В.А.ВИШНЯКОВ[1], С.С.ГОЛУБЦОВ[2]

«ТЕХНИЧЕСКИЕ РЕШЕНИЯ, СИСТЕМНОЕ И ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРИ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ «УМНЫЙ ДОМ» НА ОСНОВЕ ПРОТОКОЛА KNX»

[1]Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, профессор, кандидат технических наук, доцент.

[2]Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь, педагог дополнительного образования

Актуальность исследования обусловлена стремительным распространением технологий автоматизации зданий («Умный дом»), которые, наряду с повышением комфорта и энергоэффективности, создают новые уязвимости для кибератак. Оперативный обмен данными по сетям делает системы управления зданием потенциальной мишенью для злоумышленников, что может привести к потере конфиденциальности, материальному ущербу и даже угрозе безопасности людей. В этих условиях обеспечение информационной безопасности (ИБ) становится критически важной задачей, а международный стандарт KNX, как одна из наиболее распространенных технологий, требует тщательного анализа своих защитных механизмов.

Объектом исследования является технология KNX и потенциальные факторы риска для информационной безопасности систем автоматизации на ее основе.

Предметом исследования выступают технические и программные решения, обеспечивающие информационную безопасность в системах автоматизации, соответствующих протоколу KNX.

Цель работы – анализ, обоснование и выбор наиболее оптимальных технических и программных решений, обеспечивающих информационную безопасность систем автоматизации в соответствии с протоколом KNX.

Для достижения цели были решены следующие задачи:

Проведен обзор предпосылок возникновения и развития международного стандарта KNX.

Выполнен подробный анализ технических особенностей протокола KNX, включая среды передачи данных (витая пара, силовая линия, радиоканал, IP-сеть), топологию и элементы системы.

Систематизированы потенциальные киберугрозы для систем автоматизации на базе KNX.

Проанализированы и обоснованы наиболее эффективные способы противодействия киберугрозам с использованием решений KNX Secure.

Методы исследования: В работе применялись методы анализа научно-технической литературы и стандартов, системный анализ архитектуры KNX, сравнительный анализ механизмов безопасности, а также практическое изучение функционирования системы с помощью универсального программного обеспечения для проектирования ETS (Engineering Tool Software).

Основные результаты и выводы:

Проведен комплексный анализ технологии KNX, подтвердивший ее преимущества как открытого, гибкого и отказоустойчивого стандарта для построения систем автоматизации различного масштаба.

Выявлены и классифицированы ключевые угрозы информационной безопасности систем «Умный дом» на базе KNX, такие как несанкционированный доступ, перехват и манипуляция телеграммами, отказ в обслуживании (DoS-атаки).

Детально исследованы и рекомендованы к применению современные механизмы защиты, реализованные в рамках концепции KNX Secure:

KNX IP Secure – обеспечивает сквозное шифрование и аутентификацию всего трафика данных, передаваемого по IP-сетям (Ethernet, Wi-Fi), что критически важно для защиты от удаленных атак.

KNX Data Secure – обеспечивает шифрование и аутентификацию данных на уровне шинных телеграмм, защищая коммуникации между устройствами внутри сегментов KNX (витая пара, радио), в том числе от локального вмешательства.

Сформулированы практические рекомендации по созданию безопасных систем автоматизации, включая необходимость сегментации сети, использования аппаратных брандмауэров, физической защиты инфраструктуры и обязательного применения KNX Secure на объектах с повышенными требованиями к ИБ.

Теоретическая и практическая значимость работы. Результаты исследования вносят вклад в развитие методов защиты систем автоматизации зданий. Теоретическая ценность заключается в систематизации угроз и защитных механизмов для протокола KNX. Практическая значимость заключается в том, что выводы и рекомендации работы могут быть использованы:

Проектировщиками и системными интеграторами для создания более безопасных и надежных решений.

Инсталляторами для грамотного ввода в эксплуатацию защищенных систем.

Конечными заказчиками для формирования обоснованных требований к информационной безопасности при внедрении систем «Умный дом».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об утверждении Государственной программы развития цифровой экономики и информационного общества на 2016 – 2020 годы: постановление Совета Министров Республики Беларусь, 23 марта 2016 г., № 235: в ред. от 09.11.2018 . [Электронный ресурс].

2. Об утверждении Концепции информационной безопасности Республики Беларусь: Постановление Совета Безопасности Республики Беларусь, 18 марта 2019 г., № 1. [Электронный ресурс].

3. Жогов Николай. Основа единства «умного дома». Обзор стандарта KNX. [Электронный ресурс].

4. Пасеков В. Европейская платформа автоматизации зданий KNX: плюсы и минусы технологии // Автоматизация зданий: информационный бюллетень. 2011. №10 (51) декабрь.

5. Пасеков В. Описание платформы автоматизации зданий KNX. [Электронный ресурс].