УДК 004.318

МОДЕЛИРОВАНИЕ АСУ ТП ОБЪЕКТА НЕФТЕДОБЫЧИ В КОНТЕКСТЕ УПРАВЛЕНИЯ РИСКАМИ ИБ

А. В. Слинин

nags.09@yandex.ru

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Аннотация. В последние несколько лет наблюдается резкий рост актуальности проблемы обеспечения кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов. Осуществляется моделирование АСУ ТП первичного пункта сбора нефти.

Ключевые слова: автоматизированная система управления, кибербезопасность, моделирование, уровни безопасности.

Первичный пункт сбора нефти (ППСН) является частью промышленной системы, которая осуществляет сбор нефти на месторождениях. С целью автоматизации управления технологическими процессами на ППСН, а также для мониторинга работы оборудования ППСН применяются АСУ ТП.

Для того чтобы обеспечить защиту АСУ ТП, необходимо произвести моделирование объекта защиты, выделить активы, идентифицировать угрозы и уязвимости, оценить риски информационной безопасности. Затем, на основании полученных результатов, выбрать и применить контрмеры, необходимые для нейтрализации угроз. В рамках данной работы рассматривается этап моделирования объекта защиты на основе стандарта ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели» [1].

Согласно стандарту ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 [1], моделирование объекта защиты включает в себя разработку 4 моделей:

1. Базовая модель.
2. Объектная модель.
3. Базовая архитектура.
4. Зональная модель.

Базовая модель (рис. 1) характеризует АСУ ТП, представляя ее в виде логических уровней, каждый из которых соответствует определенному виду деятельности.

На основе базовой модели на следующем этапе строится *объектная модель* (рис. 2), которая отражает основные объекты АСУ ТП, взаимодействие с сетями и подразделениями, которые участвуют в технологических процессах и присутствуют на различных уровнях иерархии.

Следующим шагом в процессе моделирования АСУ ТП является построение модели *базовой архитектуры* (рис. 3), которая отражает все основные элементы АСУ ТП, в том числе телекоммуникационное оборудование и линии связи, строится на основе объектной модели.

Заключительным этапом моделирования является построение *зональной модели* (рис. 4), которая разделяет объект защиты на отдельные зоны – группы логических или физических объектов в пределах предприятия, объединенные по общим характеристикам (требования безопасности, критичность для ТП и т.д.).

