УДК 004.056

ИНФОРМАЦИОННАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ СИСТЕМ ВЕРХНЕГО УРОВНЯ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

Акимов Н.Н., Кольцов В.А., Павлин А.Ю.

Филиал федерального государственного унитарного предприятия «Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики» «Научно-исследовательский институт измерительных систем им. Ю.Е. Седакова»

(Нижний Новгород, Российская Федерация)

Аннотация. Работа посвящена описанию системы поддержки принятия решений при обеспечении кибербезопасности системы верхнего уровня автоматизированной системы управления технологическими процессами атомной электростанции (СВУ АСУ ТП АЭС). Алгоритм поддержки принятия решений позволяет найти и ранжировать предпочтительные конфигурации средств защиты информации.

Ключевые слова: поддержка принятия решений, кибербезопасность, АСУ ТП, система верхнего уровня, АЭС.

INFORMATION SYSTEM FOR DECISION SUPPORT IN ENSURING THE CYBERSECURITY OF UPPER-LEVEL SYSTEMS OF NUCLEAR POWER PLANTS

Nikolay N. Akimov, Vyacheslav A. Koltsov, Artem J. Pavlin

Branch of Federal State Unitary Enterprise "Russian Federal Nuclear Center – All-Russian Research Institute of Experimental Physics" "Research Institute of Measuring systems named after Yu.Ye. Sedakov"

(Nizhny Novgorod, Russian Federation)

Abstract. The work is devoted to the description of the decision support system for ensuring the cybersecurity of the upper level system of the automated control system for technological processes of a nuclear power plants (ULS APCS NPP). The decision support algorithm allows you to find and rank the preferred configurations of information security.

Keywords: decision support, cybersecurity, APCS, upper-level system, NPP.

Введение

В настоящее время в атомной энергетике предъявляются высокие требования по кибербезопасности систем верхнего уровня (СВУ) автоматизированной системы управления технологическими процессами (АСУ ТП) атомной электростанции (АЭС). Обеспечение кибербезопасности СВУ АСУ ТП АЭС регламентируется обширной международной и национальной (российской) нормативной базой [1,2]. Основными нормативными документами являются приказы ФСТЭК и стандарты международной электротехнической комиссии:

- приказ ФСТЭК России № 31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
- приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию системы безопасности значимых объектов КИИ РФ и обеспечение их функционирования»;
- приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»;
- IEC 62645:2014 Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems.

Информационная система поддержки принятия решений разработчиком при обеспечении кибербезопасности СВУ

Техническое задание на проектирование СВУ включает требования по обеспечению кибербезопасности в соответствии с одним или несколькими нормативными документами,

классом защищенности автоматизированной системы управления, которые определяют совокупность мер, составляющих искомую конфигурацию средств защиты [3]. Контекстная диаграмма А0 прототипа системы поддержки принятия решений приведена на рис. 1.

