Виталий Г. Иваненко [1], Нина Д. Иванова [2]
Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501
[2]e-mail: IvanovaND.Nina@yandex.ru, https://orcid.org/0000-0001-5942-8050

МЕТОДИКА АНАЛИЗА СТОЙКОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ ЭНЕРГОБЛОКА АЭС К ВОЗДЕЙСТВИЮ КОМПЬЮТЕРНЫХ АТАК

DOI: http://dx.doi.org/10.26583/bit.2021.4.04

Аннотация. В работе проводится разработка методики анализа стойкости автоматизированных систем управления технологическим процессом (АСУ ТП) энергоблока атомной электростанции (АЭС) к воздействию компьютерных атак, направленных на достижение исходного события аварии (целенаправленных компьютерных атак). В статье показывается необходимость рассмотрения влияния угроз безопасности информации при анализе безопасности АСУ ТП энергоблока АЭС. Рассматриваются различные методы анализа безопасности АСУ ТП энергоблока АЭС, выделяются их принципиальные недостатки: отсутствие учета фактора антропогенных угроз безопасности информации, зависимостей отказов, сложность представления результатов моделирования при большом количестве подсистем. На основе анализа существующей практики формируются требования к разрабатываемой методике. В результате разрабатывается методика анализа стойкости АСУ ТП энергоблока АЭС к воздействию целенаправленных компьютерных атак на основе применения матричных моделей оценивания рисков: матриц влияния отказов и иерархий матриц критичности. Описывается процедура анализа и моделирования компьютерных атак с использованием матриц влияния и иерархии матриц критичности. Применение методики демонстрируется на примере сегмента АСУ ТП энергоблока АЭС: с использованием иерархии матриц критичности смоделирован сценарий целенаправленной компьютерной атаки. Обосновывается целесообразность использования матриц влияния отказов и иерархии матриц критичности для моделирования целенаправленных компьютерных атак на АСУ ТП энергоблока АЭС. Научная новизна работы заключается в предложении методики анализа стойкости АСУ ТП энергоблока АЭС, учитывающей зависимость отказов и применимой для моделирования сценариев компьютерных атак. Разработанную методику возможно интегрировать в существующую практику анализа безопасности АСУ ТП энергоблока АЭС, так как матричные модели оценивания рисков являются нечетким расширением применяемого анализа вида и последствий критических отказов.

Ключевые слова: атомные электростанции, автоматизированная система управления технологическими процессами, отказы, целенаправленная компьютерная атака, иерархия матриц критичности, матрица влияния.

Для цитирования: ИВАНЕНКО, Виталий Г.; ИВАНОВА, Нина Д. МЕТОДИКА АНАЛИЗА СТОЙКОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ ЭНЕРГОБЛОКА АЭС К ВОЗДЕЙСТВИЮ КОМПЬЮТЕРНЫХ АТАК. Безопасность информационных технологий, [S.l.], т. 28, № 4, с. 52–62, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1375. DOI: http://dx.doi.org/10.26583/bit.2021.4.04.

Vitaliy G. Ivanenko[1], Nina D. Ivanova[2]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501
[2]e-mail: IvanovaND.Nina@yandex.ru, https://orcid.org/0000-0001-5942-8050

Methodology for analysing the stability of automated process control systems of nuclear power plant unit to the impact of computer attacks

DOI: http://dx.doi.org/10.26583/bit.2021.4.04

Abstract. The paper is devoted to developing a methodology for analysing the stability of Instrumentation and Control Systems (ICS) of Nuclear Power Plants (NPPs) to the impact of computer attacks aimed at producing an accident event (targeted computer attacks). The paper demonstrates the need to consider the impact of threats to information security when analysing the safety of the process control system of the NPP power unit. Various methods of safety analysis of ICS of NPPs are considered. Their fundamental shortcomings are highlighted: the lack of consideration of the factors of anthropogenic threats to information security, dependence of failures, the complexity of presentation of modelling results with a large number of subsystems. Based on the analysis of existing practices, the requirements for the developed methodology are formed. As a result, a methodology is developed for analysing the stability of ICS of NPPs to the impact of targeted computer attacks based on the use of risk assessment matrix models: failure impact matrices and criticality matrix hierarchies. The procedure for analysing and modelling computer attacks using influence matrices and a hierarchy of criticality matrices is described. The application of the method is demonstrated by the example of the ICS segment of NPP: a scenario of a targeted computer attack is modelled using the criticality matrix hierarchy. The expediency of using failure impact matrices and a criticality matrix hierarchy for modelling targeted computer attacks on the ICS of NPPs is substantiated. The scientific novelty of the study consists in the proposal of a methodology for analysing the stability of ICS of NPPs, which takes into account the dependence of failures and allows modelling scenarios of computer attacks. Since the risk assessment matrix models are an indistinct extension of the applied Failure Mode and Effects Critical Analysis, the developed methodology can be integrated into existing practices of safety analysis of the ICS of NPPs.

