпека. Якщо у випадку з провідний системою ми можемо від’єднати всі зовнішні зв'язки - WiFi, інтернет, але система продовжить працювати, то в разі відсутності дротової інформаційної шини ми не зможемо зробити цього відключення. Глушіння сигналу, переклад датчиків в режим підвищеної енергоспоживання і т.п. може швидко вивести систему з ладу.
- Частоти роботи систем 433 Мгц і 868МГц. 433 Мгц використовують такі виробники як Jung, Gira. На цій же частоті працюють бездротові телефони, які можуть створювати перешкоди в роботі радіосистеми. Деякі виробники використовують більш перспективну частоту 868 МГц - Z- Wave, Vitrum, Zamel (Extra Free), iNels і деякі інші. Однак є складнощі в реєстрації цієї частоти на державному рівні - це заважає її широкому застосуванню і просуванню.

Розглянемо централізовані системи автоматизації. Суть централізованої СА полягає в тому, що програмується один центральний логічний модуль. Зазвичай це вільно програмований контролер з великою кількістю виходів. У контролер прошивається заздалегідь спеціально створена під об'єкт програма, на основі якої йде управління виконавчими пристроями та інженерними системами. Це дозволяє використовувати широкий вибір обладнання та складних сценаріїв. Централізовані системи можуть бути як дротовими (Ctestron, AMX, Evika), так і бездротовими (Z- wave)

Переваги:

- Можливість управління всіма інженерним системами в єдиному інтерфейсі;
- Можливість створювати складні сценарії, прив'язані до часу доби, стану, температурі і т.п.;
- Можливість підключення будь-якого обладнання;

Особливості:

- Людський фактор. Програміст, який написав програму є головною фігурою. У разі, якщо з програмістом контакт втрачено, то, в разі необхідності

перепрограмувати центральний контролер, доведеться заново писати всю програму. Програмування таких систем коштує досить дорого;

- Надійність. Якщо контролер виходить з ладу, то перестає функціонувати вся система повністю. Зазвичай контролери роблять дуже надійними, але прийнято вважати цю централізацію головним недоліком, хоча вихід з ладу блоку живлення розподіленої системи також виводить з ладу всю систему, але після заміни блоку живлення працездатність повністю відновлюється, програма не знищіться;
- Вартість. Великі можливості тягнуть за собою значну вартість.

Розглянемо децентралізовані системи автоматизації. У розподілених системах автоматизації кожне виконавчий пристрій несе в собі мікропроцесор з енергонезалежною пам'яттю. Цим пояснюється надійність таких систем. При виході з ладу одного пристрою вся система працює справно, крім приладів підключених до цього пристрою. Прикладом децентралізованої системи є системи автоматизації побудовані на основі протоколу KNX (найпопулярнішого в Європі).

Переваги:

- Надійність. Всі пристрої не залежать одне від одного і мають енергонезалежну пам'ять;
- Популярність. Стандарт KNX, наприклад, має понад 400 компаній-партнерів, які розробляють, виготовляють, реалізують, обслуговують та надають технічну підтримку обладнанню та вендорам/інсталяторам, що прямцюють з обладнанням тому не виникне труднощів з обслуговуванням або заміною обладнання;
- Можливість використовувати додатковий блок логіки, який буде відповідати за специфічні сценарії та функції;
- Великий вибір керуючих панелей як по дизайну так і по функціоналу.

Особливості:

- Велика кількість пристроїв в щиті.

Розглянемо системи автоматизації з відкритим протоколом. Протокол - це «мова» якою спілкуються всі пристрої в системі Якщо розглядати протокол KNX,

то він є відкритим. Багато виробників виготовляють пристрої, що працюють з цією мовою. Асоціація KNX перевіряє їх на сумісність і тестує. Логотип KNX EIB на пристрої гарантує підвищену якість.

Переваги:

- Великий вибір виробників. Це означає, що є великий вибір пристроїв за дизайном, ціною та характеристиками;
- Оновлення та конкуренція. Виробники конкурують в одному сегменті, що змушує їх розвиватися і придумувати нові пристрої.

Особливості:

- Вартість трохи вище ніж у систем із закритим протоколом за рахунок підвищеного контролю якості та просування єдиного стандарту;
- Не висока гнучкість при створенні нових пристроїв. Необхідність проходження стандартам накладає свій відбиток.

Системи автоматизації з закритим протоколом

Для того, щоб спростити процес програмування, зменшити витрати на виробництво устаткування деякі виробники випускають обладнання, яке працює на власному закритому протоколі. Інші компанії таке обладнання не випускають.

Переваги:

- Наявність цікавих рішень за нижчою ціною;
- Вартість в цілому нижче, ніж у систем з відкритим протоколом (хоча і не завжди);
- Більш швидке реагування на вимоги ринку.

Особливості:

- Залежність від одного виробника;
- Частіше усічені функції. [4]

1.1. ЗАГАЛЬНА КОНЦЕПЦІЯ ПОБУДОВИ KNX СТРУКТУР

Розглянемо, як в цілому будується система автоматизації:

1. Обирається одна (інколи 2) технології на базі яких буде будуватися система, це може бути шинна або мережева технологія. У сучасному світі, майже завжди, використовуються мережеві технології, як провідні так і безпровідні, але за для підвищення надійності роботи системи і подвійної відмовостікості додається нижній рівень комунікації між пристроями - шинний. В результаті чітко визначаються протоколи взаємодії між пристроями у системі.

2. Проектується система - формально або не формально перелічується всі системи, що потребують керування, отже й інтеграції в систему (рис. 1.2),

Рис. 1.2 – Приклад переліку підсистем СА

Зазвичай це освітлення, електроприводи штори, охоронна система (фізичний периметр, система протизатоплення, відеоспостереження, контроль доступу), HVAC. HVAC - Опалення, вентиляція та кондиціювання повітря, (скор. ОВК, або HVAC від англ. *Heating, Ventilation, & Air Conditioning*), це сукупність інженерних систем, метою яких є створення необхідних чи оптимальних умов мікроклімату, потрібних для перебування людей чи протікання технологічних процесів в приміщеннях будинків та споруд, засобах пересування тощо. ОВК часто розглядають у сукупності з системами холодопостачання, теплогазопостачання Оскільки всі системи ОВК працюють із одним повітряним середовищем, тісно взаємодіють одна з одною, вони можуть розглядатися як єдина інженерна система. Проект являє собою блок документів, що складається з креслень всіх підсистем з визначенням способу їх керування, кабельного журналу, логічної схеми взаємодії обладнання, однолінійної або багатолінійної

схеми підключення щита автоматики, компонування щита, специфікацій обладнання та кабельно-провідникової продукції. Рідше, в разі необхідності, може включати в себе фактичне документування прокладки кабельних трас, переносів і консервації кабелю.

3. Етап програмування.

На цьому етапі інженер-програміст знайомиться з документацією, відвідує об'єкт і спілкується з замовником з метою отримання кінцевого технічного завдання на роботу системи - особливості управління, дизайну, способів підключення. Після цього починаються роботи безпосередньо з програмування. Після їх завершення починається етап пуско–налагодження системи

4. Впровадження системи до вже існуючої мережі або побудова мережі з врахування запланованої СА.

Після впровадження системи в експлуатацію, протягом обумовленого часу (частіше один місяць) власник системи звертається з зауваженнями і побажаннями до системи. По закінченню часу наладки підписується акт передачі системи управління і всі наступні роботи вимагають окремого договору та узгодження.

1.2. АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ KNX ТА SCADA СИСТЕМ

Сучасні системи управління - це складні системи, що включають в свій склад велику кількість підсистем, які, в свою чергу, також є складними системами. Автоматизовані системи управління (АСУ) крім головної функції (управління об'єктом або процесом) виконують безліч допоміжних функцій, використовуючи для цього різні технічні засоби. Найчастіше результат виконання головної функції залежить від того, чи виконані (або наскільки якісно виконані)

додаткові функції. В таких умовах різко зростають вимоги до стійкості функціонування АСУ і безпеки оброблюваної в ний інформації. Під інформаційною безпекою (ІБ) розуміється стан захищеності інформації та захист інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести до нанесенням шкоди власникам або користувачам інформації і підтримуючої інфраструктури [7]. Критичними, як для АСУ так і для SCADA є загрози цілісності, конфіденційності, доступності.

Зловмисні дії або інформаційні загрози полягають в навмисному або випадковому порушенні властивостей конфіденційності, цілісності та доступності обчислювальної системи. Під загрозою інформаційної безпеки АСУ/SCADA розуміються дії (шляхи впливу) на систему (на активи і ресурси, пов'язані з системою), які прямо або побічно можуть завдати шкоди її безпеки. Прийнято виділяти три типи загроз: порушення конфіденційності, цілісності та доступності (відмова в обслуговуванні) оброблюваної, інформації Загрози можуть виникати в результаті як навмисних дій, так і випадково; існують класифікації загроз та уразливостей.

Зв'язок між видом небезпеки (вразливістю) і можливою загрозою полягає в місці, часі та типе атаки, що реалізує загрозу [9]. Мета системи захисту - протидія загрозам безпеки. "Безпечна АСУ" - це система, що володіє засобами захисту, успішно і ефективно протистоїть інформаційним загрозам [8; 9]. Однак для побудови економічно ефективної системи захисту необхідно вирішити завдання оптимального вибору набору засобів реалізації системи захисту від комплексу можливих загроз ІБ, які відповідають заданим обмеженням (вартість всієї системи, загальний рівень безпеки, швидкість роботи і т.п.). Необхідно розробити методики аналізу та оцінки ІБ АСУ/SCADA так, щоб було можливо отримати кількісну оцінку рівня захищеності з даного критерію і отримати можливість порівнювати різні комплекси засобів захисту. Крім того, сьогодні все рідше говорять про засоби забезпечення гарантованого захисту, а частіше - про засоби, що перешкоджають атаці, що уповільнюють процес її реалізації з метою

збільшення часу на прийняття відповідних дій або дій із запобігання загрозі безпеки.

1.2.1 Система аналізу і оцінки інформаційної безпеки

Відмінною особливістю SCADA спеціального призначення є те, що вони функціонують постійно. Тому, в разі порушення ІБ, постійно потрібно аналізувати стан ІБ і приймати рішення, спрямовані на недопущення або запобігання реалізації загроз. Для виконання функцій аналізу і оцінки ІБ АСУ повинна бути розроблена система аналізу і оцінки (САО) ІБ, яка, в свою чергу, може входити до складу системи захисту інформації (СЗІ). Крім того, з метою підвищення об'єктивності проведеного аналізу (наприклад, в тих випадках, коли СЗІ піддалася атакам або порушено її функціонування), така система може функціонувати окремо, незалежно від СЗІ. САО ІБ повинна реалізовувати методики аналізу та оцінки інформаційної безпеки.

Структурно до складу САО ІБ повинні входити модулі (рис. 1.3), що реалізують функції:

- Аналізу загроз;
- Аналізу уразливостей;
- Прийняття рішено про рівень ІБ;
- Управління процесом аналізу та оцінки ІБ;

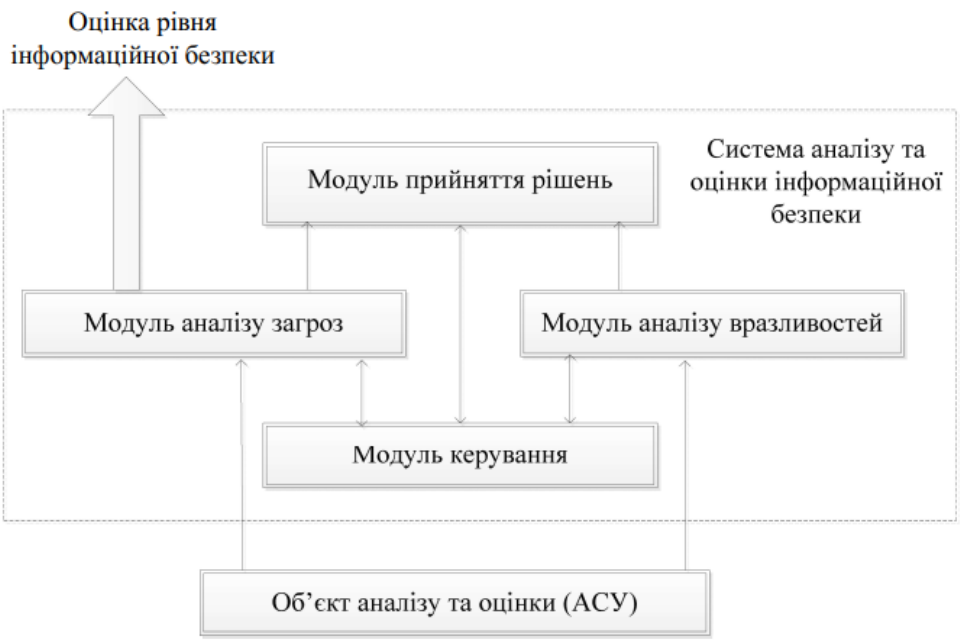

Рис. 1.3 – Система аналізу та оцінки ІБ

Під аналізом загроз розуміється всебічне вивчення можливих загроз ІБ і способів їх реалізації. Аналіз уразливостей - комплекс заходів щодо всебічного вивчення властивостей АСУ, здатних привести до порушення ІБ. Як правило, аналіз загроз і уразливостей проводиться для конкретної АСУ з урахуванням її застосування, умов експлуатації, з побудовою моделі ймовірного порушника, що враховує стратегію поведінки порушника, уточнюючої характер загроз, джерелом яких він може бути [10].

Функція прийняття рішення про рівень ІБ передбачає наявність процесу, що реалізує на основі методики оцінки ІБ оцінку загального рівня ІБ АСУ/SCADA. Вхідними параметрами для даної методики будуть результати аналізу загроз і уразливостей. Очевидно, що запропонована САО ІБ АСУ в процесі функціонування буде використовувати обчислювальні ресурси всієї системи. Тому до САО пред'являються вимоги, спрямовані на недопущення зниження загальної продуктивності АСУ:

- застосування переважно пасивних методів аналізу (наприклад, спостереження за мережевими інтерфейсами замість відправки запитів на отримання інформації про їх стан);
- вибір оптимальної частоти виконуваних перевірок;

- в разі виконання у вигляді окремої підсистеми, використання переважно власних обчислювальних ресурсів та інші.

1.2.2. Моделі аналізу та оцінки інформаційної безпеки

Розробка методики аналізу і оцінки ІБ є можливою тільки після побудови моделі АСУ в контексті ІБ. Розглянуті в літературі з даної тематики моделі не дозволяють адекватно і повно описати інформаційні процеси, що відбуваються в АСУ. Крім того, не існує єдиної моделі, комплексно охоплює три основних напрямки забезпечення безпеки, кожна з них описує один з аспектів захисту: конфіденційність, цілісність або доступність. З огляду на, це, оцінка кожного із зазначених аспектів можлива за кількома критеріями, а також те, що таку складну систему неможливо повно охарактеризувати з допомогою єдиного показника, оцінка ІБ в загальному випадку є завданням багатокритеріальної оцінки.

Існують два основні підходи до багатокритеріальної оцінки ефективності складних систем [12]. Перший так чи інакше пов'язаний зі зведенням безлічі приватних показників { *Wi* } до єдиного інтегральним показником *Wo*. Другий використовується при наявності значного числа приватних показників ефективності, приблизно однаково важливих, і передбачає використання методів теорії багатокритеріального вибору і прийняття рішень. Мета функціонування СЗІ - підтримання заданого рівня захищеності. Тому показники ефективності повинні характеризувати динамічні властивості СЗІ і дозволяти оцінювати її як характеристики адаптивної системи. Для отримання таких показників на основі аналізу існуючих формальних моделей безпеки [12] і стандартів інформаційної безпеки повинна бути розроблена адекватна модель АСУ з наявної в її складі СЗІ (в контексті інформаційної безпеки), що усуває виявлені недоліки в досліджених моделях і стандартах. Першочерговим завданням створення подібної моделі є адекватне формальне опис інформаційних процесів, що відбуваються в АСУ спеціального призначення.

Перевагою формального опису є відсутність протиріч в політиці безпеки і можливість теоретичного доказу безпеки системи при дотриманні всіх умов політики безпеки. [15]

KNX - це стандартизований протокол зв'язку для інтелектуальних будівель. KNX є спадкоємцем трьох попередніх стандартів: Європейського протоколу домашніх систем (EHS), BatiBUS та європейської інсталяційної шини (EIB або Instabus).

На відміну від стандартної електроустановки, між блоками управління та джерелом живлення немає жорсткого провідного з'єднання, наприклад, вимикач світла не підключений безпосередньо до відповідного світла. Натомість пристрої та електричні засоби підключаються через шину, яка працює на 29 вольт. Всі шинні пристрої можна запрограмувати за допомогою одного загального інструменту – ETS5 (середовище параметризації), таким чином KNX BUS дозволяє легке та дуже гнучке встановлення, без зміни електропроводки можна замінити усю систему.