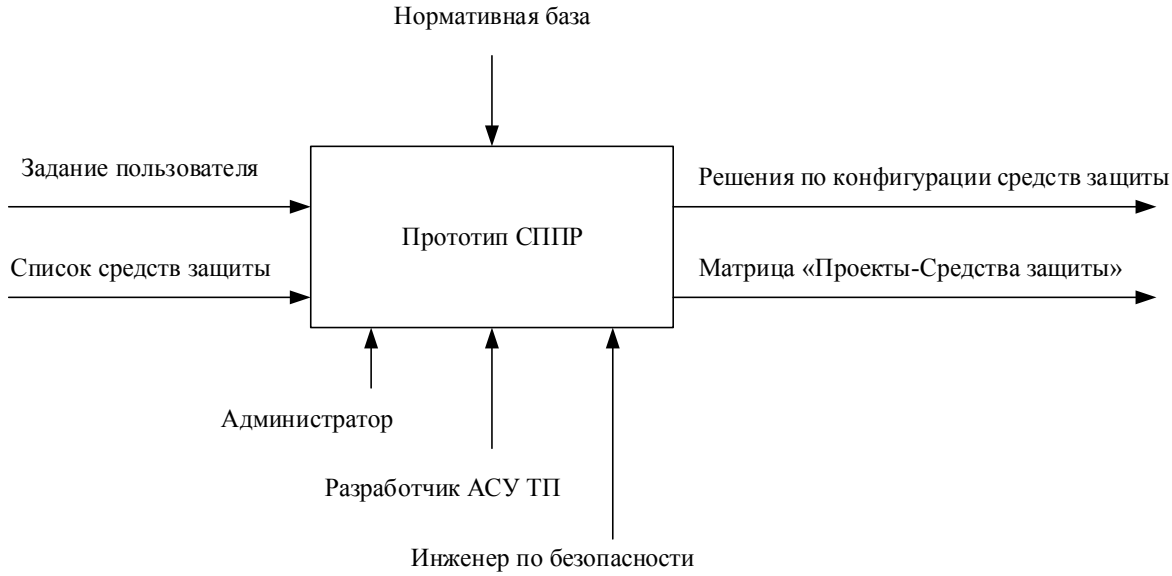

Рис.1. Контекстная диаграмма А0 прототипа системы поддержки принятия решений

Проектирование с учетом обеспечения кибербезопасности СВУ АСУ ТП АЭС заключается в выборе совокупности средств защиты, покрывающих все меры, определенные нормативным документом. Для поддержки жизненного цикла проектирования информационно-управляющих систем [4] и автоматизации процесса определения конфигурации средств защиты информации выполняется разработка системы поддержки принятия решений (СППР). Основу СППР составляют алгоритмы, позволяющие формализовать показатели качества конфигураций средств защиты.

Функции, выполняемые СППР:

- формализация мер безопасности согласно нормативной документации;
- формирование и ведение реестра средств защиты;
- формирование и ведение реестра подтверждающих документов;
- формирование и ведение реестра проектов;
- автоматизация процесса покрытия мер безопасности средствами защиты;
- расчет оптимальной конфигурации покрытия средствами защиты мер безопасности (по стоимости и защищенности);
- формирование отчетной документации.

В СППР реализованы несколько ролей пользователей для обеспечения разграничения прав:

- администратор (управление учетными записями пользователей);
- руководитель проектов (осуществляет верификацию и валидацию проектов);
- инженер по безопасности (ввод мер по обеспечению безопасности и средств защиты);
- инженер-разработчик АСУ ТП (создание и редактирование сведений о проекте, определение состава средств защиты конфигураций и автоматизированный выбор их конфигураций).

Структура СППР приведена на рис. 2.

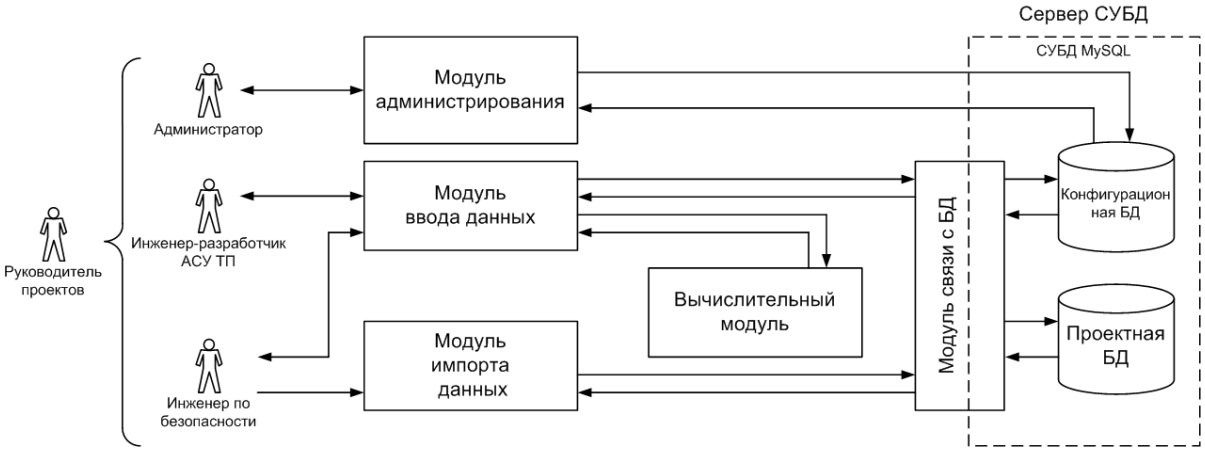

Рис.2. Структура СППР

Множество допустимых конфигураций средств защиты составляют те меры, которые обеспечивают защищенность объекта защиты. Условие защищенности является выполненным при наличии в k-й конфигурации средства защиты для каждой меры. Некоторую k-ю конфигурацию средств защиты определим, как вектор

$$\mathrm{v}_k = [v_{1k}, \quad v_{2k}, \quad \dots \quad v_{Nk}]^{\mathbf{T}} \tag{1}$$

с компонентами $v_{nk} = \begin{cases} 1, \text{ если средство } n \text{ используется в -й конфигурации;} \\ 0, \text{ если средство } n \text{ не используется } k\text{-й конфигурации,} \end{cases}$

где T – транспонирование вектора;

$n = \overline{1, N}$– средства защиты.