Keywords: nuclear power plants, instrumentation and control systems, failures, targeted computer attack, criticality matrix hierarchy, failure impact matrix.

For citation: IVANENKO, Vitaliy G.; IVANOVA, Nina D. Method for analysis of the stability of nuclear power plant systems to the impact of computer attacks. IT Security (Russia), [S.l.], v. 28, n. 4, p. 52–62, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1375. DOI: http://dx.doi.org/10.26583/bit.2021.4.04.

Введение

Современные атомные электростанции (АЭС) характеризуются широким внедрением автоматизированных систем управления технологическими процессами (АСУ ТП). При этом в АСУ ТП повсеместно используются программные и программно-технические компоненты в качестве средств автоматизации [1]. Режим функционирования АСУ ТП энергоблока АЭС может быть нарушен, в том числе, из-за компьютерных атак на программные и программно-технические компоненты АСУ ТП энергоблока АЭС [2–5]. Компьютерные атаки представляют собой целенаправленное несанкционированное воздействие на информационные системы АСУ ТП энергоблока АЭС с применением программных или программно-аппаратных средств[1]. Наиболее опасной является целенаправленная компьютерная атака, процесс которой контролируется в реальном времени человеком, являющимся исполнителем атаки [6]. Воздействие сложной комбинированной целенаправленной компьютерной атаки может привести к событиям различной степени тяжести ущерба для энергоблока, в том числе, к тяжелой аварии [7]. Следовательно, возникает необходимость обеспечить функционирование АСУ ТП энергоблока АЭС под воздействием угроз безопасности информации – обеспечение информационной безопасности АСУ ТП энергоблока АЭС.

Для того чтобы максимально обеспечить безопасность информации АСУ ТП энергоблока АЭС необходимо проанализировать все аспекты данной системы, собрать информацию о среде функционирования АСУ ТП, определить активы, подлежащие защите, и источники угроз [8–10]. Для оценки возможности либо невозможности выполнения компьютерной атаки на системы АСУ ТП необходимо провести ее моделирование: оценить наличие векторов атак, уязвимостей в информационной

[1]Техническая защита информации. Основные термины и определения: Р 50.1.056-2005. 2006.

инфраструктуре АСУ ТП, мотивации и возможностей нарушителя. Между состояниями безопасности информации систем, подсистем и компонентов АСУ ТП существуют взаимовлияния, обусловленные наличием информационных связей, что добавляет возможностей нарушителю для проведения компьютерной атаки и усложняет задачу моделирования.

Принятые для обоснования безопасности АЭС документы[2] рассматривают влияния непреднамеренных отказов оборудования энергоблока АЭС и не учитывают фактор антропогенных угроз безопасности информации. Существующие документы ФСТЭК[3] обуславливают необходимость рассмотрения угроз безопасности информации, но не содержат аппарат оценки последствий компьютерных атак на состояние энергоблока. Таким образом, возникает необходимость в разработке методики оценки воздействия компьютерных атак на АСУ ТП и энергоблок в целом.

Для безопасности энергоблока АЭС является важным поддержание работоспособного состояния в течение всего срока эксплуатации под воздействием внешних воздействующих факторов [11]. В настоящей статье применяется термин стойкость, характеризующий способность системы сохранять работоспособное состояние как и во время действия компьютерной атаки, так и после[4]. Стойкость АСУ ТП энергоблока АЭС в рамках данного исследования измеряется возможностью либо невозможностью успешного выполнения компьютерной атаки на компоненты АСУ ТП с последующим нарушением выполняемых на АСУ ТП функций.