В основному для системи KNX(рис. 1.4) потрібні такі компоненти:

- Блок живлення для потужності установки
- Датчики - кнопкові/сенсорні вимикачі та панелі керування, термостати, вимірювачі швидкості повітря, тощо, які генерують команди у вигляді телеграм
- Приводи (актуатори) - перемикачі реле для освітлення, жалюзі, тощо, які приймають телеграми і виконують певні дії
- Шина, яка з'єднує всі датчики та виконавчі пристрої

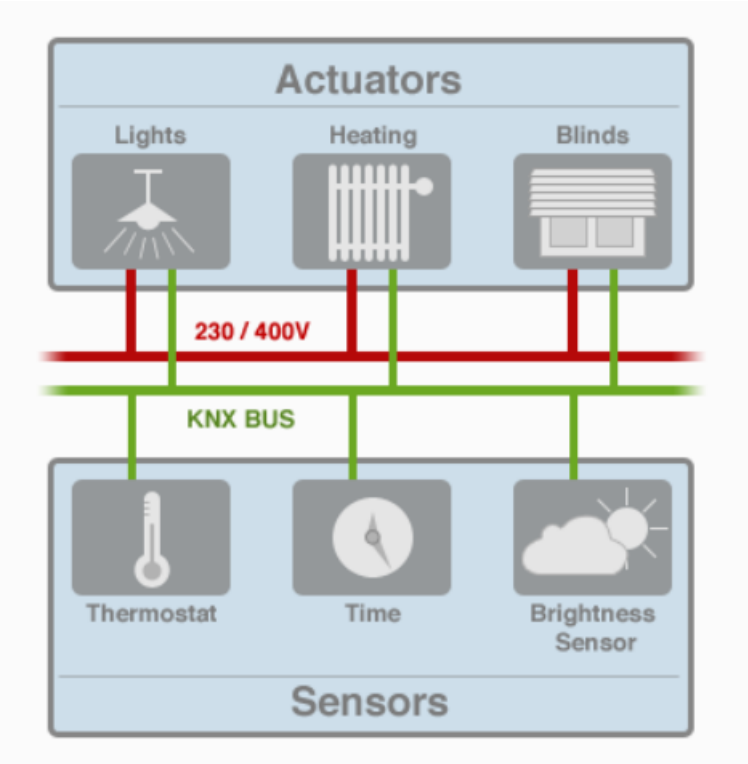

Рис. 1.4 - Приклад системи KNX

Найменшою сутністю в топології KNX(Рис. 1.5) є лінія. Лінія може містити максимум 64 пристрої. Цього достатньо для більшості невеликих проектів.

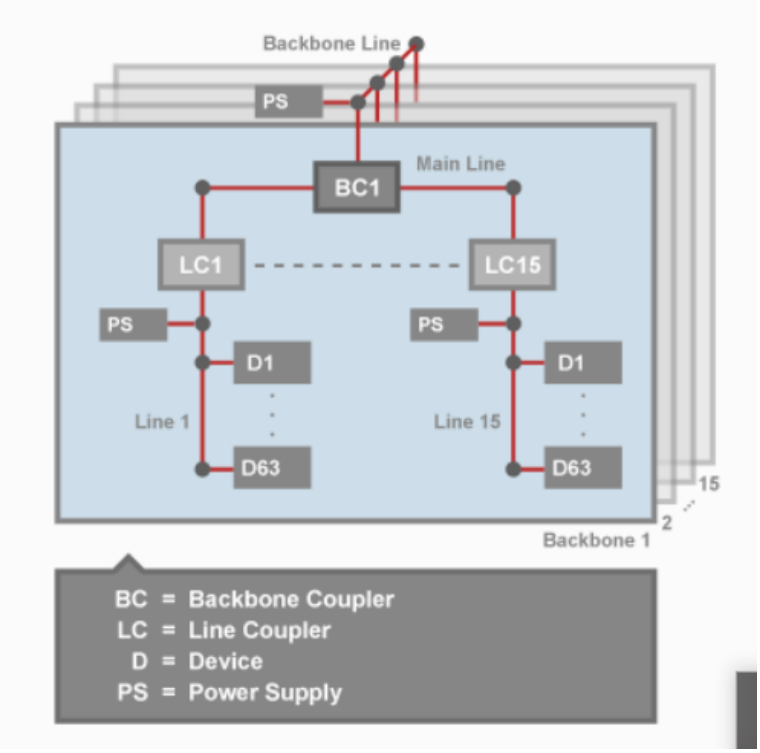

Рис. 1.5 - Приклад топології KNX

Для великих проектів до однієї області може бути об'єднано до 15 ліній - з'єднаних через основну лінію. Різні лінії можуть бути з'єднані з основною лінією за допомогою з'єднувача ліній(Line Coupler).

Крім того, також можна підключити до магістралі до 15 областей, де поодинокі ділянки з'єднані з магістральною лінією за допомогою з'єднувача магістрального з'єднувача (Backbone Coupler). Таким чином, одна повна топологія може містити порядку 65 тисяч пристроїв.

Кінцеві пристрої KNX можуть бути підключені будь-де в цій топології. До 255 кінцевих пристроїв KNX може бути адресовано в будь-якій підмережі. Кінцеві пристрої KNX можуть бути пронумеровані від 1 до 255. Але кінцеві пристрої KNX не можуть мати номер пристрою 0.

Кожен пристрій KNX (магістральний з'єднувач, з'єднувач ліній, кінцевий пристрій KNX і т.д) повинен мати індивідуальну адресу. Ця індивідуальна адреса є унікальною у всій топології. [11]

Інформація у середовищі передається у вигляді телеграм (рис. 1.6) – набору двійкових значень довжиною від 6 до 263 октетів, що містять у собі:

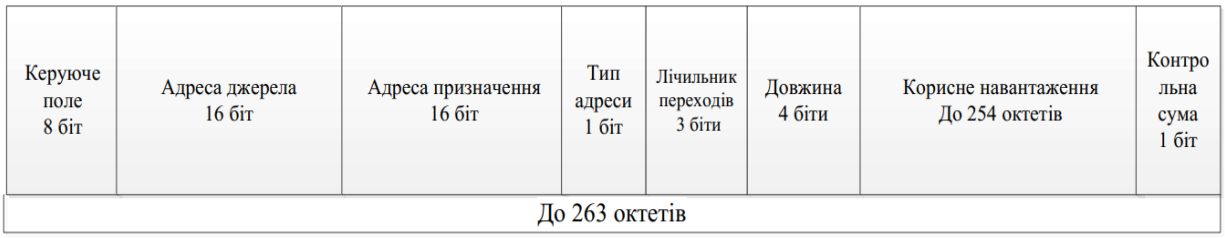

Рис. 1.6 – Структура телеграми KNX

- Поле керування (керуюче поле - The control field) - Має довжину 8 біт та включає в себе інформацію про тип телеграми, статус та пріоритет;
- Адреса джерела – поле, що містить фізичну (індивідуальну) адресу пристрою, що надсилає телеграму довжиною 16 біт;

- Адреса призначення - поле, що містить фізичну (індивідуальну) адресу пристрою, що має отримати телеграму, довжиною 16 біт;
- Тип адреси – довжина 1 біт;
- Лічильник переходів – довжина 3 біти – відображає кількість переходів телеграми між різними рівнями топології;
- Довжина – відображає довжину корисного навантаження та містить 4 біти;
- Корисне навантаження – містить у собі статус телеграми, ідентифікатор, безпосередньо інформацію, що передається та ідентифікатор сервісу
- Контрольна сума – відображає цілісність телеграми шляхом вирахування біту парності за допомогою логічної операції NOT XOR, довжина – 1 біт

Телеграма транслюється на усі пристрої та лише пристрій за зазначеною фізичною адресою реагує на телеграму. Службові телеграми можуть мати іншу структуру

Технологія KNX надає можливість на додачу до провідного середовища передачі інформації використовувати шлюзи для IP(Wi-Fi) та RF(Radio frequency). Тим самим збільшуючи гнучкість системи

Проблеми забезпечення безпеки, а, як наслідок, і уразливості подібних систем можна розділити на 2 категорії (рис. 1.7).

Рис. 1.7 – Типи уразливостей систем KNX

Перша – це проблеми пов’язані безпосередньо з технологією KNX, до них відносяться:

- Збій електропостачання – як наслідок , в разі відсутності електропостачання система не працює, або, в разі перевантаження потужності, знищується основній блок живлення системи, який не тільки забезпечує живлення система, але й генерує телеграми на фізичному рівні;
- Фізичний доступ зловмисника - як наслідок, система може біти перепрограмована і функціонувати не коректно, знищена на програмному рівні або може буті викрадено безпосередньо програму керування або зчитано телеграми, що передаються в мережі, оскільки вони не зашифровані. Більш того, при фізичному доступі можна не лише видалити програму, а й заблокувати можливість програмування пристроїв, що призведе до значних фінансових втрат.;
- Знищення кабельної структури – як наслідок, не функціонує частина системи можливе двома способами, перший – фізичне пошкодження сегменту

кабелю, другий подача високої напруги на кабель, оскільки перетин кабелю 2*2*2,8 мм, ізоляція просто розплавиться;

- Електромагнітні наведення – можуть спотворювати чи знищувати інформацію, що циркулює у системі
- Відсутність шифрування телеграм

Друга – це проблеми пов'язані з віддаленим доступом через мережу Internt, зв'язок забезпечується за допомогою шлюза взаємодії двох середовищ передачі даних. У цьому випадку інтегратор підключається до мережі VPN яка дозволяє звертатися до комутатора в локальній підмережі, де фізично знаходиться шлюз. У цьому випадку мова йде не про уразливості протоколу KNX, а про уразливості Ethernet. Найпростіший засіб захисту від уразливостей езернет у системах KNX, це їх незадіяність у системі.

1.3. МЕТА ТА ЗАВДАННЯ ЗАХИСТУ KNX ТА SCADA СИСТЕМ

У попередніх підрозділах ми визначали призначення подібних систем, що приводить нас до таких виводів, що SCADA побудовані на KNX провідним децентралізованим методом можна використовувати у широкому діапазоні випадків, від приватного мешкання до структур КВОІ, наприклад: заводів, електростанцій, лікарень.

Вищезазначене означає, що для непорушності критично важливих об'єктів інфраструктури необхідно забезпечити захист систем керування, а саме реалізувати стан захищеності інформації та, безпосередньо обладнання, при якому будуть зберігатися такі властивості, як конфіденційність, доступність, спостережність, своєчасність та автентичність, як циркулюючої інформації, так і дій усього персоналу, включаючи вищій ешелон керівництва. Наприклад, на сьогодні систему автоматизованого керування частково встановлено у Верховній раді України, що означає, що ми не можемо допустити ні витоку інформації на її викривлення ні знищення, також необхідно логування усіх дій та рішень.

У випадку реалізації загрози у приватному мешканні також можливі негативні наслідки, вид спотворення чи знищення важливої інформації, блокування обладнання, що вимагає повної заміни, чи методично порушення психологічної рівноваги власника, шляхом зовнішнього керування системою. У разі об’єктів КВОІ мова йде про більш серйозні наслідки на рівні міста, області, чи навіть держави. Наприклад зловмисник, отримавши фізичній доступ пошкодив лінії комунікації між обладнанням, у разі відсутності резервної кабельної системи, це приведе до повної зупинки керованого виробництва. У раз не захищених методів віддаленого доступу, зловмисник може перехопити керування системою і нанести суттєвих збитків, наприклад заблокувавши обладнання на фізичному рівні, чи коректуючи систему таким чином, що її діяльність буде призводити до зниження продуктивності працівників, порушення технологічних умов виробництва, чи, навіть, до виходу виробничого обладнання з ладу.

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ТЕХНОЛОГІЧНИХ ДАНИХ У KNX СИСТЕМАХ

У попередньому розділі були представлені характерні уразливості систем KNX, далі будуть розглянуті засоби та методи протидії їм

Збій електропостачання – для захисту в даному випадку доцільно використовувати додаткове незалежне джерело живлення (генератор, акумулятори, додатковій ввід живлення до будинку). Для захисту від перевантажень необхідно звертати увагу на побудові системі електрики в цілому – забезпечити селективність захисту, грозо захист, заземлення і т.д., за для швидкого відновлення роботи системі необхідно мати обладнання гарячої заміни, в даному випадку це резервній блок живлення необхідної потужності. У разі критичності безперебійної роботи необхідно провести інструктаж користувачів з заміни блоків живлення або використовувати декілька блоків на одній лінії (така практика офіційно не підтримується асоціацію, але працює на практиці).

Фізичний доступ зловмисника - найкращим засобом захисту від усіх загроз пов’язаних з фізичним засобом буде контроль доступу та організація захищеного периметру та демілітаризованої зони, але не практиці, у приватному будинку це дуже рідко реалізовано на високому рівні, як правило це токен чи пароль доступу для постановки/зняття з охорони, примітивні датчики відкриття вікон, розбиття скла та присутності. Нажаль усі цивільні системи охороні дозволяють скинути усі паролі фізичним замиканням необхідних контактів на платі і професійний зловмисник встигне це зробити до того, як система спрацює. Датчики відкриття також можна знешкодити за допомогою звичайних магнітів певним чином, а датчики присутності створивши певні перешкоди, але дане питання не відноситься до теми роботи. Тобто, зрозуміло, що неможливо виключити фізичній доступ, тому необхідно створювати систему припускаючи, що зловмисник легко може його отримати.

В першу чергу необхідно встановити ключ BCU (universal bus controller) – це універсальній шинний контролер, мікропроцесор, що реалізує функції пристрою. Після встановлення ключа без нього неможливо змінити прикладну програму пристрою, цей пароль не зберігається на жодному рівні ні пристрою, ні системи, на пристрої інтегратора з якого його було встановлено, у разі, якщо інтегратор забуває пароль, єдиний спосіб його «скинути» - повернення пристрою виробнику. За для того, щоб зловмисник не міг зчитати телеграми, і, як наслідок, саму програму їх необхідно зашифрувати. Знищення кабельної структури – ця проблема також відноситься до питання фізичного доступу, і єдиним способом захисту буде не допуск злочинця до системи, але для зменшення вірогідних збитків доцільно використовувати максимально розкинуту систему замість однієї суцільної шини та мати резервні лінії;

Електромагнітні наведення – в першу чергу необхідно використовувати екранований кабель, за можливістю, з сертифікацією асоціації, по друге необхідно дотримуватись правил прокладання слабострумних мереж, по трете, за можливістю, прокладати кабель в екранованих лотках;

Налаштування VPN, як правило, використовується або L2TP або PPTP підключення. Для забезпечення базового рівня безпеки необхідно встановити стійкі паролі, у випадку з L2TP окрім паролю, спільний ключ, не повідомляти їх нікому та увімкнути обов’язкове шифрування.

За для того, щоб зловмисник не міг зчитати телеграми, і, як наслідок, саму програму їх необхідно зашифрувати.

За замовчуванням система не має шифрування але його можна примусово додати використавши одну з технологій - KNX Secure чи KNX IP Secure – в розрізі шифрування різниця між ними полягає в тому, що KNX Secure шифрує лише частину телеграми з корисним навантаженням та чек сумою, а KNX IP Secure шифрує усю телеграму. В обох випадках використовується шифрування AES;

2.1. МОЖЛИВОСТІ ЩОДО АДМІНІСТРУВАННЯ СИСТЕМИ KNX У ETS-5

ETS ще нещодавно була єдиною можливістю програмування та параметризації KNX пристроїв, що затверджена та гарантує 100% якість роботи будь-яких KNX інсталяцій від особі Асоціації. Цей програмній продукт дозволяє будувати топології, безпосередньо програмувати та параметризувати пристрої, створювати та редагувати фізичні та групові адреси, завдяки яким і відбувається маршрутизація та керування у системі. Також до функціоналу ETS 5 можна віднести можливість створення ключів БЦУ, паролів захисту проекту, зміну портів доступу та налаштування KNX secure/ KNX IPsecure.

Восени 2021 року Асоціацією KNX було випущено у широкий доступ новий програмний продукт ETS 6, який має більш широкий функціонал, як з точки зору інтегратора, тобто функціональних можливостей системи, так і з точки зобу забезпечення безпеки, нижче розглянуто основні відмінності та переваги.

2.2. МОЖЛИВОСТІ ЩОДО АДМІНІСТРУВАННЯ СИСТЕМИ KNX У ETS-6

Інтернет-браузери все частіше використовуються для виконання щоденних завдань. ETS6 керує цим безперешкодно, використовуючи користувальницький досвід (UX), схожий на браузер, із гнучким керуванням вкладками та вікнами.

1. Кілька екземплярів головного вікна

ETS6 пропонує покращене керування вікнами та панелями, що дозволяє одночасно запускати декілька екземплярів вікон. Це дозволяє легко перевіряти та порівнювати дані в межах проекту або між кількома проектами.