Тогда стоимость совокупности средств защиты, соответствующих k-й конфигурации определяется выражением

$$C_{\boldsymbol{k}} = \sum_{n=1}^{N} v_{nk} c_{\boldsymbol{n}} = \mathrm{c}^{\mathrm{T}} \mathrm{v}_k, \tag{2}$$

где $c_n = [c_1, \quad c_2, \quad \dots \quad c_N]^{\mathbf{T}}$ – вектор стоимостей средств защиты;

T – транспонирование вектора.

Условие защищенности является выполненным при наличии в k-й конфигурации средства защиты для каждой меры. Для проверки условия защищенности введем вектор

$$\mathrm{a}_{mk} = D\, \mathrm{v}_k, \tag{3}$$

где a_{mk} – вектор средств защиты для каждой меры;

D – количество средств защиты.

компоненты которого равны количеству средств, покрывающих соответствующие меры.

Компоненты вектора

$$a_{mk} = [a_{1k}, \quad a_{2k}, \quad \dots \quad a_{Mk}]^{\mathbf{T}}, \tag{4}$$

где $m = \overline{1, M}$;

T – транспонирование вектора.

равны количеству средств, покрывающих соответствующие меры.

Условие защищенности выполняется (защищенность обеспечена), если для k-й конфигурации средств защиты

$$a_{mk} \geq 1, m = \overline{1, M}. \tag{5}$$

Представим условие защищенности в виде

$$s_k \geq 1, \tag{6}$$

где

$$S_k = \min_{m=\overline{1,M}} a_{mk} \tag{7}$$

Условие защищенности будет выполняться в случае, когда все компоненты вектора

$$a_{mk} = 1, m = \overline{1, M} \tag{8}$$

При этом каждая мера покрывается одним средством, что является достаточным для обеспечения защищенности. Если условие защищенности не выполняется, то конфигурация является недопустимой. Однако на практике ряд мер могут быть покрыты несколькими средствами, что приводит к избыточности полученного решения.

Задача поиска допустимых конфигураций средств, обеспечивающих защищенность объекта защиты, может быть представлена, как задача о нахождении столбцового покрытия булевой матрицы. Эта задача заключается в поиске множества столбцов, покрывающих все строки матрицы *D* «меры-средства». Говорят [4], что m-я строка покрывается n-м столбцом, если в m-й строке n-ого столбца стоит единица., т.е. $d_{mn} = 1$. Соответственно m-я мера покрывается n-м средством защиты. Обычно при решении задачи о покрытии булевых матриц требуется найти наименьшее столбцовое покрытие, т.е. наименьшее количество столбцов матрицы D, покрывающих все строки.

Дальнейшее развитие СППР основано на учете экспертных оценок результативностей применения средств защиты. Эти оценки определяются на основе сведений, полученных в результате удачного или неудачного применения средств защиты на эксплуатируемых АЭС. Характеристика результативности применения средства защиты определена в виде порядковой переменной, принимающей следующие значения:

A – средство применялось успешно;

B – средство ранее не применялось (новое средств

C – средство применялось и были выявлены недочеты;

D – средство снято с производства;

E – средство не рекомендовано к применению.

Очевидно, что предпочтительными являются конфигурации, в которых как можно больше средств защиты находятся в состоянии *A* (средство применялось успешно) и небольшая часть в состояниях *B* и/или *C*.

Алгоритм выбора конфигураций средств защиты приведен на рис. 3.