Все вышеизложенное свидетельствует об актуальности и важности создания методики анализа стойкости систем АСУ ТП энергоблока АЭС, учитывающей фактор антропогенных угроз безопасности информации и зависимости отказов.

1. Методы анализа безопасности АСУ ТП энергоблока АЭС

К наиболее известным и широко используемым на практике методам качественной оценки безопасности АСУ ТП энергоблока АЭС относятся:

– метод анализа вида и последствий (критических) отказов: FME(C)A (Failure Mode and Effects (Critical) Analysis)[5];

– метод анализа «дерева событий»: ETA (Event Tree Analysis)[6];

– метод анализа деревьев отказов: FTA (Fault Tree Analysis)[7];

– исследование опасности и связанных с ней проблем: HAZOP (Hazard and operability studies)[8];

– вероятностный анализ безопасности (ВАБ): PRA (Probabilistic risk assessment)[9];

– метод диаграмм надежности: RBD (Reliability Block Diagram)[10].

Недостатками вышеперечисленных методов анализа безопасности являются:

– отсутствие учета фактора антропогенных угроз безопасности информации;

[2]Федеральные нормы и правила в области использования атомной энергии «Требования к содержанию отчета по обоснованию безопасности блока атомной станции с реактором типа ВВЭР»: НП 006-16. 2017.

[3]Методика оценки угроз безопасности информации: утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г. 2021.

[4]Внешние воздействующие факторы. Термины и определения: ГОСТ 26883-86. 2008.

[5]Метод анализа видов и последствий отказов: МЭК 60812:2006. 2008.

[6]Менеджмент риска. Анализ риска технологических систем: ГОСТ Р 51901.1-2002. 2003.

[7]Менеджмент риска. Анализ дерева неисправностей: МЭК 61025:1990. 2005.

[8]Надежность в технике. Анализ опасности и работоспособности (HAZOP): МЭК 61882:2016. 2020.

[9]Атомные станции. Проектирование пунктов управления. Функциональный анализ и распределение функций: МЭК 61839:2011. 2011.

[10]Менеджмент риска. Структурная схема надежности и булевы методы: МЭК 61078:2006. 2008.

– постулирование единовременных отказов;
– отсутствие учета зависимостей между подсистемами одного уровня;
– учет только двух состояний системы: рабочее и отказавшее;
– сложность представления результатов анализа при большом количестве подсистем.

Таким образом, возникает необходимость дальнейшего развития качественных методов анализа безопасности АСУ ТП энергоблока АЭС, которые учитывали бы инфраструктурную комплексность, динамичность и взаимовлияние между системами.

Анализ безопасности инфраструктуры с использованием иерархий матриц критичности (ИМК) является нечетким расширением FMECA и учитывает принципы динамичности, иерархии и взаимовлияния риск-анализа безопасности энергосистем [12]. Состояние безопасности системы можно визуализировать с помощью матрицы критичности [12, 13], также известной как матрица рисков [14–16]. Матрица критичности представляет собой двумерную матрицу, описывающую состояние безопасности системы в параметрах вероятности отказа (инцидента) и тяжести его последствий (ущерба). Пример матрицы критичности представлен на рис. 1. На основании матрицы критичности, представленной на рис. 1, отказ S_1 имеет среднее значение вероятности наступления и среднюю степень тяжести последствий; отказ S_2 имеет высокую вероятность наступления и низкую тяжесть последствий.

	H	M	L
H			S_2
M		S_1	
L			

Рис. 1. Пример матрицы критичности
Fig. 1. Example of a criticality matrix

В матрице критичности множество отказов подсистем разбивается на два подмножества:

– подмножество отказов, расположенных над диагональю матрицы критичности (множество критических отказов);
– подмножество отказов, расположенных под диагональю матрицы (множество некритических отказов).

Для иерархического представления структуры сложных систем строится граф критичности, представляющий собой ИМК. Графом критичности G_{crt} называется пара $(V(G_{crt}),E(G_{crt}))$, где $V(G_{crt})$ – непустое конечное множество элементов, называемых вершинами графа критичности, а $E(G_{crt})$ – семейство ребер графа критичности G_{crt}. Каждое ребро графа критичности вида $(M_{crt}{}^{Si}{}_i, M_{crt}{}^{Sj})$ соединяет вершины $M_{crt}{}^{Si}$ и $M_{crt}{}^{Sj}$.