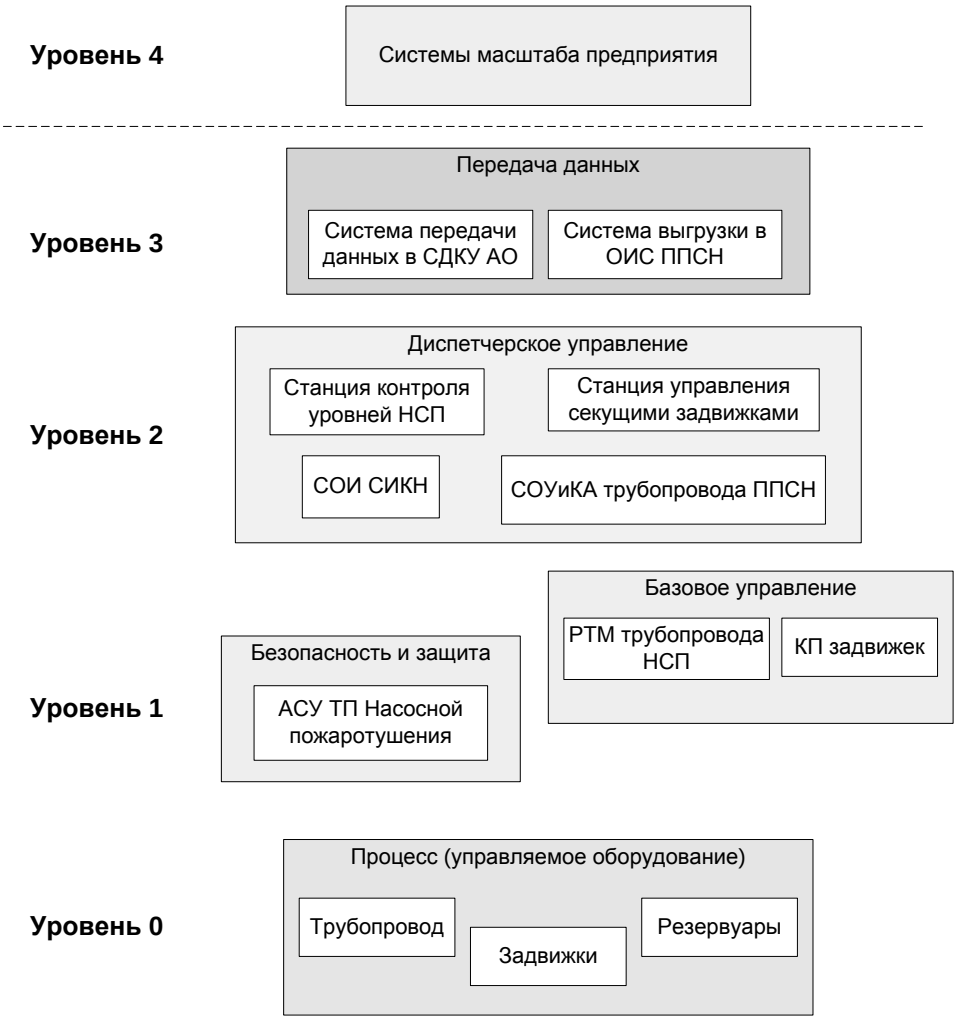

Рис. 1. Базовая модель объекта защиты

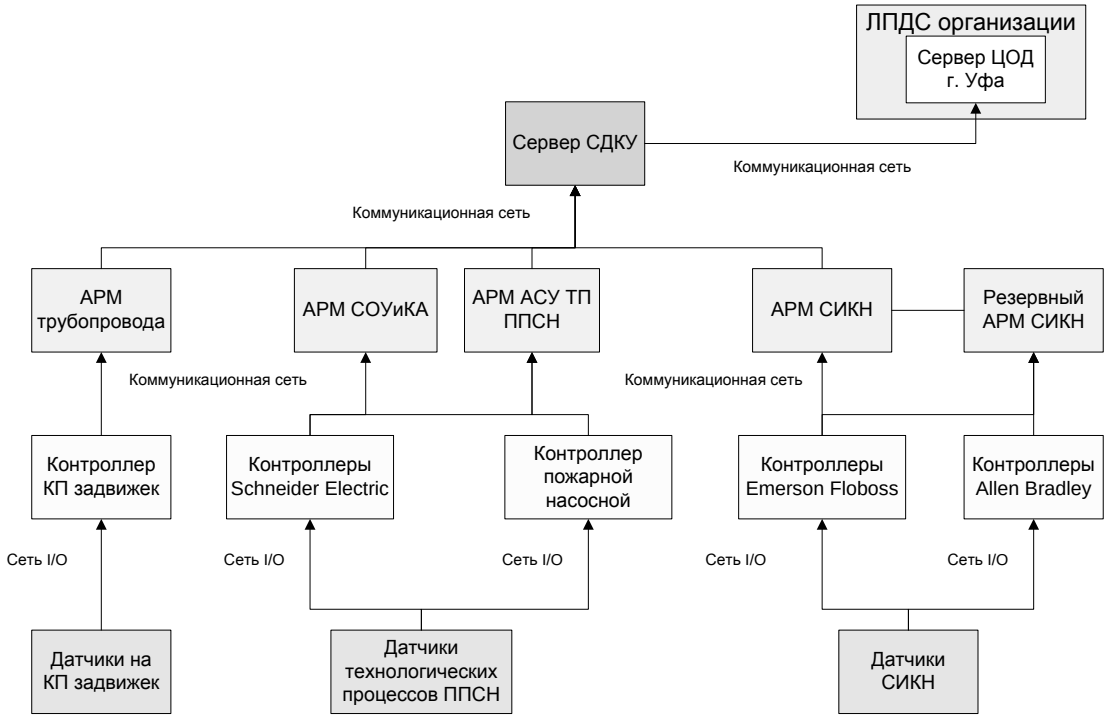

Рис. 2. Объектная модель

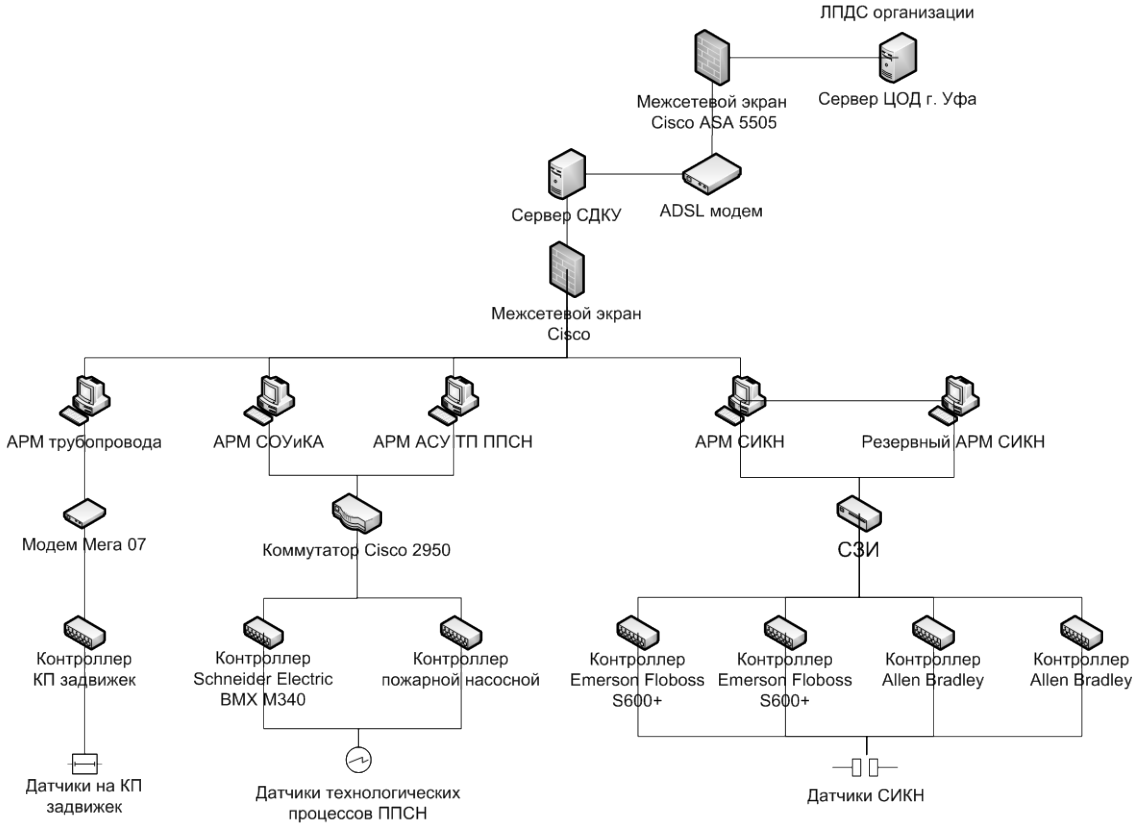

Рис. 3. Базовая архитектура

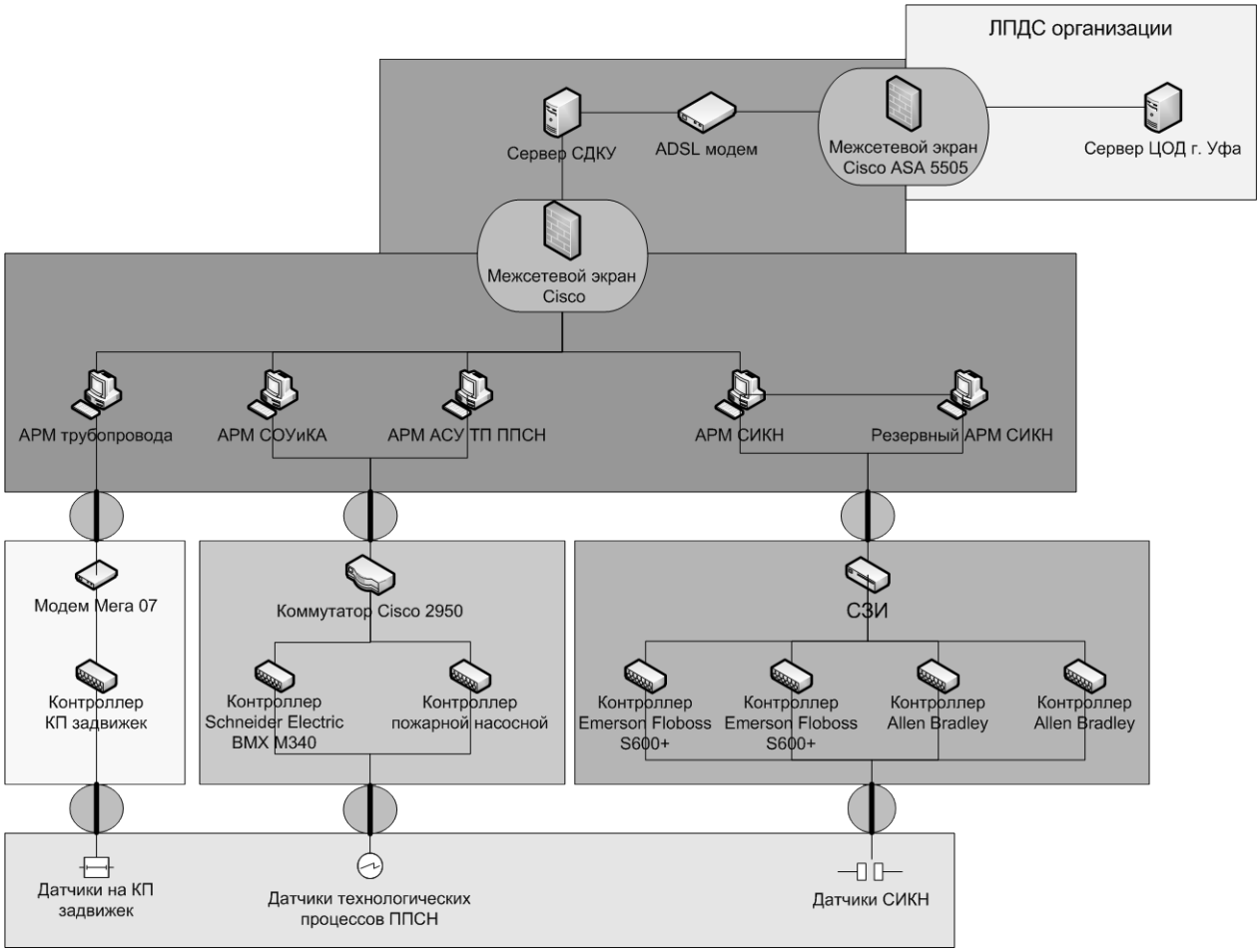

Рис. 4. Зональная модель

Как видно на рис. 4, объект защиты разделен на 7 зон безопасности: зона датчиков, зона управления задвижками, зона управления технологическими процессами ППСН, зона управления СИКН (система измерения количества нефти), зона критических устройств управления, зона сервера, зона ЛПДС (линейная производственно-диспетчерская станция) организации.

На основании полученной *зональной модели* на следующей стадии осуществляется детальная оценка рисков ИБ, которая включает в себя подробный анализ угроз и уязвимостей устройств в зоне критических устройств управления, т.