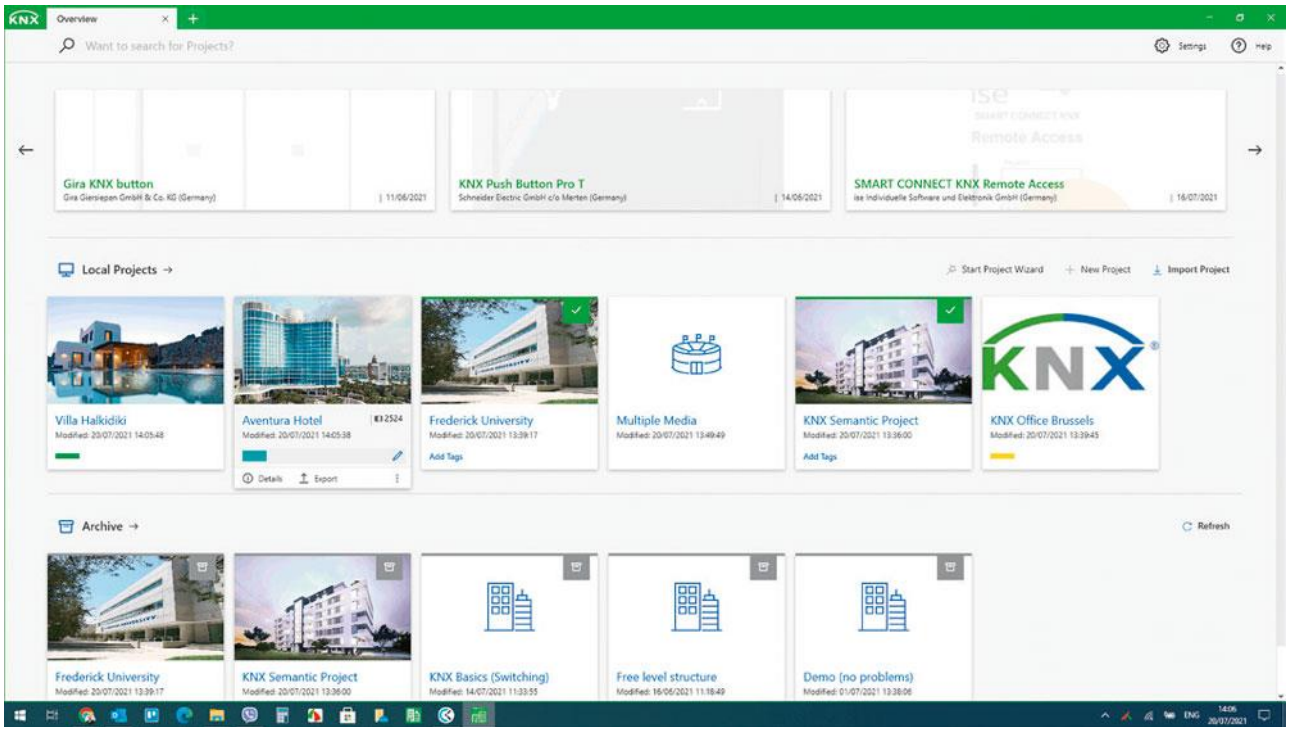

Рис. 2.1 Огляд основного меню ETS6

2. Гнучка обробка вкладок

Легко розгорнути, перетягнути та опустити вкладки, щоб вставити або створити нові екземпляри в ETS6. Щоб створити нову вкладку в тому самому екземплярі ETS6, просто розгорніть її. Потім цю нову вкладку можна перетягнути, щоб створити новий екземпляр, або перетягнути в інший екземпляр ETS6, щоб вона стала вбудованою в цей екземпляр.

3. Хмарне ліцензування

Нова модель ліцензування ETS6 підтримує як хмарне, так і ключове ліцензування. Це дозволяє працювати в автономному режимі, якщо немає підключення до Інтернету. ETS6 підключається до облікового запису MyKNX користувача для отримання інформації про ліцензію.

4. Адаптивна приладова панель

ETS6 кластеризує та сортує проекти на адаптивній та повністю переробленій панелі інструментів. Завдяки доступним метаданим, таким як зображення

обкладинки проекту, тип проекту, теги та піктограми, можна швидко й легко знайти проекти та отримати доступ до них.

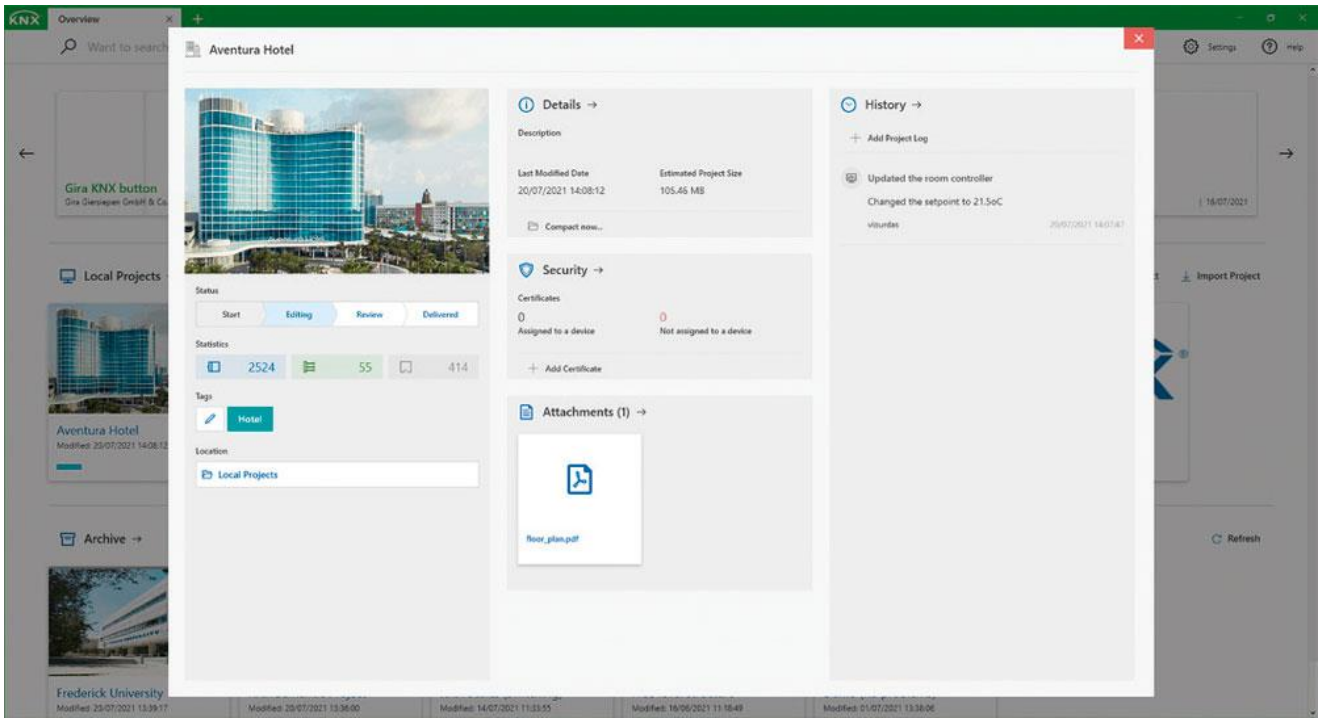

Рис 2.2 – Інформація про проект в ETS6

5. Розширений архів проектів

Спільна робота над проектами спрощена завдяки розширеному архіву проектів у ETS6, який пропонує різні рівні функціональності для різних типів користувачів. Звичайні користувачі можуть використовувати архів проекту як резервну копію своїх файлів проекту. А досвідчені користувачі можуть скористатися розширеними функціями співпраці, які дозволяють кільком людям працювати над

одним проектом.

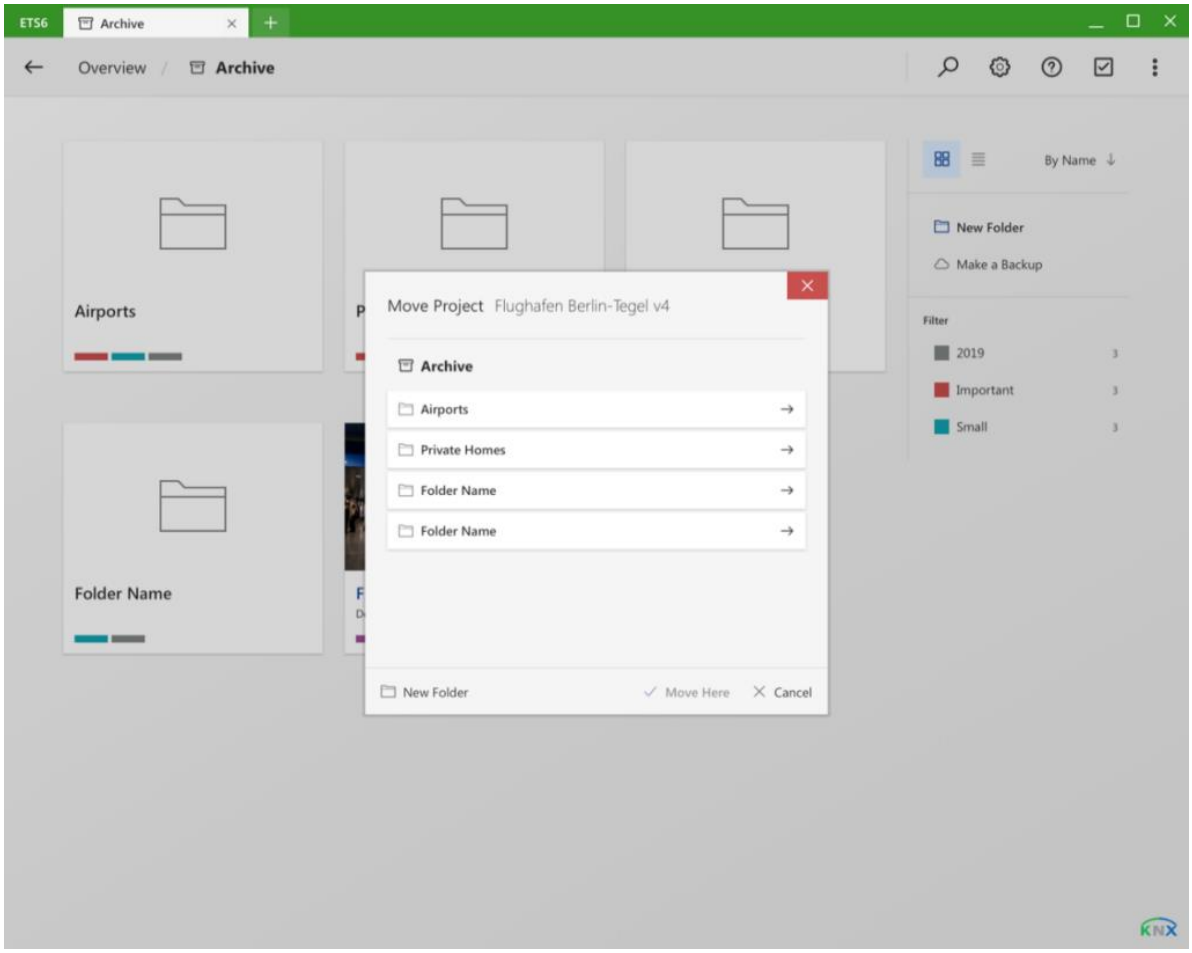

Рис 2.3 – Огляд архіву ETS6

6. «Breadcrumb» навігація

Робоче місце проекту було перероблено, що спрощує переміщення між файлами, ніж будь-коли раніше, завдяки навігації «хлібна дрібка» та опціям «назад/назад» (за допомогою кнопок швидкісного доступу, комбінацій клавіш або клацань мишею). Насправді шукати проект KNX в ETS6 — це як користуватися інтернет браузером

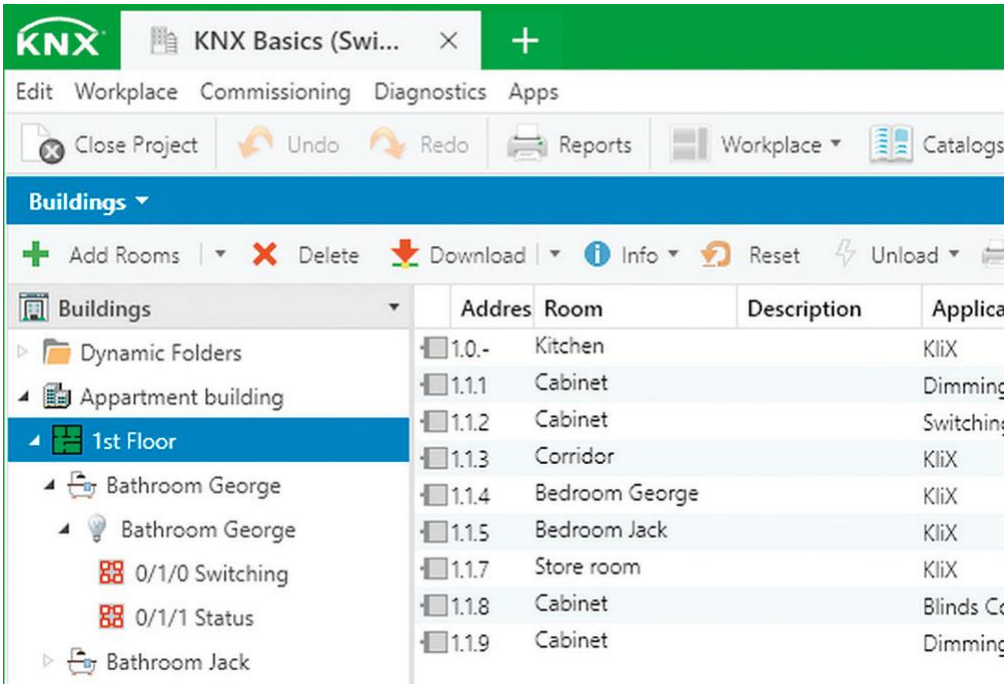

Рис 2.4 – Розробка проекту в ETS6

7. Оптимізоване діалогове вікно «Зв’язати з».

У ETS6 ви можете зв’язати групові адреси набагато швидше завдяки діалоговому вікну «Зв’язати з». Крім того, «Створити нову групову адресу» та «Використовувати наявну групову адресу» тепер легко доступні, що допомагає користувачам не пам’ятати поточну структуру групової адреси.

ETS6 також використовується для частого зв’язування групових об’єктів з груповими адресами. Розширене діалогове вікно «Зв’язати з» полегшує вибір як одного, так і кількох групових об’єктів та/або каналів на пристрої як джерела для посилання на ціль (цілі), у порядку слів Функції або групові адреси для кожного об’єкта. Це означає, що ETS6 підтримує масове зв’язування групових об’єктів з груповими адресами.

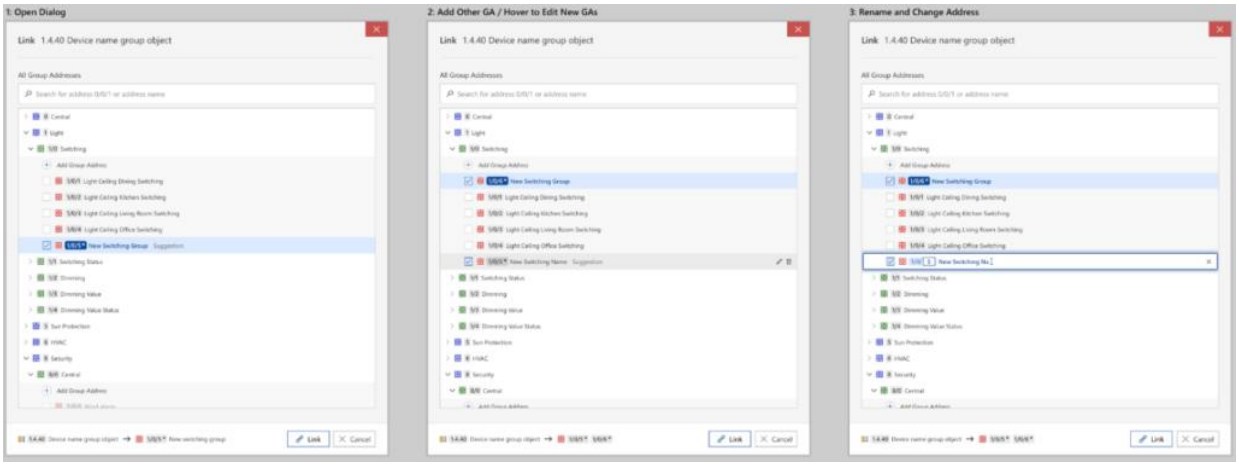

Рис 2.5 – Створення групових адрес ETS6

8. Покращений інструмент оновлення

Ніколи не пропустить важливе оновлення з інтуїтивно зрозумілою системою сповіщень про оновлення ETS6. Підтримка ETS6 в актуальному стані гарантує постійні вдосконалення, а також стабільність вашого програмного забезпечення ETS. Примітки до випуску доступні перед кожним оновленням, а оновлення можна пропустити, якщо хочете.

ETS6 розвиває та покращує функціональні можливості, які пропонує ETS5 Professional для роботи з пристроями KNX Data Secure та KNX IP Secure. Крім того, ETS6 підтримує новітні розширення системи KNX для безпечнішого встановлення KNX, легшого масштабування топології та нового покоління радіочастотних пристроїв.

