***В.С. Толстогузов, А.А. Оленников***

*Тюменский государственный университет, г. Тюмень*

**УДК 004.942**

# РАЗРАБОТКА ВИРТУАЛЬНОГО ТРЕНАЖЕРА АВТОМАТИЗИРОВАННОГО ТЕПЛОВОГО ПУНКТА

**Аннотация.** Объектом исследования данной статьи является технология работы индивидуального автоматизированного теплового пункта и виды атак на оборудование и узлы систем автоматизации.

**Ключевые слова:** индивидуальный тепловой пункт, АСУ ТП, схема теплоснабжения, сетевая атака, трубопроводы.

Важнейшей задачей современных ТЭЦ и котельных является предоставление теплоносителя для отопления и горячего водоснабжения с максимальной эффективностью и минимальной себестоимостью.

Данного эффекта невозможно добиться без современных средств управления и автоматизации, которые требуют с одной стороны, безотказности аппаратной части, с другой стороны вмешательства посторонних лиц в технологию работы.

Целью данной работы является разработка виртуального тренажер для моделирования режимов работы индивидуального теплового пункта с учетом воздействия атак на узел учета тепловой энергии и систему управления погодным регулированием.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Разработать алгоритм работы ИТП, с закрытой системой отопления и независимым подключением горячего водоснабжения.
2. Разработать модели и алгоритмы атак на узлы автоматизации ИТП.
3. Разработать виртуальный тренажер.
4. Провести тестирование и отладку разработанного приложения.

**Системы ИТП и схемы их подключения:**

Тепловой пункт – это высокотехнологичное оборудование представляет собой сложную установку для передачи теплоэнергии от наружных теплосетей (котельных, ТЭЦ или РТС) во внутреннюю систему отопления, водоснабжения и вентиляции [1].

Основной целью теплового пункта поддержание необходимого уровня давления и температуры в различных системах и коммуникациях, а также предотвращение возможных аварий из-за перепадов температуры и давления.

Индивидуальный тепловой пункт имеет следующие виды тепловых нагрузок:

Система горячего водоснабжения (ГВС) предназначена для снабжения потребителей горячей водой. Различают закрытые и открытые системы горячего водоснабжения.

Система отопления предназначена для обогрева помещений с целью поддержания в них заданной температуры воздуха. Различают зависимые и независимые схемы присоединения систем отопления.

В данной работе будет рассмотрена закрытая система теплоснабжения с независимым подключением ГВС, приведенная на рисунке 1.

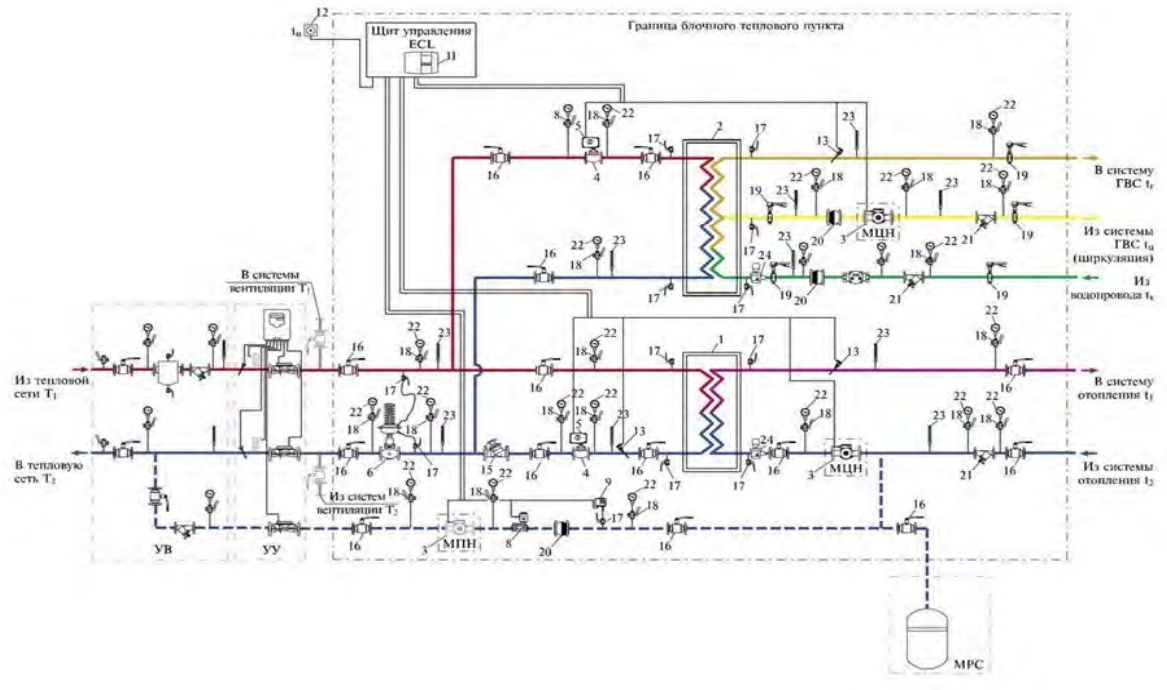


*Рис. 1.* ИТП, закрытая СО с независимым подключением ГВС

**Принцип работы:**

Рассмотрим принцип работы ИТП, с закрытой СО и независимым подключением ГВС.

Теплоэлектроцентраль или котельные, как источники тепла, нагревают теплоноситель, далее по магистральным сетям он поступает в тепловой пункт. На входе устанавливается фильтры и грязевики, контрольно-измерительное оборудование, которое определяет параметры теплоносителя.