к. к ней предъявляются наиболее строгие требования безопасности. Оценка рисков ИБ в выбранной зоне будет производиться на основе нечеткой нейронной сети (ANFIS). Результаты данной стадии ложатся в основу формирования перечня контрмер, необходимых для нейтрализации угроз.

Исследование показало следующее:

Моделирование АСУ ТП в контексте управления рисками ИБ сводится к описанию и составлению «общей картины» защищаемой системы. В рамках данного процесса происходит поэтапное построение моделей. Результатом моделирования является зональная модель, логически разделяющая систему на группы с соответствующим уровнем безопасности. Необходимо уделять особое внимание проведению данного этапа в контексте управления рисками ИБ, так как ошибки, допущенные при моделировании, станут причиной неэффективности дальнейшей оценки рисков.

Данная работа выполнена при поддержке гранта РФФИ-Поволжье № 17-48-020095.

СПИСОК ЛИТЕРАТУРЫ

1. **ГОСТ** Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели». **[** *Industrial communication networks. Network and system security. Part 1-1. Terminology, concepts and models.* IEC/TS 62443-1-1:2009, 2009. **]**

ОБ АВТОРЕ

СЛИНИН Андрей Владимирович, магистрант. каф. ВТиЗИ.

METADATA

Title: Modeling of the oil production automated process control system in the risk management context

Authors: A. V. Slinin

Affiliation: Ufa State Aviation Technical University (UGATU), Russia.

Email: nags.09@yandex.ru

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), no. 1 (20), pp. 170-173, 2019**.** ISSN 2225-9309 (Print).

Abstract: In the past few years, there has been a sharp increase in the relevance of the problem of ensuring the cybersecurity of automated process control systems of industrial facilities. In this article, the simulation of the automated control system for the primary oil recovery station is carried out.

Key words: automated control system, cybersecurity, modeling, security levels.

About author:

SLININ, Andrey Vladimirovich., master student 2 year, Ufa state aviation technical University