Системні інтегратори можуть легко розширити існуючі проекти новими пристроями, що підтримують безпеку або радіочастотними пристроями, завдяки ETS6, що підтримує з'єднувачі з функцією з'єднання сегментів і проксі безпеки. Крім усього цього, попередні інвестиції KNX включені в нове програмне забезпечення.

9. Сегментні муфти KNX

З'єднувач сегментів – це розширення медіа-з'єднувача, яке з'єднує відрізки ліній разом, незалежно від їх типу медіа. Сегментні роз'єднувачі KNX – це пристрої,

які розширюють існуючу лінію KNX TP1 за допомогою радіочастотних пристроїв або пристроїв TP1 з фільтрацією або підключають безліч невеликих островів TP1 до KNXnet/IP за допомогою фільтрації

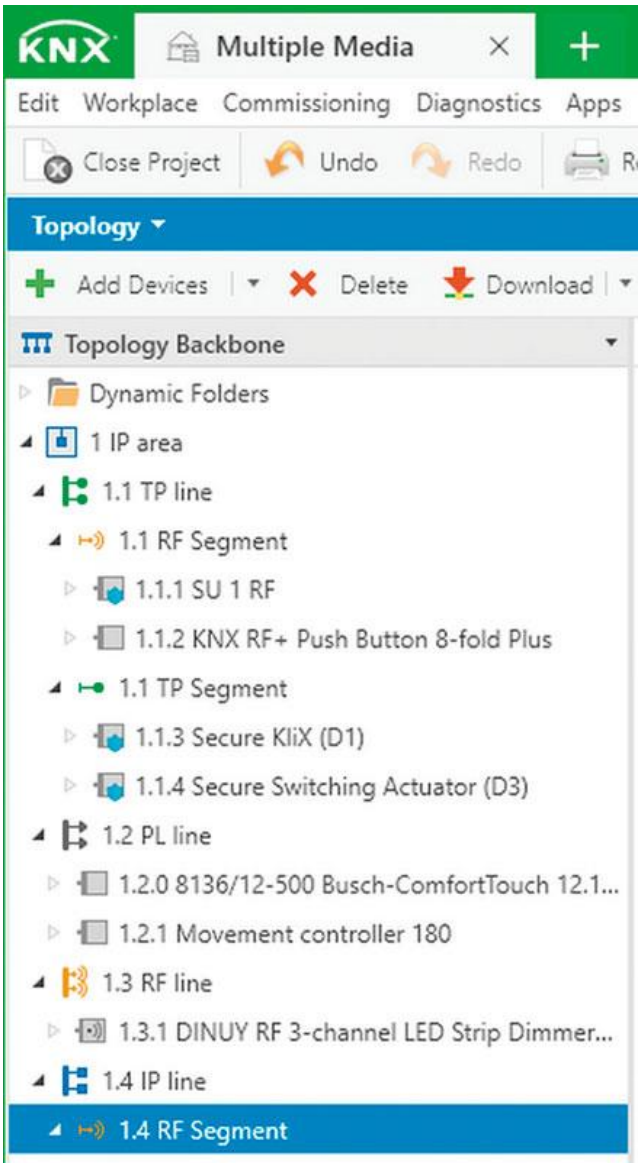

Рис 2.6 – Структура проекту в ETS6

10. KNX Security Proxy

ETS6 підтримує Secure Proxy, розширення з’єднання, яке дозволяє простим пристроям зв’язуватися з пристроями, які працюють безпечно. Це робить це ідеальним способом забезпечення безпеки на нещодавно доданому пристрої під час модернізації існуючих установок захищених пристроями без видалення всіх наявних простих пристроїв KNX.

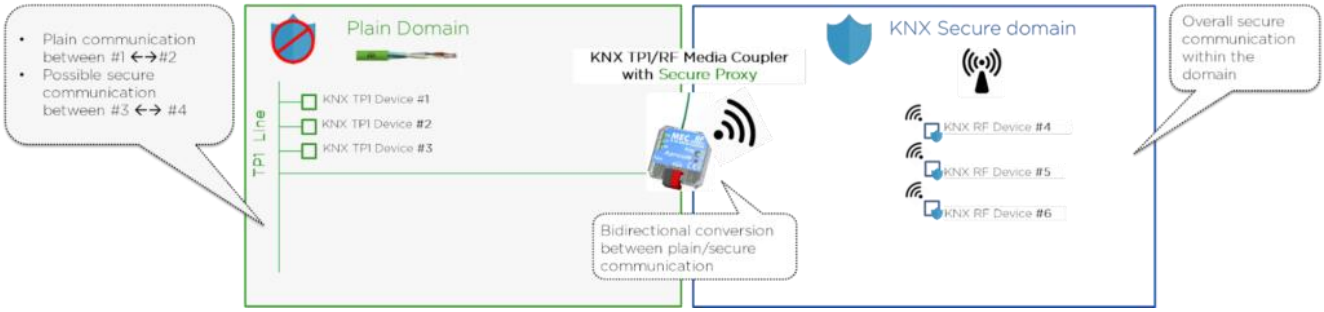

Рис 2.7 – Структура захисту KNX

Пристрої KNX Secure Proxy захищають:

- зв'язок KNX у відкритих підмережах (KNX Data Security)
- Конфігурація пристроїв в установці (KNX Data Security і KNX IP Secure Device Management)
- Зв'язок під час виконання певних програм (KNX Data Security)

11. KNX RF Multi Devices

ETS6 Professional підтримує KNX RF Multi, нове покоління пристроїв KNX RF і заміну KNX RF і KNX Ready. Цей надійний і надійний бездротовий протокол для додатків керування будівлею підтримує гнучкість частоти, використовуючи п’ять різних частот, повторювачі (повторні передавачі), швидкі та повільні режими, «слухати, перш ніж говорити» та швидке підтвердження від до 64 пристроїв (перезавантаження, якщо не вдалося). .

Пристрої RF Multi мають обов’язкову підтримку безпеки та просту конфігурацію, оскільки всі налаштування частоти автоматично встановлюються ETS6. А можливості виконання походять із запису продукту, створеного за допомогою Manufacturer Tool.

KNX RF Multi Devices пропонує:

- Пристрої в системному режимі (на основі можливостей під час виконання із запису продукту ETS6)
- Просте налаштування, оскільки установник нічого не повинен робити
- Безпека з обов'язковим захистом даних KNX

- Автоматична конфігурація частот для кожного каналу (Готовий, Багатошвидкий і Багатоповільний) за допомогою ETS6
- Швидка активація ACK за замовчуванням
- Автоматичне налаштування номера слота ACK за допомогою ETS6[3]

З наведеної вище інформації очевидно, що розробники попіклувалися як про зниження впливу людського фактору – більш комфортна та інтуїтивно зрозуміла середа програмування з можливістю візуалізації дій та перехресної перевірки групових адрес, так і над організацією безпеки безпосередня, додавши можливість швидкого шифрування, покрашеного авто-налаштування девайсів та можливість безпечного налаштування проксі безпосередньо у середовищі розробки, без необхідності для інтегратора специфічних знань в області налаштування мережевих пристроїв.

2.3. ПРИЗНАЧЕННЯ, МОЖЛИВОСТІ ТА ФУНКЦІЇ KNX SECURE

Запобігання доступу мережі до різних фізичних засобів KNX

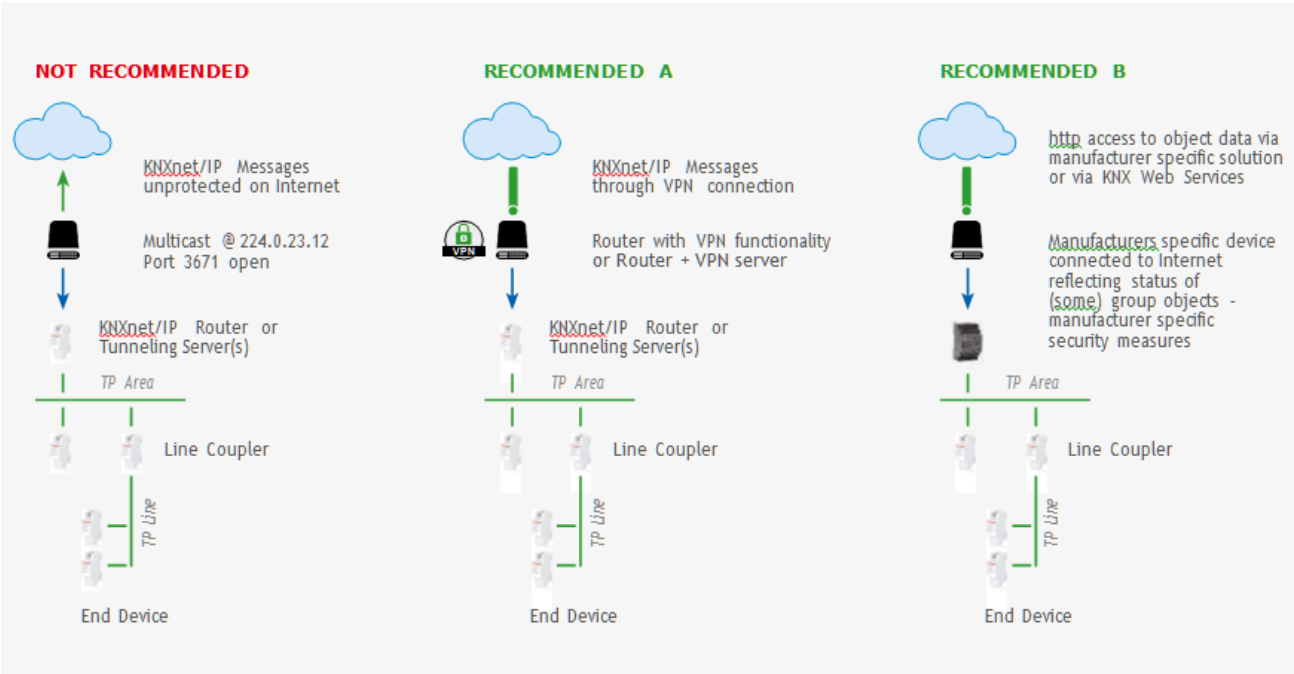

Рис 2.8 – Рекомендації щодо запобігання доступу мережі до різних фізичних засобів KNX

Обмеження небажаних комунікацій в мережі

• Індивідуальні адреси пристроїв мають бути належним чином призначені відповідно до топології, а маршрутизатори мають бути налаштовані так, щоб не передавати повідомлення з невідповідною адресою джерела. Таким чином небажане спілкування може бути обмежено однією лінією.

• Зв'язок "точка-точка" і, можливо, широкомовний зв'язок через маршрутизатори мають бути заблоковані. Таким чином, реконфігурація знову може бути обмежена однією лінією.

• З'єднувачі мають бути налаштовані на активне використання таблиць фільтрів і не передавати групові адреси, які не використовуються всередині певного рядка. Якщо ні, зв’язок, підключений до певної лінії, ризикує неконтрольовано поширюватися на всю установку KNX.

Захист конфігурації зв'язку

ETS дозволяє визначити специфічний для проекту пароль, за допомогою якого можна блокувати пристрої від несанкціонованого доступу. Це
запобігає тому, що конфігурація встановлення може бути прочитана або змінена неавторизованими особами.

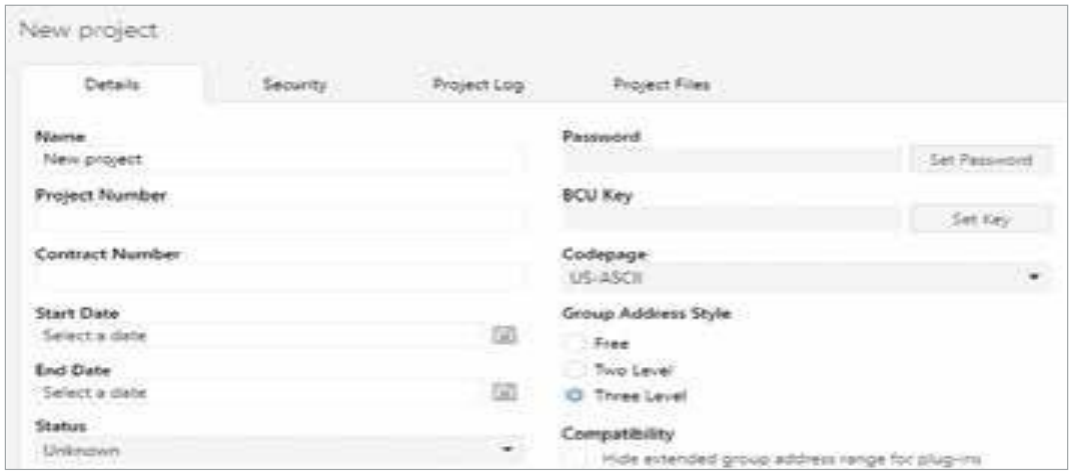

Рис 2.9 – Встановлення парольного захисту

Захист передачі технологічних даних

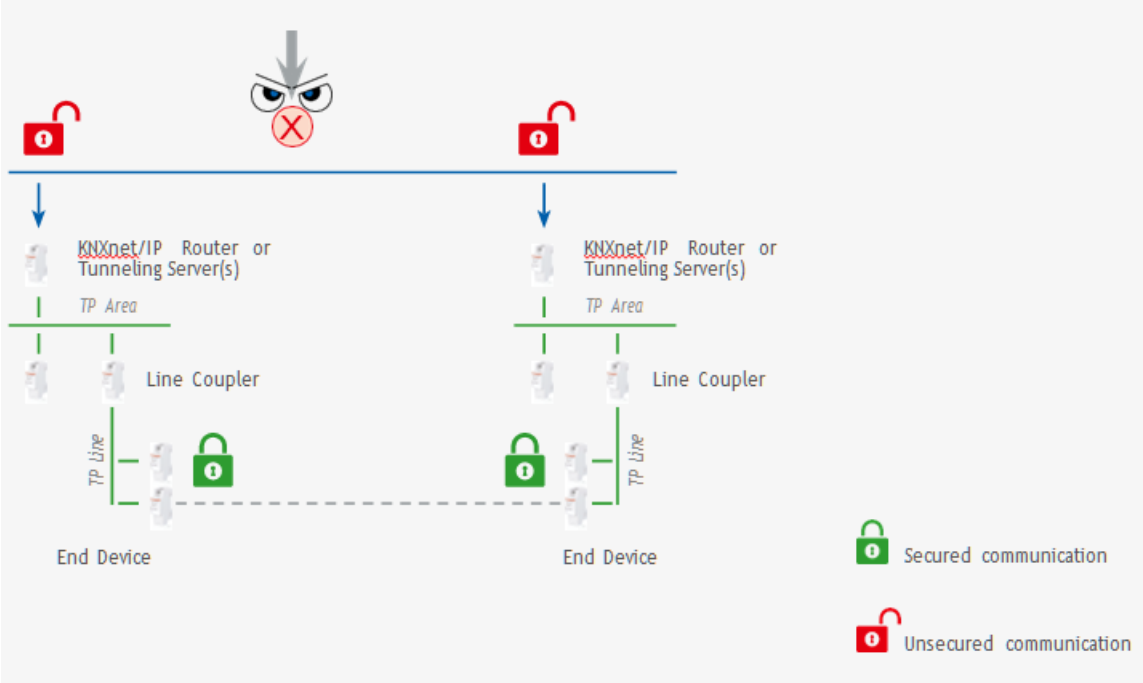

Рис 2.10 –Структура захисту передачі технологічних даних

• Поряд із вищезгаданими заходами, зв'язок під час виконання KNX може бути захищена за допомогою зазначеного

• KNX Data Secure та

• Механізми захисту IP KNX

• KNX Data Secure гарантує, що незалежно від середовища KNX, вибрані повідомлення, надіслані пристроями KNX, можуть бути аутентифіковані та/або зашифровані. Щоб гарантувати, що навіть у випадку, коли такий зв’язок не буде захищеним і такі мережі будуть підключені до IP, KNX IP Secure

Крім цього, були визначені механізми. Таким чином гарантується, що повідомлення про тунелювання або маршрутизацію KNX IP не можуть бути записаними або переданими на IP. Механізми KNX IP Secure забезпечують додавання оболонки безпеки навколо всього трафіку даних KNXnet/IP.

• Механізми захисту даних KNX і KNX IP Secure гарантують, що пристрої можуть встановити захищений канал зв'язку, забезпечуючи таким чином:

• Цілісність даних, тобто. е. запобігання зловмиснику отримати перевагу

контролю за допомогою введення маніпульованих кадрів. У KNX це забезпечується шляхом додавання коду автентифікації до кожного повідомлення: цей доданий код дозволяє перевірити, що повідомлення не було змінено і що воно фактично походить від довіреного партнера по комунікації.

• Свіжість, тобто запобігання зловмиснику записувати кадри та відтворювати їх пізніше, не маніпулюючи вмістом. У KNX Data Secure це забезпечується порядковим номером, а в KNX IP Secure — ідентифікатором послідовності.

• Конфіденційність, тобто шифрування мережевого трафіку, щоб гарантувати, що зловмисник має найменше уявлення про фактично передані дані. Дозволяючи шифрувати мережевий трафік KNX, пристрої KNX забезпечують принаймні шифрування відповідно до алгоритмів AES-128 CCM разом із симетричним ключем.