В соответствии с принципом взаимовлияния, отказ подсистемы *i*-го уровня имеет последствия не только для подсистем более высокого уровня иерархии, но и для подсистем данного уровня при наличии взаимосвязей между подсистемами. Элементами матрицы влияния отказов $M_{\inf}{}^{S_i \to S_j}$ могут быть значения лингвистической переменной «Влияние отказа S_i на критичность отказа S_j», $i \neq j, i = 1,m; j = 1,n$. Значениями переменной могут быть лингвистические термы: «высокое», «среднее», «низкое».

Этапы анализа с использованием ИМК:

– декомпозиция структуры системы, идентификация отказов;
– определение ущерба, вероятности и критичности отказов (FMECA);
– построение ИМК на начальный момент времени;
– определение влияния отказов систем на наступление отказов систем *i*-го уровня и *(i–1)*-го уровня (составление матриц влияния отказов $M_{\text{inf}}^{S_i \to S_j}$);
– оценка изменений ИМК при наступлении некритических и критических отказов.

Проведение анализа безопасности с использование ИМК позволяет определять эффективные стратегии управления безопасностью, поскольку риск, связанный с появлением отказа, постоянно изменяется. Учет взаимовлияния отказов позволяет выявить узкие места в безопасности системы.

В предложенном в работе [12] методе анализа безопасности АСУ ТП энергоблока АЭС с использованием ИМК не учитывается фактор антропогенных угроз безопасности информации. В рамках настоящего исследования рассматриваются отказы, обусловленные фактором антропогенных угроз безопасности информации, и формируется методика анализа стойкости АСУ ТП энергоблока АЭС к воздействию целенаправленных компьютерных атак, основанная на применении матричных моделей оценивания рисков.

2. Методика анализа стойкости АСУ ТП энергоблока АЭС

Для анализа стойкости АСУ ТП энергоблока АЭС к воздействию целенаправленных компьютерных атак в настоящей работе предлагается проводить моделирование сценариев компьютерных атак с использованием ИМК. Учет принципа динамичности риск-анализа безопасности энергосистем [12] позволяет рассмотреть изменение критичности отказов подсистем и компонентов на каждом этапе целенаправленной компьютерной атаки. Представление структуры сложных систем в виде иерархии является одним из основных принципов анализа безопасности сложных систем. Учет принципа взаимовлияния позволяет учесть не только обмен информации между системами и подсистемами при выполнении операционных задач, но и обмен информацией между подсистемами одного уровня.

В общем случае для подсистем и компонентов АСУ ТП энергоблока АЭС можно выделить три вида взаимодействия:

– физическое влияние, обусловленное потоками энергии между подсистемами и компонентами АСУ ТП (например, общее питание);
– информационное влияние, обусловленное информационным обменом между подсистемами и компонентами АСУ ТП;
– географическое влияние, обусловленное близостью подсистем и компонентов АСУ ТП между собой (распространение последствий).

Для подсистем и компонентов АСУ ТП при рассмотрении угрозы успешной реализации целенаправленной компьютерной атаки наиболее важным видом взаимовлияния является информационное взаимодействие.

В анализе с использованием ИМК состояние безопасности информации подсистемы или компонента АСУ ТП определяется не только собственным состоянием безопасности, но также состояниями зависимых компонентов/подсистем. Использование ИМК позволяет учитывать изменение критичности отказов на каждом этапе компьютерной атаки, взаимовлияние отказов и иерархическое представление структуры системы.

В основу подхода к методике были положены консолидированные положения серии ГОСТ Р МЭК 61508[11] в части анализа рисков опасных отказов для различных объектов. Предложенная в данной статье методика анализа стойкости АСУ ТП энергоблока АЭС включает в себя 3 взаимосвязанных последовательных этапа:

– Этап 1: анализ на уровне энергоблока АЭС;

– Этап 2: анализ на уровне архитектуры (функциональной структуры) АСУ ТП энергоблока АЭС;

– Этап 3: анализ на уровне компонентов АСУ ТП энергоблока АЭС.