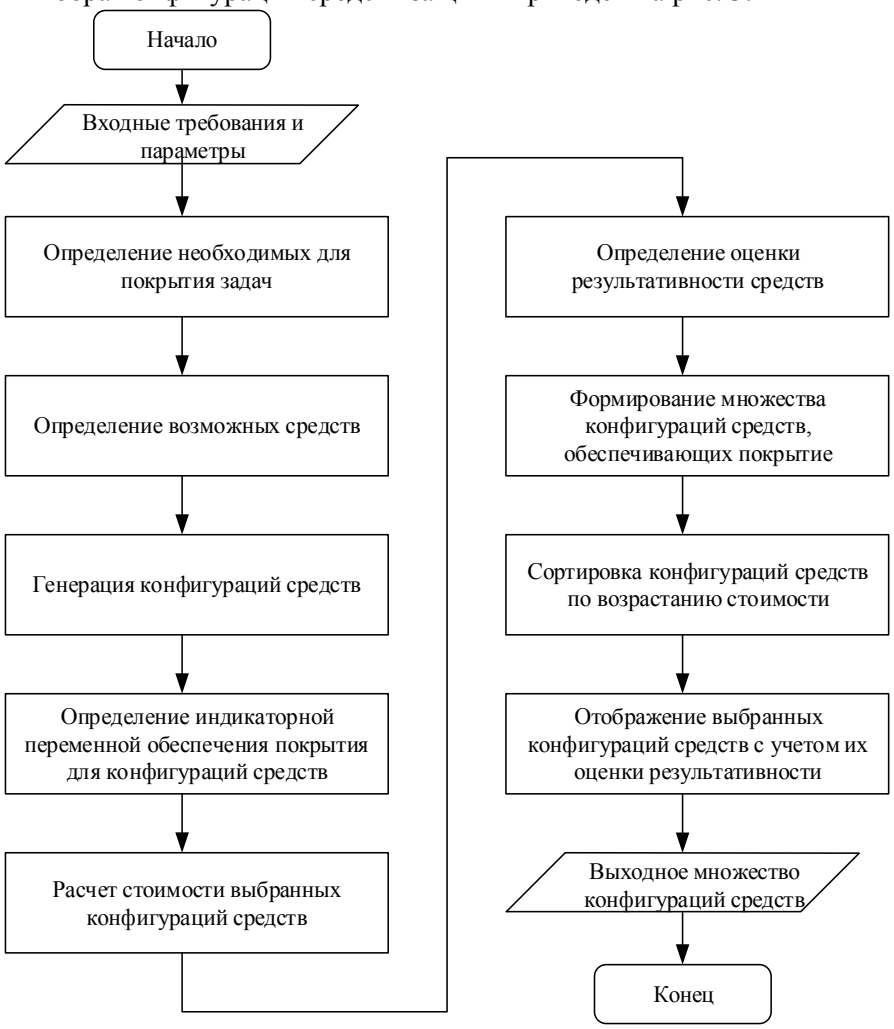

Рис.3. Алгоритм выбора конфигураций средств защиты

Для поиска оптимального решения можно применить варианты алгоритма ограниченного перебора. В качестве базового алгоритма предлагается использовать, разработанный в [5] алгоритм, в процессе функционирования которого формируется дерево перебора покрытий. Комбинирование этого алгоритма с методом ветвей и границ может составить основу для СППР при обеспечении кибербезопасности СВУ АСУ ТП АЭС.

Заключение

В результате разработанна СППР с возможностью выбора конфигураций средств защиты, обеспечивающих кибербезопасность СВУ АСУ ТП АЭС. Разработано алгоритмическое и программное обеспечение СППР, которое позволяет помочь разработчику СВУ покрыть все требуемые меры безопасности, обозначенные в нормативной документации, необходимыми средствами защиты при минимальной стоимости или максимальной защищенности. Автоматизация процесса покрытия мер безопасности способствует сокращению сроков реализации проектов, минимизации ошибок при выборе средств защиты, а также повышению информированности при формировании отчетов.

Список литературы

1. Дмитриев С.М., Акимов Н.Н., Кольцов В.А., Аспекты обеспечения кибербезопасности АСУ ТП АЭС // Информационно-измерительные и управляющие системы. 2017. № 8. С. 7-13.
2. Акимов Н.Н., Милов В.Р., Егоров Ю.С. Элементы концептуальной модели обеспечения кибербезопасности критически важных промышленных объектов // Материалы XXIV Международной научно-технической конференции «Информационные системы и технологии» (ИСТ – 2018). – Н. Новгород: НГТУ, 2018. С. 463-467.
3. Акимов Н.Н., Кольцов В.А., Павлин А.Ю., Милов В.Р., Кирбенева А.Ю. Математическая модель системы поддержки принятия решений при обеспечении кибербезопасности СВУ АСУ ТП АЭС // Сборник материалов XXVI Международной научно-технической конференции «Информационные системы и технологии» (ИСТ – 2020). – Н. Новгород: НГТУ, 2020. С. 36-40.
Методы проектирования информационно-управляющих и телекоммуникационных систем / Под ред. В.Р. Милова, В.Г. Баранова. – М.: Радиотехника, 2016. – 216 с.
4. Леончик П.В. Алгоритм поиска покрытия разреженных булевых матриц // Информатика. 2007. №2. С. 53-61.