Симетричний ключ означає, що той самий ключ використовується відправником для захисту вихідного повідомлення (автентифікація + конфіденційність!), а також одержувачем(ами) для перевірки при отриманні цього повідомлення.

Пристрої KNX Data Secure використовують довший формат телеграм KNX під час передачі автентифікованих та зашифрованих даних. Це не впливає на швидкість реакції пристроїв. Для KNX Data Secure пристрої захищені таким чином:

• Пристрій постачається з унікальним ключем заводського налаштування пристрою (FDSK).

• Програма встановлення вводить цей FDSK в інструмент конфігурації ETS (ця дія в будь-якому випадку виконується не через шину).

• Інструмент конфігурації створює ключ інструмента для конкретного пристрою.

• Через шину ETS надсилає на пристрій, який потрібно налаштувати його ключ інструменту, однак шляхом шифрування та автентифікації цього

повідомлення за допомогою попередньо введеного FDSK. Ні інструмент, ні ключ FDSK в будь-який час не передаються у вигляді простого тексту по шині.

• З цього моменту пристрій приймає лише ключ інструменту для подальшої конфігурації за допомогою ETS. FDSK більше не використовується під час подальшого зв’язку, якщо пристрій не буде скинуто до заводського стану, після чого всі захищені дані в пристрої будуть стерті.

• ETS створює ключі часу виконання (скільки необхідно) для групового зв'язку, який необхідно захистити.

• Через шину ETS надсилає на пристрій для налаштування ці ключі виконання, однак шляхом шифрування та автентифікації цих повідомлень за допомогою ключа інструмента. Ключі часу виконання ніколи не передаються у вигляді простого тексту по шині.

Для KNX IP Secure безпечне з’єднання (тунелювання або керування пристроями) встановлюється таким чином:

• І клієнт, і сервер створюють окрему пару відкритих/приватних ключів. Це називається асиметричним шифруванням.

• Клієнт надсилає свій відкритий ключ на сервер у вигляді простого тексту.

• Сервер відповідає своїм відкритим ключем у вигляді простого тексту, доповненим результатом наступного обчислення: він обчислює значення XOR свого відкритого ключа сервера з відкритим ключем клієнта, шифрує його кодом пристрою для автентифікації в клієнта і шифрує це вдруге за допомогою обчисленого ключа сеансу.

Код автентифікації пристрою призначається ETS під час конфігурації або клавішею інструменту. Цей код автентифікації пристрою необхідно надати оператору.

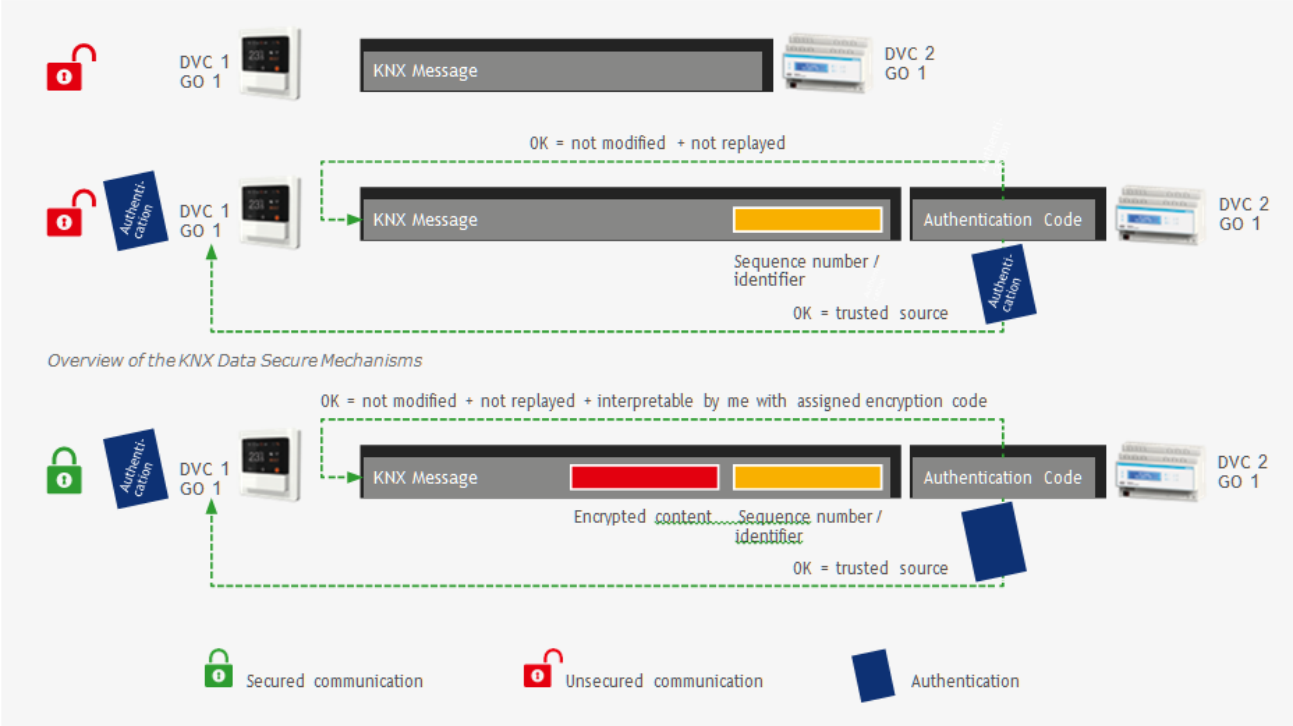

Рис. 2.11 – Структура KNX Secure

Візуалізація, яка бажає встановити безпечне з'єднання з відповідним сервером.

• Клієнт виконує ту ж операцію XOR, але авторизується, спочатку зашифрувавши це одним із паролів сервера, а вдруге — ключем сеансу.

Слід зазначити, що використаний алгоритм шифрування (Diffie Hellmann) гарантує, що ключ сеансу клієнта та сервера ідентичні. Паролі сервера необхідно надати оператору візуалізації, який бажає встановити безпечне з'єднання з відповідним сервером.

Що стосується вищеописаних заходів для захисту зв’язку під час виконання, слід зазначити, що:

• Пристрої KNX Data Secure можна без проблем використовувати поруч із «класичними» пристроями KNX. Це означає, що дані KNX та IP Secure можуть бути реалізовані як додатковий захід безпеки.

• Якщо установник вирішує використовувати пристрій KNX IP Secure в IP-магістралі, усі IP-з'єднувачі та будь-які IP-пристрої KNX у цій магістралі повинні мати тип KNX IP Secure.

• Якщо установник – за бажанням клієнта – використовував для функції захищений пристрій KNX для забезпечення зв’язку під час виконання, кожен партнер по комунікації цього пристрою також повинен підтримувати KNX Secure для пов’язаної функції. Іншими словами, комунікаційний об’єкт безпечного пристрою KNX не може бути пов’язаний один раз із захищеною груповою адресою і один раз із звичайною груповою адресою. Пристрої, які підтримують дані KNX та захист IP, можна відрізнити від «класичних» пристроїв KNX, оскільки на етикетці продукту зображений знак «X».

ETS підтримує KNX IP Secure і KNX Data Secure від версії 5,5 і далі. ETS дозволяє налаштувати нові пристрої KNX Secure, а також замінити несправні пристрої KNX Secure.

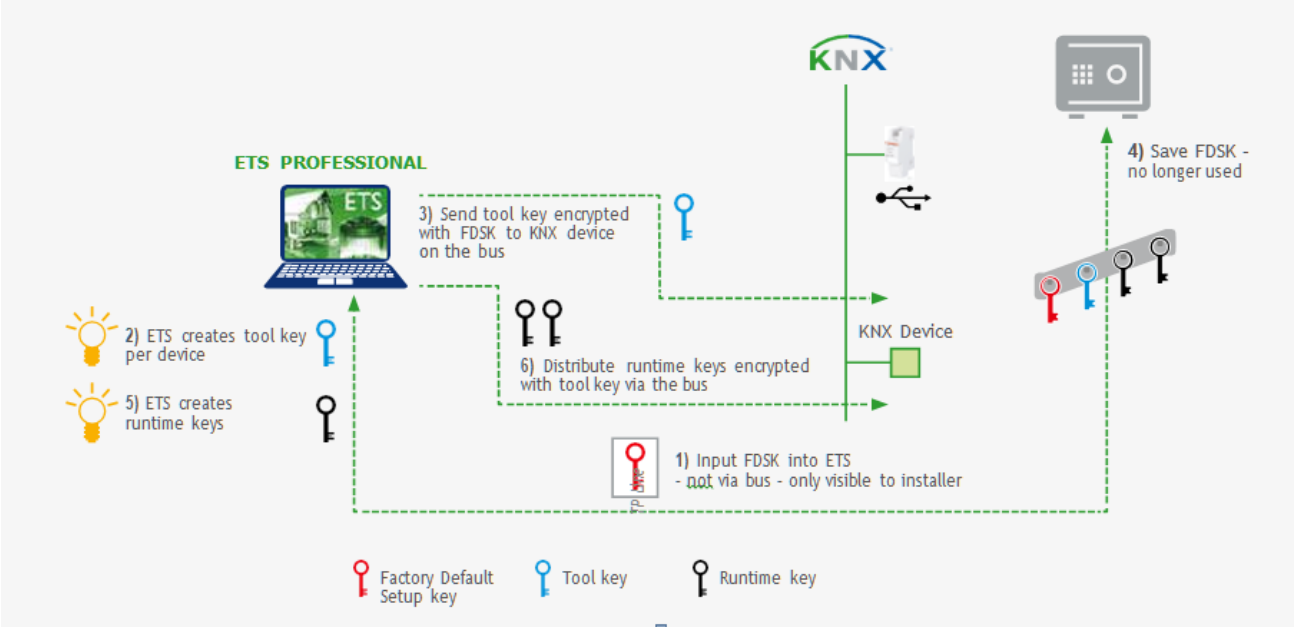

Рис 2.12 KNX IP Secure і KNX Data Secure

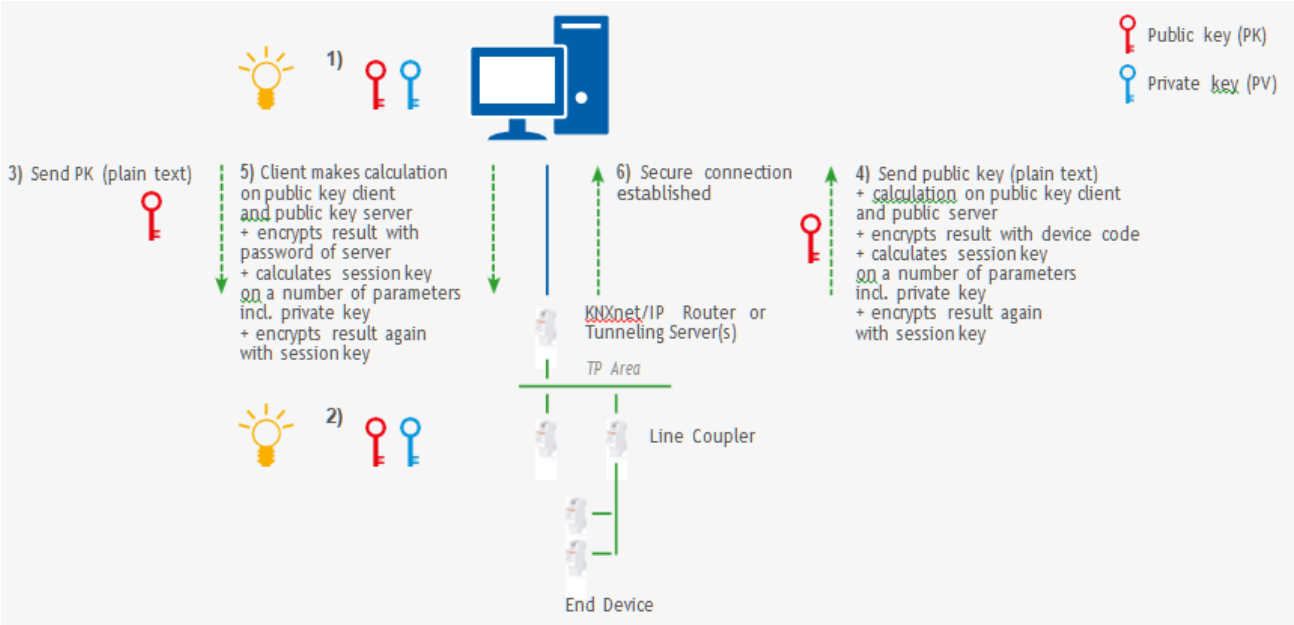

Рис 2.13 - Зв'язок KNX до систем безпеки

Під час підключення KNX до таких застосувань, як системи захисту від злому / протипожежного захисту / систем відкривання дверей, це можна забезпечити за допомогою:

• Пристрої або інтерфейси KNX з відповідною сертифікацією від місцевих страхових компаній;

• контакти без потенціалу (напруги) (бінарні входи, кнопкові інтерфейси, і т. д.);

• відповідні інтерфейси (RS232, ...) або шлюзи: у цьому випадку має бути впевнено, що зв'язок KNX не може запустити функції, пов'язані з безпекою, у частині безпеки установки.

Визначення несанкціонованого доступу до шини

• Очевидно, що шину можна відстежувати та відстежувати незвичайний рух.

• Пристрої KNX Secure відстежують злому в журналах збоїв безпеки: таким чином можна в будь-який час перевірити, чи інсталяція KNX піддалася атакам безпеки.

• Деякі типи пристроїв можуть визначити, чи інший пристрій надсилає телеграми зі своєю індивідуальною адресою. Це не оголошується спонтанно в мережі, але це можна прочитати в PID_DEVICE_CONTROL.

• Зовсім нещодавнє впровадження може вже показувати PID_DOWNLOAD_COUNTER. Порівняння зчитуваного значення (періодично) з опорним значенням сигналізує про зміни в конфігурації пристрою.

Відповідність регламенту ЄС GDPR

• GDPR – це абревіатура від загального регламенту захисту даних (див. https://ec.europa.eu/info/law/law-topic/data-protection_en).

Постанова спрямована на гармонізацію законів про захист даних у всій Європі.

• Для дотримання регламенту GDPR установник повинен передати файл проекту ETS замовнику. Установник і замовник повинні підписати декларацію про захист даних.

• Дані, які генеруються пристроями KNX, можуть використовуватися лише з метою дистанційного керування пристроєм клієнтом (через додаток), для діагностичних цілей та для подальшого розвитку продукту. Їх не можна використовувати для персоналізованої реклами.

2.4. РОХРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ KNX СИСТЕМ

Останнім часом почастішали атаки хакерів на інсталяції KNX. Вже відомо чимало випадків, включаючи Україну, коли KNX інсталяції виявилися з ладу, а самі пристрої KNX, встановлені на об'єктах - заблокованими для користувачів та інтеграторів.

Для «злому» шини KNX використовувалася безтурботно залишена інтеграторами можливість віддаленого інтернет-підключення до об'єктного KNX IP-інтерфейсу через порт 3671. У таких випадках зловмисники таємно збирають інформацію про встановлені на об'єкті пристрої KNX, а пізніше протягом лічені

хвилини перепрограмують ті з них , які опинилися у безпосередній досяжності з топології шини KNX.

Метою атак були «обнулення» пристроїв KNX шляхом завантаження в них програм – «пустушок» і, що найнеприємніше, встановлення пароля (т.зв. ключ BCU), що блокує доступ до пристроїв для їхнього перепрограмування в подальшому.

Зняття блокування пристроїв KNX без знання встановленого хакером пароля можливе лише за умов заводу-виробника. Отже, принаймні один або кілька пристроїв KNX повинні бути демонтовані з об'єкта і відправлені виробнику. Крім того, такі випадки не є гарантійними, і послуга розблокування може бути платною. Підсумок - губляться час та гроші.

Гірка іронія в тому, що для заподіяння максимальної шкоди злочинці використовують штатний засіб KNX, призначений для захисту від подібних загроз - встановлення всередині пристроїв KNX системного парольного захисту.

У будь-якому випадку є недолік досвіду або невиправдана безтурботність інтеграторів. Для фахівців, хто ще не знайомий з практикою анти кримінального захисту в KNX, нижче наводяться рекомендації, дотримання яких надійно захистить KNX інсталяцію від неприємностей.

Заходи захисту IT

Закриття порту 3671.

Порт 3671 використовується протоколом KNXnet/IP Tunneling стандарту KNX для IP підключення програми ETS (інструментальне програмне забезпечення KNX) до KNXIP-інтерфейсів або KNX IP-роутерів з метою діагностичного сканування шини KNX TP, збору даних про підключені до шини KNX пристрої та їх програмування. Таким чином, якщо на об'єкті передбачено підключення KNX інсталяції до мережі Інтернет, то настійно рекомендується не залишати в інтернет-роутері відкритим порт 3671 протягом тривалого часу.