Температура теплоносителя и давление от ТЭЦ, как правило, не соответствует параметрам по СанПиН и устанавливается самим ТЭЦ исходя из климатических условий обусловлено это тем, что тепловые сети городов имеют большую протяженность и неоднородную топологию, вследствие чего потребители тепловой энергии удалены от источника тепловой энергии на различные расстояния. Кроме того, тепловые нагрузки потребителей также отличаются друг от друга.

Воду при различных условиях с высокой температурой подавать в системы отопления здания и ГВС нельзя, так как температура в ГВС и систем отопления должна варьироваться от 55 до 60 $^{o}$C из-за превышения этой температуры могут произойти нежелательные последствия такие как ожоги [2]. Следовательно, необходимо понижать температуру теплоносителя. В данной работе это возможно реализовать, используя теплообменники. Таким образом, вода из тепловой сети циркулирует через теплообменник, нагревая внутренний контур.

При необходимости на входе в тепловой пункт устанавливается регулятор давления, который понижает исходное давление теплоносителя. Условное давление варьируется от 0,2 до 0,5 Мпа [2]. Помимо очистного оборудования в тепловых пунктах устанавливают системы водоподготовки, чтобы продлить срок службы всего оборудования расположенного как на источниках приготовления тепла, так и на стороне абонентов. К тому же вода для горячего водоснабжения должна пройти специальный этап очистки. На данном этапе корректируется жесткость воды и содержание химических примесей, влияющих на коррозию [3].

Тепловой пункт работает по закрытой системе отопления с независимы подключении контура ГВС, таким образом в технологической линейке появляться 2 теплообменника для отопления и ГВС. Тип теплообменника, его мощность и конструкция подбираются исходя из требуемой мощности теплового пункта.

Циркуляция теплоносителя в системе осуществляется насосными группами. Количество насосных групп и их производительность так же подбираются исходя из требуемой производительности теплового пункта.

Согласно современной нормативно-технической документации проектируемы или реконструируемые ИТП должны быть полностью автоматизированы. В настоящее время появляется все больше тепловых пунктов управляемы дистанционно.

**Разработка моделей и алгоритмов атак:**

В последнее время участились APT атаки на промышленность. Так в 2019 году «Positive Technologies» проанализировали поведение 22 APT-группировок, атаковавших российские организации на протяжении последних двух лет. Среди целей этих группировок множество организаций, входящих в списки крупнейших компаний России и являющихся лидерами в своих отраслях статистика таких атак приведена на рисунке выше [4].

Поэтому необходимо обратить внимание на АИТП, так как на территории объектов каждый день находятся люди, которые могут пострадать вследствие атаки.

Алгоритмы атак:

Атака 1. Коррекция температурной карты в результате вмешательства непосредственно в блок погодного регулирования.

Алгоритм:

1. Злоумышленник атакует преобразователь интерфейсов, сопряженный с контроллером управления погодным регулированием.
2. Искусственно корректируются данные температурной карты.
3. Возникает, перегрев или недогрев подаваемой воды в здание.

4. Датчики температуры передают неверные сигналы на контроллер;

5. Возникают штрафы за неиспользованную тепловую энергию и нарушается СанПИН.

Результат: в данной ситуации люди могут получить ожоги, а тепловая система может стать не пригодной к дальнейшей эксплуатации, также были получены штрафы за чрезмерное сжигание топлива.

Атака 2. Диспетчер не видит, что происходит с системой ИТП в реальном времени.

Алгоритм:

1. Злоумышленник атакует контроллер, забивая Ethernet порт.

2. Возникает, перегрев или недогрев подаваемой воды в здание.

3. Датчики температуры передают данные, а контроллер не реагирует на эти данные.

4. Возникают штрафы за неиспользованную тепловую энергию и нарушается СанПИН.

Результат: в данной ситуации люди могут получить ожоги, а тепловая система может стать не пригодной к дальнейшей эксплуатации, также были получены штрафы за чрезмерное сжигание топлива.

Атака 3. Прекращение подачи воды в ИТП

Алгоритм:

1. злоумышленник атакует интерфейс контроллера RS-485, получая доступ к оборудованию;

2. злоумышленник закрывает запирающую арматуру

3. отключает все датчики системы водоснабжения

4. в связи с тем, что система перестает функционировать должным образом, она может выйти из строя

Результат: тепловая система может стать не пригодной к дальнейшей эксплуатации, а люди, находящиеся в холодный период времени на территории объекта, могут получить обморожения.

**Заключение**

- Рассмотрены схемы ИТП и типы их подключения, также продемонстрирован принцип работы АИТП.
- Разработана модель и алгоритм атаки на тепловые пункты, представлены возможные последствия.

В дальнейшем планируется реализовать виртуальный тренажер, а также разработать дополнительные алгоритмы атак.

## СПИСОК ЛИТЕРАТУРЫ

1. Тепловые пункты в тепловых сетях [Электронный ресурс]. – Режим доступа: https://proteplo.org/blog/teplovoi-punkt (дата обращения: 14.05.2021).

2. СП 41-101-95 Проектирование тепловых пунктов.

3 СП 60.13330.2016 Отопление, вентиляция и кондиционирование воздуха. Актуализированная редакция СНиП 41-01-2003 (с Изменением N 1): Министерство строительства и жилищно-коммунального хозяйства Российской Федерации от 16 декабря 2016 № 60.13330.2016 // Официальное издание. – М.: Стандартинформ, 2017.

4 APT-атаки на промышленные компании в России: обзор тактик и техник [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-industry-2019/ (дата обращения: 16.05.2021).