Як додатковий захід безпеки, віддалений зв'язок з об'єктом за протоколом KNXnet/IP Tunneling можна налаштувати, використовуючи будь-який нестандартний порт, відмінний від стандартного 3671. Це реалізується

налаштуваннями зв'язуваних інтернет-роутерів - того, що на об'єкті і віддаленого. Але і подібний "проксі"-порт повинен залишатися закритим, коли інтегратором не ведуться роботи у віддаленому режимі.

Настроювання брандмауера (firewall).

Локальна мережа, яка використовується як частина KNX інсталяції, повинна бути відокремлена від зовнішнього інтернету відповідним настроюванням брандмауера роутера так, щоб пакети KNXnet/IP трафіку не мали можливості для виходу до зовнішнього інтернету. Це досягається закриттям портів роутера із боку домашньої локальної мережі у зовнішньому напрямку. Зокрема, брандмауер повинен ізолювати внутрішню локальну мережу, використовувану KNX як середовище передачі для головних ліній областей або магістралі від широкомовного трафіку (broadcast), що надходить із зовнішньої сторони і, навпаки, замикати груповий трафік KNX (multicast) всередині локальної мережі об'єкта.

Використання каналу VPN для зовнішнього доступу.

Найкраще, якщо зовнішні з'єднання з локальною мережею об'єкта здійснюються через захищені канали VPN. Для цього на об'єкті рекомендується передбачити встановлення інтернет-роутера з функцією VPN сервера або встановлення автономного VPN сервера на ПК платформі.

WEB доступ до KNX інсталяції.

Дистанційне керування KNX інсталяцією може здійснюватися через спеціалізовані KNX пристрої з вбудованим web-сервером за протоколом HTTP або через інші стандартизовані в KNX web-сервіси. У цьому випадку мережна безпека забезпечується розробником такого рішення.

Встановлення на об'єкті сервісного комп'ютера із ETS.

Якщо віддалене інтернет-підключення до шини KNX необхідно інтегратору тільки в налагоджувальних та сервісних цілях, то можливе встановлення на об'єкті сервісного ПК з програмою ETS та програмою віддаленого доступу (TeamViewer, Chrome Remote Desktop тощо). У цьому випадку, очевидно, IP-

інтерфейс KNX може бути повністю відключений від зовнішньої мережі (порт 3671 закритий в інтернет-роутері).

Фільтрування IP та MAC адрес.

Додатковим захисним заходом від несанкціонованого проникнення зловмисників у локальну мережу об'єкта може стати настроювання в інтернет-роутері фільтра довірених IP адрес. Таким чином, спроби зовнішнього підключення з IP адрес, що не потрапили до списку довірених, блокуватимуться роутером.

У разі розгортання на об'єкті бездротової WiFi мережі (WLAN), крім фільтрації IP адреса в, не зайвим буде налаштування MAC фільтра при конфігуруванні роутерів та точок доступу WiFi.

Безпечне налаштування бездротової локальної мережі.

Якщо на об'єкті розгорнуто WLAN, то слід дотримуватися стандартних заходів щодо її безпечного конфігурування: зміна всіх заводських налаштувань за замовчуванням на користувацькі; відключення періодичної трансляції в ефір SSID (beaconing); настроювання надійного пароля та шифрування трафіку не нижче рівня WPA2; використання MAC фільтрів і т.д.

BMS на базі окремої локальної мережі.

Для середніх і великих проектів KNX ідеальним рішенням є створення для системи управління будівлею (BMS) незалежної локальної мережі. У цьому випадку ступінь захищеності KNX BMS буде значно вищим.

Заходи захисту KNX

Зміна стандартної мультикастної адреси KNXnet/IP Routing

За замовчуванням у протоколі KNXnet/IP Routing для групової (multicust) комунікації між IP-роутерами KNX використовується адреса 224.0.23.12. Для кращої безпеки KNX інсталяції рекомендується його заміна на інше значення з допустимого мультикаст-діапазону адрес (224.0.0.0 - 239.255.255.255). Для цього необхідно зробити у програмі ETS відповідне налаштування при параметризації KNX IP-роутерів або змінити цей параметр у властивостях магістральної IP-лінії вікна Топологія ETS.

Безпечне настроювання KNX IP-роутерів.

Налаштуванням KNX IP-роутерів та лінійних з'єднувачів може бути блокована передача фізичних телеграм* у нормальному режимі експлуатації KNX інсталяції.

У цьому випадку ризику несанкціонованої переконфігурації може бути схильна лише одна лінія KNX.*) Телеграми, що передаються з ETS до пристроїв KNX при їх програмуванні або діагностиці.

Встановлення BCU ключа.

Для повного виключення можливості несанкціонованої установки ключа BCU третіми особами, інтегратору, за погодженням із замовником, це можна виконати превентивно. Встановлення такого пароля здійснюється в програмі ETS на панелі «Деталі» в параметрах властивостей проекту (Рис. 2.14).[1]

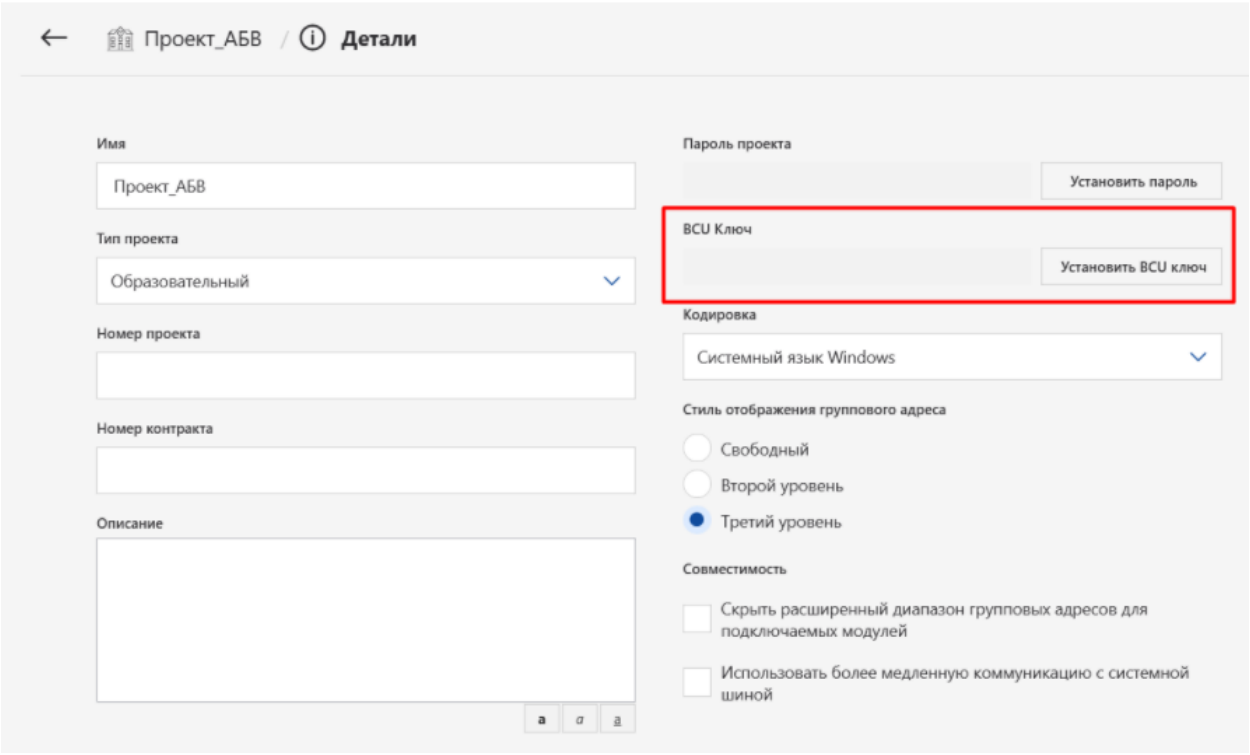

Рис. 2.14 – Параметри властивостей проекту

Після введення у відповідний рядок цифрового ключа та його підтвердження, ключ буде збережено у проекті (Рис. 2.15). Надалі, по ходу послідовного програмування пристроїв KNX, цей ключ-пароль буде встановлюватися вже всередині самих пристроїв KNX. Після цього будь-яке перепрограмування пристроїв KNX без введення пароля виявиться неможливим.

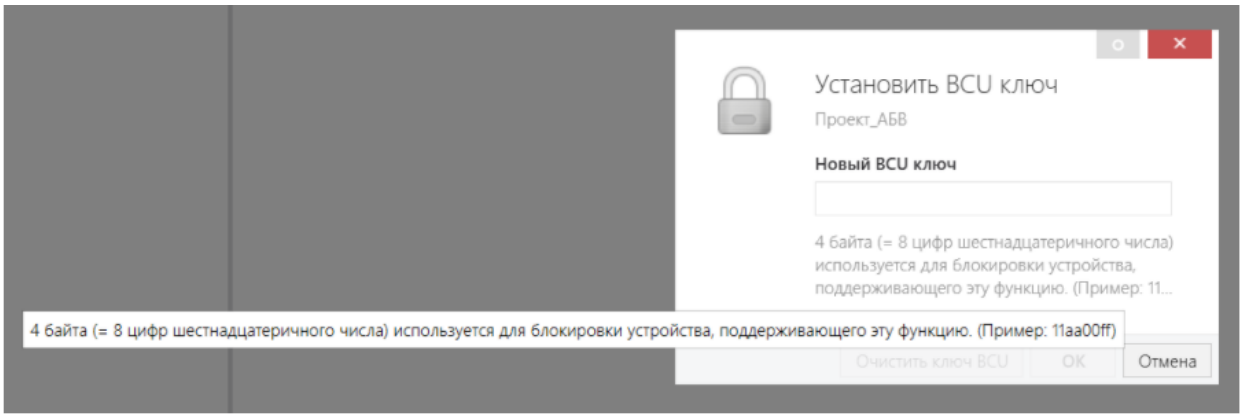

Рис 2.15 – Встановлення ключа

Напевно, зайве говорити, що встановлений пароль BCU треба надійно зберігати та не забувати, щоб не постраждати від власних дій.

3. РОЗРОБЛЕННЯ ВАРІНТУ ПОБУДОВИ ТА ІМПЛЕМЕНТАЦІЇ ЗАХИЩЕНОЇ KNX СТРУКТУРИ SCADA НА ОБ'ЄКТАХ КВОІ

«Слід зазначити, що останнім часом спостерігається стале зростання кількості спроб несанкціонованого втручання в роботу АСУ/SCADA КВОІ (кібернетичних атак) внаслідок чого органи державного та військового управління, суб'єкти господарювання державного та приватного секторів економіки отримують величезні збитки, а суспільство опиняється на межі як локальних, так і глобальних техногенних катастроф» [13]. «При цьому, технології та методи забезпечення інформаційної безпеки впроваджуються переважно в автоматизованих системах, у яких обробляється інформація, щодо якої законодавчо визначена відповідальність за реалізацію та дотримання відповідної системи нормативно-організаційних та інженерно-технічних заходів» [14].

Взагалі, КВОІ – це критично важливі об'єкти інфраструктури, тобто такі об'єкти перебої у функціонуванні яких призведуть до порушення штатного режиму, що може призвести до надзвичайної ситуації техногенного характеру, порушенню функціонування суспільства даного міста/регіону/країни, прикладом таких об'єктів будуть електростанції, хім. заводи великого масштабу, містоутворюючі підприємства, продовольчі заводи, що формують великий об'єм продуктів споживання громадян, або настільки великий об'єм продукції, що порушення роботи такого заводу призведе до значного зменшення об'єму ВВП.
Оскільки креслення та структура управляння діючих КВОІ є що найменш інформацією для службового користування, у рамках дослідження було побудовано умовний цех виготовлення хлібу, в рамках роботу було встановлено допущення, що у зв'язку з віддаленістю населеного пункту, у разі погіршення погідних умов, дане підприємство буде єдиним, що забезпечує виготовлення та реалізацію хлібних продуктів, що належать до споживчого кошику.

3.1. РОЗРОБЛЕННЯ ТОПОЛОГІЇ ТА ФУНКЦІОНАЛУ ЗАХИЩЕНОЇ KNX СТРУКТУРИ

Для побудови захищеної системи автоматизації в першу чергу необхідно розглянути склад систем, які необхідно автоматизувати: в даному випадку це система освітлення з можливістю зміни яскравості, клімат(повітряна система, було використано канальні 4х трубні фанкойли, що дозволяє як нагрівати, так і охолоджувати повітря, припливно-витяжну вентиляційну установку), виробниче обладнання, систему охорони периметру.

Рис. 3.1 – Основне креслення цеху

На Рис. 3.-1 видно основну структуру приміщення, входи/виходи, вікна та функціональні призначення робочих зон.

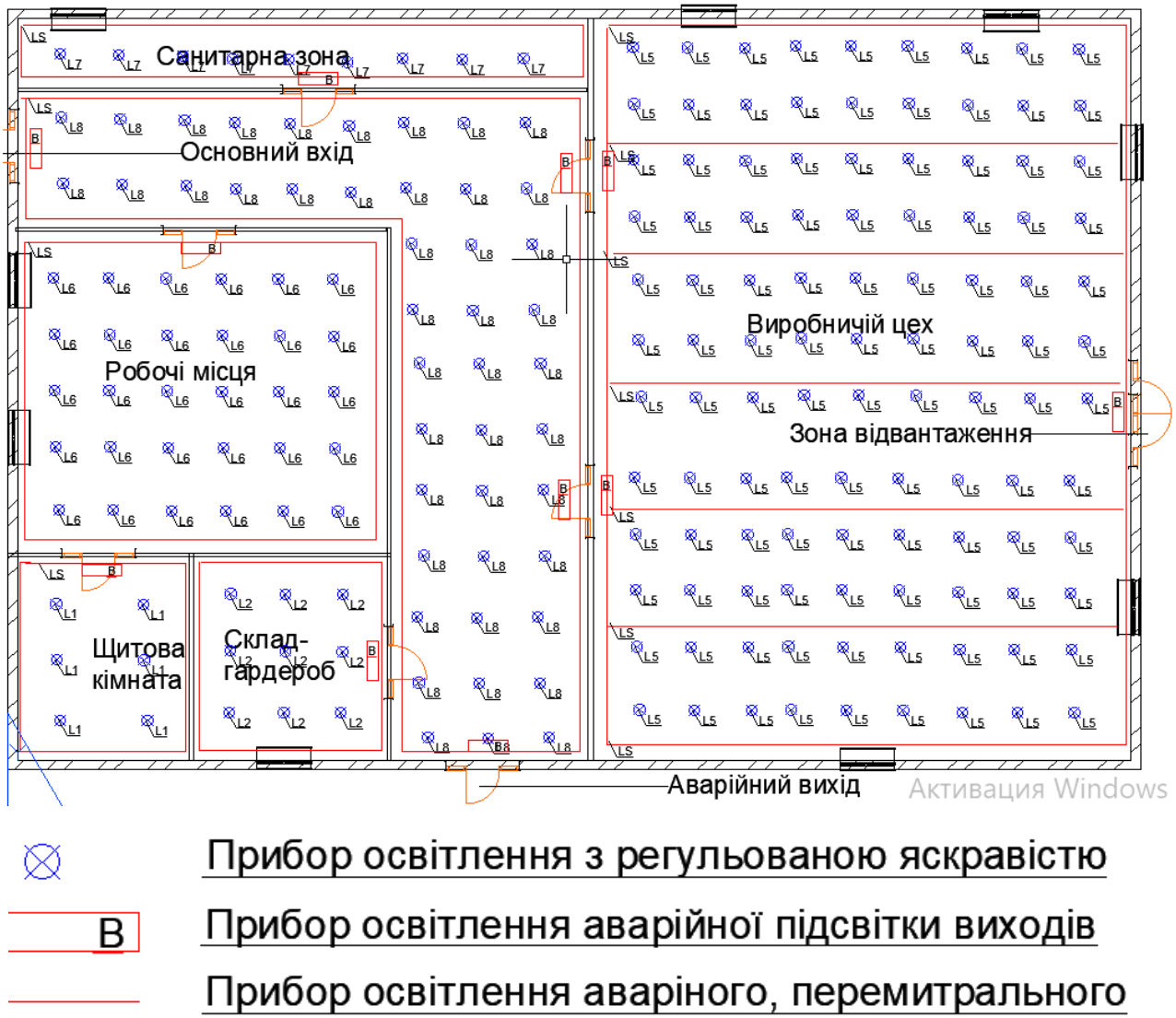

Рис. 3.2 – Схема освітлення

На Рис. 3.2 розглянуто структурне розміщення груп освітлення. Було використано точкові LED-світильники з керуванням за протоколом DALI, що дозволяє змінювати як яскравість освітлення, так і тип(можливість задавати у відсотковому співвідношенні теплоту освітлення), як для групи освітлення, так і безпосередньо для кожного світильника.

Також було використано, у якості аварійного освітлення профілі з LED-стрічкою та світильники з написом «Вихід» у відповідних місцях. Взявши до уваги важливість аварійного освітлення та малу споживчу потужність, було прийнято рішення про підключення аварійного освітлення до джерела безперебійного живлення з використанням жаростійкого кабелю.

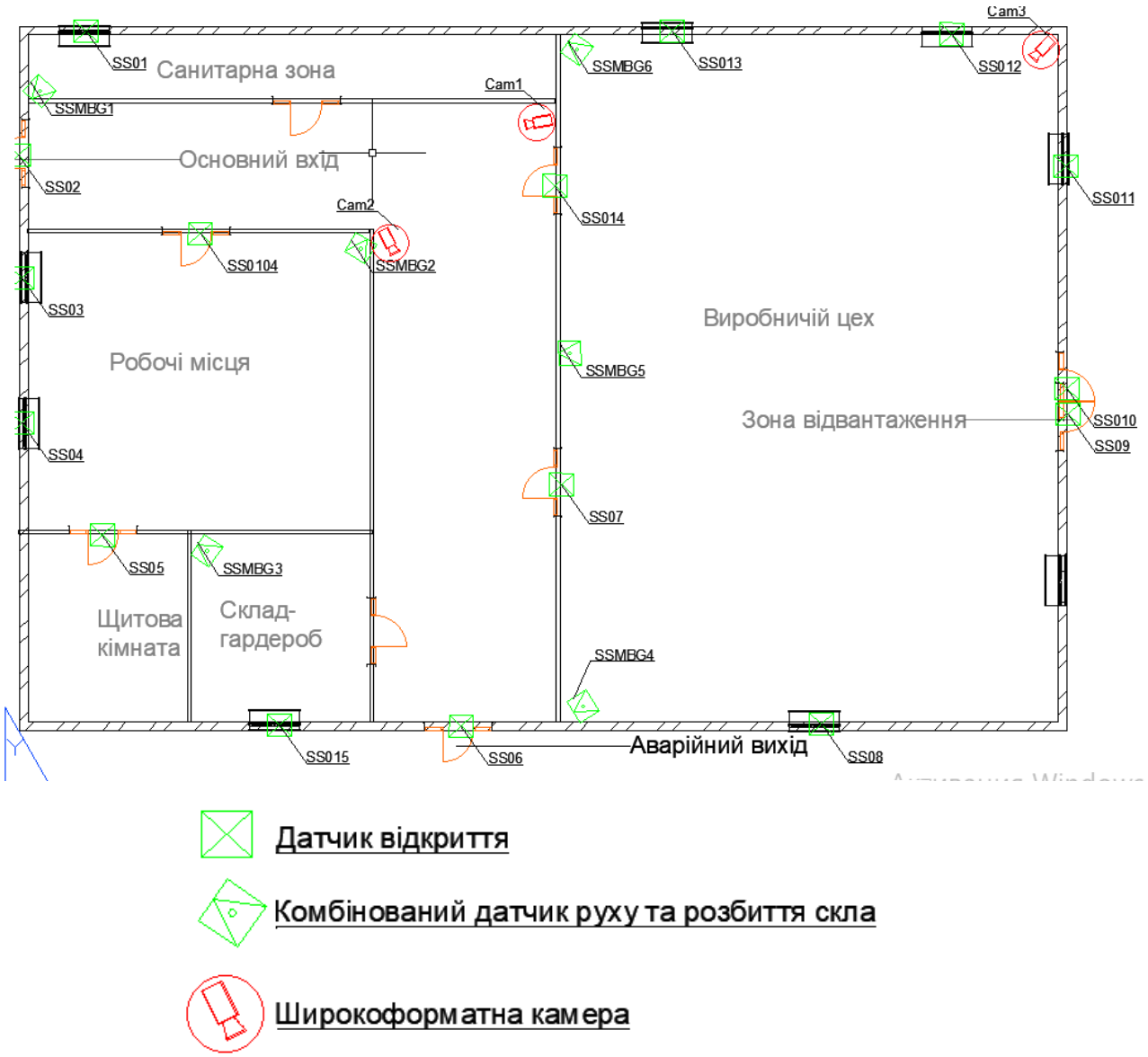

Рис. 3.3 – Основні технічні засоби захисту

На Рис. 3.3 показана система периметральної охорони. Було використано класичні магнітна датчики відкриття вікон та дверей (геркони), комбіновані датчики розбиття скла та руху у відповідних приміщенях. Також було встановлено широкоформатні камери з можливістю зйомки в темноті, розпізнаванням руху та обличчь і фукцією сповіщення відповідальних осіб у раз фіксації віщеназваного у визначений(неробочий) час.

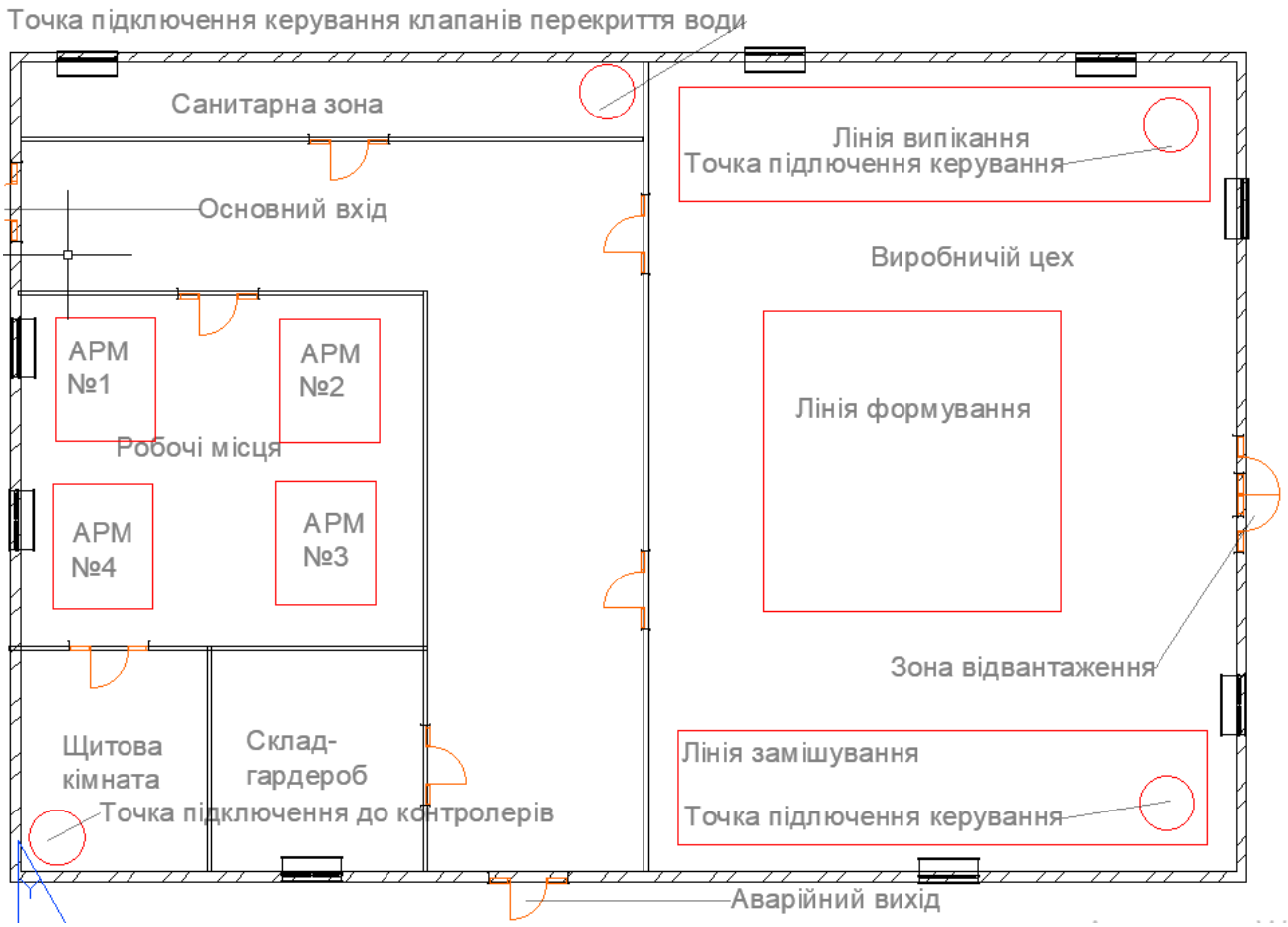

Рис. 3.4 – Схема розташування виробничого обладнання

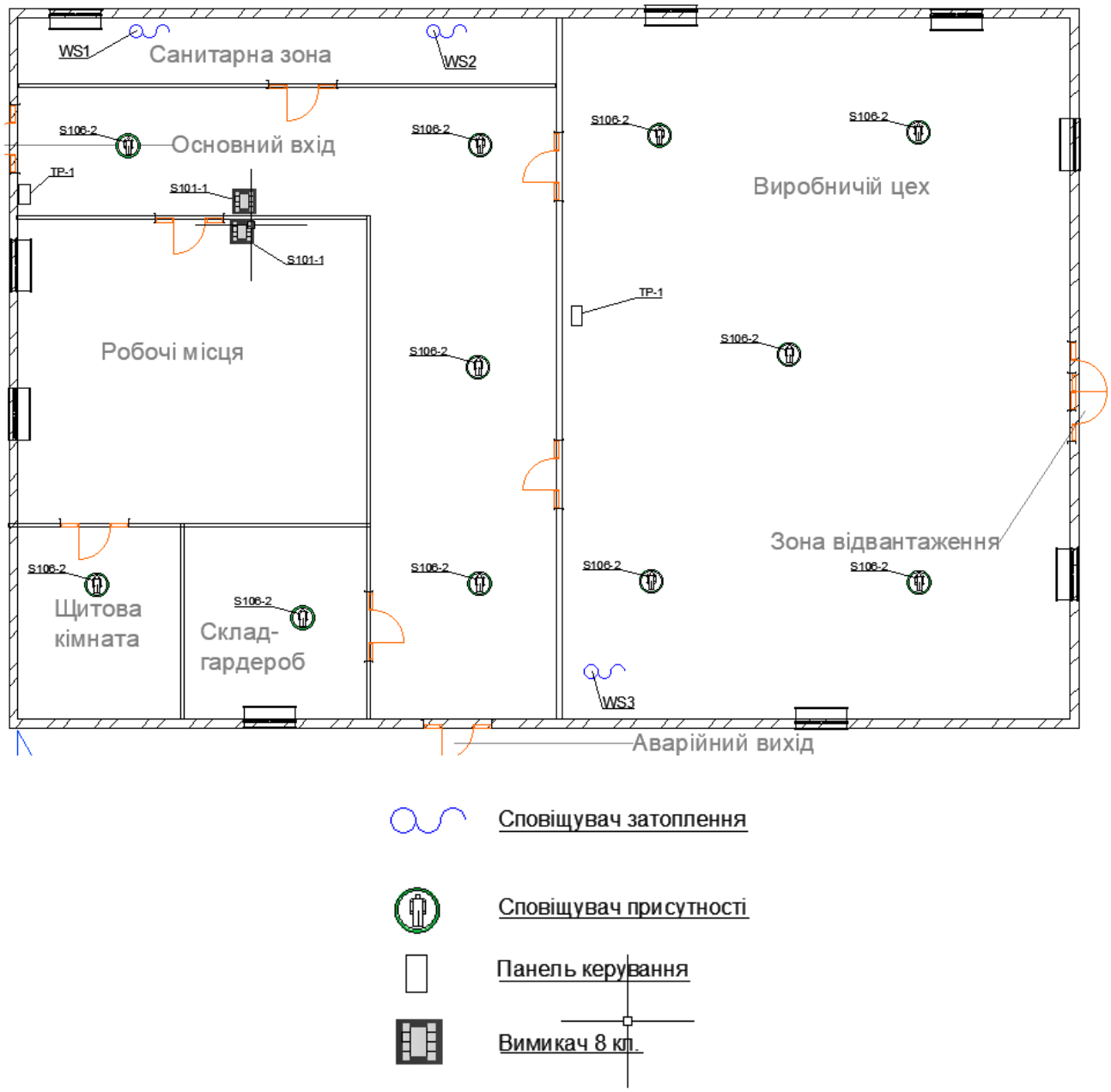

Рис. 3.5 – Сенсори керування

На Рис. 3.5 – можна побачити схему розташування обладнання сенсорів керування, датчики присутності персоналу з функцією оцінки освітлення та температури, що дозволяє при попередньому налаштуванні обладнання автоматично обирати яскравість та теплоту освітлення в залежності від технологічного процесу. Сповіщувачі затоплення розташовані у «мокрих» зонах, тобто місцях підводу води, а саме у санітарній зоні та зоні замісу, що дозволить

автоматично перекрити водопостачання у разі аварійної ситуації. При вході та у виробничому цеху розташовані панелі керування, які дозволяють керувати усіма системами, як коригуючі автоматичні налаштування, так і переходити в ручній режим керування. Вимикачі на 8 клавіш розташовано біля входу в офісну зону та всередині, дані вимикачі є вільно програмованими, що дозволяю змінювати призначення клавіш, у разі необхідності.

3.2. ПОБУДОВА АРХІТЕКТУРИ ПРОЕКТУ ЗАХИЩЕНОЇ KNX СТРУКТУРИ

У попередньому підрозділі було розглянуто інженерні системи, які потребують автоматизації та систему сенсорів KNX необхідну для організації керування. Розглянемо безпосередньо пристрої керування(актуатори) та шляхи їх захисту. Зробимо допущення у рамках роботи, що для керування виробничім обладнанням необхідно

1. Керувати шляхом вім/викл. Лінією замішування та випічки
2. Керувати температурою лінії випічки
3. Регулювати в автоматичному режимі яскравістю та температурою освітлення у різних зонах виробничого цеху
4. Регулювати з вимикача яскравістю та температурою освітлення зони офісу та коридору
5. В автоматичному режимі керувати вім/викл освітленням технічних приміщення
6. Перекривати ввід водопостачання у разі витоку води
7. Керувати температурою та якістю повітря у всіх зонах
8. У разі порушення периметру передавати показання відповідальній особі та на пункт швидкого реагування охорони.

Обладнання для реалізації

1. Актуатор реле для вім/викл 4х канальний

2. Аналоговий актуатор для керування температурою лінії випічки та перекриття запорних клапанів водопостачання 4х канальний
3. Контролер DALI для керування освітленням
4. Контролер фанкойлів зі входом підключення датчика температури
5. Контролер припливно-витяжної вент. машини
6. Прибор приємно контрольний для охоронної системи з можливістю інтеграції до KNX систем
7. Блок живлення шини KNX

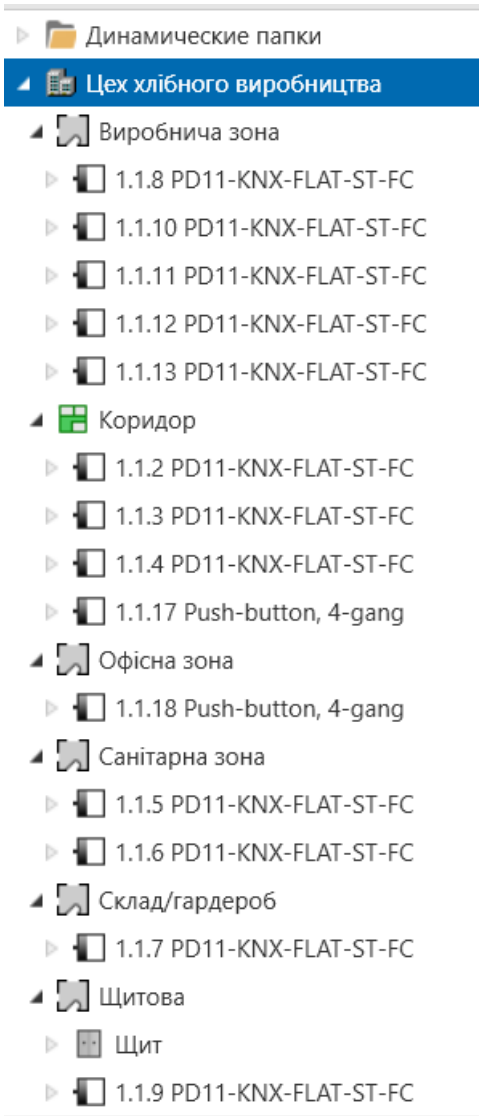

Рис. 3.6 – Структура обладнання системи автоматизації.

На основі побудованої структури проекту (Рис. 3.6) розглянуто шляхи захисту.

1. Перші кроки зроблено на етапі монтажу
    - використання екранованого кабелю
    - Резервна кабельна структура
    - Надійне фіксування обладнання
    - Відмова від використання радіочастотних засобів зв’язку
    - Відмова від використання коплерів
    - Обмежений доступ до місця розташування обладнання
2. Встановлення ключів BCU

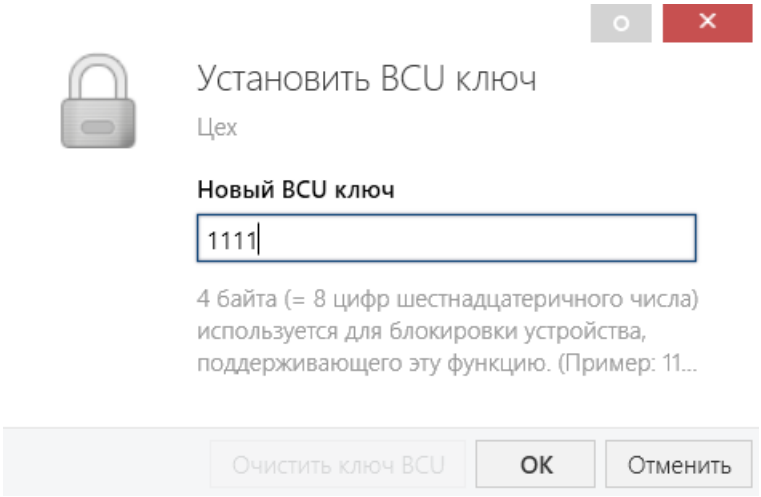

Рис. 3.7. – вікно встановлення ключа в ETS 5

3. Налаштування KNX Secure
    - Додання до проекту пристрою шифрування
    - Встановлення паролю проекту (Рис. 3.7)
    - Базові налаштування шифрування (Рис. 3.8)

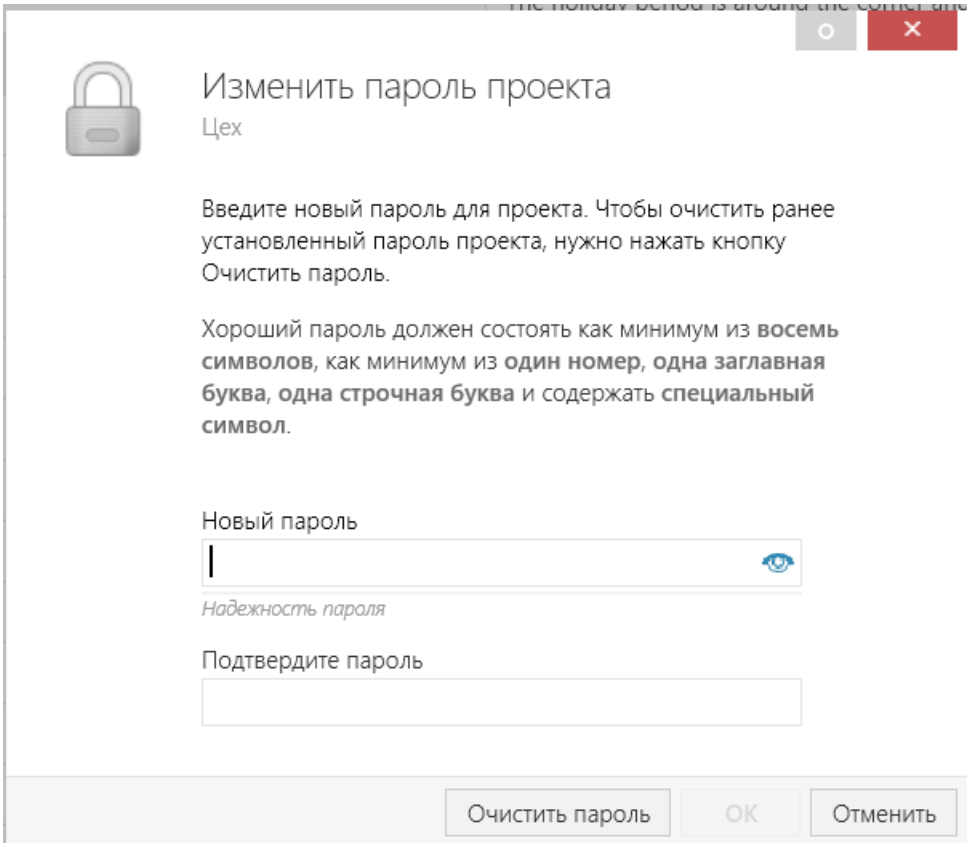

Рис. 3.8 – Встановлення паролю проекту

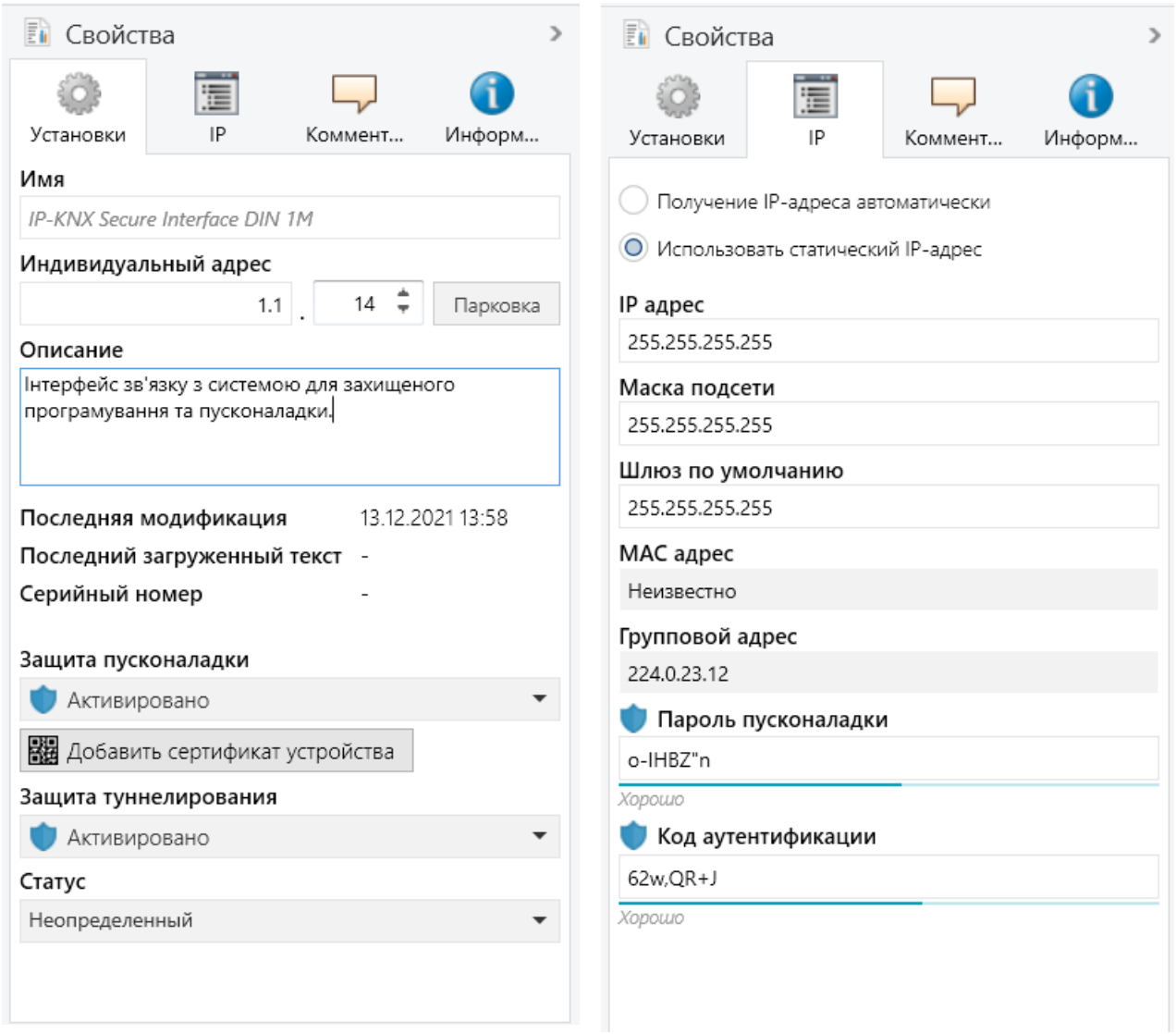

Рис. 3.9 – Базові налаштування KNX Secure

4. Захист тач-панелей керування паролем в залежності від рівня доступу

3.3. РОХРОБЛЕННЯ КОНТРОЛЬНОГО СПИСКУ ПЕРЕВІРКИ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМИ KNX

Нижче представлено список вимог для організації захищеності системи побудованої на технології KNX, з урахуванням вимог асоціації та принципу «найкращої практики».

Для легітимного надання будь-яких рекомендацій щодо роботи з системою, а особливо щодо питань організації стану захищеності необхідно бути партнером Асоціації KNX.

KNX CERTIFICATE

Partner No. 91222
Inna Semenova

is herewith declared

KNX PARTNER

KNX Association hereby confirms that the above person has successfully attended the **KNX Basic course** and has the right to use the "KNX Partner logo" according to the terms agreed upon.

By attending this course the above person is qualified to design, commission and diagnose smart home and building solutions based on KNX.

Joost Demarest, CTO
KNX Association

Brussels, date
14/02/2020

KNX
Smart home and building solutions.
Global. Secure. Connected.

Join **us**
www.knx.org

Рис. 3.10 – Сертифікат партнерства Асоціації KNX

Забезпечення доступу до мережі до різних фізичних засобів KNX Чи були враховані наступні заходи під час встановлення?

1. Чи встановлені пристрої та програми фіксовано?

   Чи забезпечено належний захист пристроївпроти демонтажу (наприклад, використання засобів захисту від крадіжок)?

 Чи забезпечено обмежений доступ сторонніх осіб до розподільчих щитів з встановленими установками KNX (наприклад, завжди замкненими або розташованими в замкнених приміщеннях)?

 Чи важко отримати доступ до пристроїв у зовнішніх зонах? (наприклад, встановлений на достатній висоті)?

 У разі, якщо установкою KNX можна управляти з місць у громадських будівлях і не під наглядом, чи замислювалися ви про використання двійкових входів (вмонтованих в розподільних щитах) або кнопкові інтерфейси?

 Чи захищені панелі KNX Touch паролем (режим користувача, групи чи гостя)?

2. Чи використовується вита пара як засіб спілкування?

    Чи захищений кабель у будь-якому місці будинку чи будівлі або поза ним

    проти несанкціонованого доступу?

    Якщо кабель витої пари використовується в місцях, де потрібні додаткові заходи захисту, чи вжили ви заходів, зазначених у пункті 6?

    Чи використовується Powerline як засіб спілкування?

    Чи встановлено смугові фільтри?

    Якщо Powerline також використовується поза будівлею, чи вжили ви ті самі заходи для медіа-з'єднувача, як зазначено в пункті 6?

3. Чи використовується IP як засіб зв'язку?

    Налаштування мережі задокументовано та передано власнику будинку або адміністратор локальної мережі?

    Чи були налаштовані комутатори та маршрутизатори таким чином, щоб відомі лише MAC-адреси

    чи можете отримати доступ до засобу зв'язку?

    Чи використовується окрема мережа LAN або WLAN з власним обладнанням для зв’язку KNX?

 Чи доступ до IP-мереж (KNX) обмежений уповноваженими особами через відповідні імена користувачів і надійні паролі?

 Для зв’язку KNX IP Multicast слід використовувати іншу IP-адресу як адресу за замовчуванням (як правило, 224.0.23.12). Чи була змінена ця адреса багатоадресної IP-адреси?

 Чи було змінено SSID за замовчуванням точки бездротового доступу? Була періодична передача SSID після встановлення деактивовано?

 Порти маршрутизаторів для KNX були закриті для доступу до Інтернету та були шлюзом за замовчуванням використаний маршрутизатор KNXnet/IP встановлено на 0? Чи була інсталяція (W)LAN захищена відповідним брандмауером?

 Якщо для встановлення KNX потрібен доступ до Інтернету, перевірте можливість реалізації:

- Встановлення VPN-з'єднання з Інтернет-роутером
- Встановлення специфічних для виробника KNX Object Servers

4. Чи використовується радіочастота як засіб спілкування?

 Чи вжили ви ті самі заходи для медіа-з’єднувача, як зазначено в пункті 6?

 Чи кожен домен РФ має різну адресу домену?

 Чи використовували ви стяжки в установці?

 Чи були призначені окремі адреси пристроїв відповідно до їх місця в топології?

 Чи можна запобігти за допомогою налаштування відповідних параметрів у муфтах що неправильні адреси джерела не пересилаються за межі рядка?

 Чи блокуєте ви зв'язок "точка-точка" і широкомовний зв'язок через з'єднувачі?

- Чи правильно завантажено таблиці фільтрів та чи виконано налаштування таким чином, щоб таблиці фільтрів враховувалися з'єднувачами?

5. Чи були заблоковані пристрої проти переконфігурації?
   - Якщо ні, введіть ключ BCU 1 у проекті ETS ПК (USB, зовнішній жорсткий диск, …).
   - Плагіни та програми ETS бажано встановлювати до встановлення
   - Створіть резервну копію файлу проекту після встановлення (в ідеалі на захищеному USB-накопичувачі, який безпечно зберігається) і видаліть проект з ПК.
   - Чи оновлена прошивка використовуваних пристроїв?
6. Подальші заходи щодо конфіденційності (GDPR)
   - Установник і замовник повинні підписати декларацію про конфіденційність.
   - Для виконання правил GDPR установник повинен передати копію файлу проекту ETS до замовника. [2]

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення захисту обміну технологічними даними між KNX -пристроями, встановлена сутність завдань їх захисту. Встановлено сутність та зміст управління захистом обміну технологічними даними між KNX –пристроями на підприємстві.

Проаналізовано існуючі технології захисту обміну технологічними даними між KNX-пристроями Досліджена технологія управління захистом обміну технологічними даними між KNX -пристроями підприємства на базі KNX-Secure/IPSecure.

Визначено методи та засоби забезпечення стану захищеності технологічних даних у KNX –системах SCADA.

Встановлено основні функції та принципи роботи протоколу KNX. Платформа ETS5 – це набір продуктів, який забезпечує швидке та інтуїтивно зрозуміле рішення для побудови системи автоматизації на базі обладнання будь-яких виробників, що підтримує протокол KNX, та дозволяє використовувати широкий спектр технологій захисту обміну технологічними даними між KNX -пристроями.

Досліджено типову архітектуру рішення KNX, яка надає уявлення про середовище платформи та можливість її правильного планування застосування.

У роботі запропоновано варіант технології захисту обміну технологічними даними між KNX -пристроями. для цього було розглянуто приклад робочої системи автоматизації на підприємстві з використанням KNX структури.

У роботі розглянуто додаткові можливості захисту новітнього програмного забезпечення для роботи з KNX – ETS6.

Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології управління захистом обміну технологічними даними між KNX -пристроями.

Таким чином, правильна реалізація технології управління захистом обміну технологічними даними між KNX -пристроями має забезпечити ефективний захист даних та кібербезпеку інформаційної та виробничої системи підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Хакерские атаки на KNX [Електронний ресурс] // zennio. – 2021. – Режим доступу до ресурсу: https://zenniorussia.ru/informacziya/publikaczii/xakerskie-ataki-na-knx.html?fbclid=IwAR1wI9sIFmcwUz49NKasp4FrATSTB7QvsjJTGTOSYfTI_YOaN8iMk-k48xs
2. KNX Secure is there to use [Електронний ресурс] // knx. – 2021. – Режим доступу до ресурсу: https://www.knx.org/knx-en/for-professionals/benefits/knx-secure/
3. The main features of ETS6 [Електронний ресурс] // zennio. – 2021. – Режим доступу до ресурсу:https://www.ets6.org/12-main-characteristics-of-ets6/
4. Николаев П. Какие бывают "умные дома". Обзор. [Електронний ресурс] / Павел Николаев // BeSmart. – 2019. – Режим доступу до ресурсу: http://www.besmart.su/article/kakie-byvayut-umnye-doma.
5. Экономия с системами Умный дом [Електронний ресурс] // BeSmart. – 2018. – Режим доступу до ресурсу: http://www.besmart.su/article/ekonomia_s_umnim_domom.
6. BMS: преимущества комплексной автоматизации зданий [Електронний ресурс] // Commercial Property. – 2019. – Режим доступу до ресурсу: https://commercialproperty.ua/cp-articles/bms-preimushchestva-kompleksnoy-avtomatizatsii-zdaniy/.
7. Ярочкин В. И. Информационная безопасность. Учебное пособие для студентов непрофильных вузов. / В. И. Ярочкин. – Москва, 2000.
8. Мельников В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. – Москва, 2003.

9. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – Москва, 1996.
10. Department of Defense Trusted Computer System Evaluation Criteria, TCSEC: 5200.28-STD. – Введ. 1985.12.26 – Department of Defense, 1985.
11. KNX eCampus ETS5 [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. — Режим доступу: https://wbt5.knx.org/. – Назва з екрана.
12. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – Київ, 2002.
13. Наговицин А.И., Севрюков А.Г. Робототехнические комплексы военного назначения, опыт и перспективы их применения в РВиА СВ // Известия Южного федерального округа, – 2016, – с. 197-210.
14. Сашников Т.К. К вопросу обеспечения информационной безопасности беспилотных авиационных систем с летательными аппаратами малого и лёгкого класса в специализированных АСУ // Журнал T-Comm - Телекоммуникации и Транспорт, – 2013, №6, – с. 71-72.
15. Таненбаум Е. Компьютерные сети / Ендрю Таненбаум. – Санкт-Петербург: Издательский дом «Питер», 2014. – 992 с.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)