В рамках анализа должна быть проведена декомпозиция структуры систем, задействованных в рассматриваемом нарушении, и FMECA отказов систем, подсистем и компонентов, задействованных в рассматриваемом нарушении ТП.

На первом этапе анализа определяется нарушение ТП (его результирующие события), основные системы энергоблока АЭС, задействованные в сценарии, и проводится FMECA нарушения ТП. На основе проведенного FMECA строится матрица критичности нарушения ТП, визуализирующее состояние безопасности системы.

Основной целью второго этапа анализа является определение условий необходимых для реализации нарушения ТП. Также на данном этапе необходимо выделить задействованные в реализации нарушения ТП подсистемы АСУ ТП энергоблока АЭС и определить тяжести ущерба и вероятности реализации отказов этих подсистем (провести FMECA отказов подсистем АСУ ТП энергоблока АЭС). Для последующего моделирования сценариев компьютерных атак на втором этапе анализа составляется матрица влияния отказов выделенных подсистем $M_{\inf}^{S_i \to S_j}$.

На третьем этапе анализа определяются задействованные в реализации нарушения ТП компоненты АСУ ТП энергоблока АЭС, проводится FMECA их отказов, строится матрица влияния отказов и составляются сценарии целенаправленных компьютерных атак с использованием ИМК.

При моделировании сценариев целенаправленных компьютерных атак с использованием ИМК для каждого этапа компьютерной атаки определяются:

– действия нарушителя;

– объекты воздействия компьютерной атаки (системы, подсистемы, компоненты), критичность которых повышается или наступает их отказ;

– необходимые возможности нарушителя;

– уточненные ИМК всех систем, подсистем и компонентов, задействованных в сценарии.

Моделирование сценариев компьютерных атак происходит «снизу-вверх»: на каждый из компонентов АСУ ТП энергоблока АЭС, определенных на 3-м этапе, моделируются сценарии компьютерных атак. С помощью матриц влияния определяются возможные сценарии целенаправленных компьютерных атак, что позволяет учесть их возможные векторы развития.

Результатом анализа является ИМК всех систем на начальный момент времени G_{crt}, матрицы влияния отказов $M_{\inf}^{S_i \to S_j}$ и уточненные ИМК с учетом наступления некритических и критических отказов.

[11]Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью: ГОСТ Р МЭК 61508. 2012.

3. Пример моделирования компьютерной атаки с использованием матричных моделей оценивания риска

Для демонстрации методики рассмотрим условный пример сегмента АСУ ТП энергоблока АЭС, состоящий из технологической части управляющей системы безопасности (УСБТ), системы верхнего (блочного) управления (СВБУ) и их компонентов: технических средств УСБТ в составе шкафа АСУ ТП, инженерной станции УСБТ, автоматизированного рабочего места (АРМ) оперативного персонала СВБУ, устройства передачи данных СВБУ. Исходное событие аварии S происходит в результате отказа S_1 функции УСБТ. К отказу функции УСБТ может привести отправка команды управления со стороны технических средств УСБТ в составе шкафа АСУ ТП (ложное срабатывание, отказ S_{11}), инициированной управляющим сигналом со стороны инженерной станции УСБТ (ложное срабатывание, отказ S_{12}). Отказ инженерной станции может наступить в результате отказа СВБУ S_2 путем отправки видеокадра с АРМ оперативного персонала СВБУ (ложное срабатывание, отказ S_{21}). Несанкционированный терминальный доступ к АРМ оперативного персонала СВБУ может быть получен из сети СВБУ со стороны устройства передачи данных (отказ S_{22}). Матрица влияния отказов сегмента АСУ ТП энергоблока АЭС представлена в табл. 1. На рис. 2 представлена ИМК на начальный момент времени.

Таблица 1. Матрица влияния отказов АСУ ТП энергоблока АЭС

Отказ	S	S_1	S_2	S_{11}	S_{12}	S_{21}	S_{22}
S_1	Высокое	—	—	—	—	—	—
S_2	Среднее	Среднее	—	—	—	—	—
S_{11}	—	Высокое	—	—	—	—	—
S_{12}	—	Среднее	—	Высокое	—	—	—
S_{21}	—	—	—	—	Среднее	—	Среднее
S_{22}	—	—	—	—	—	Среднее	—

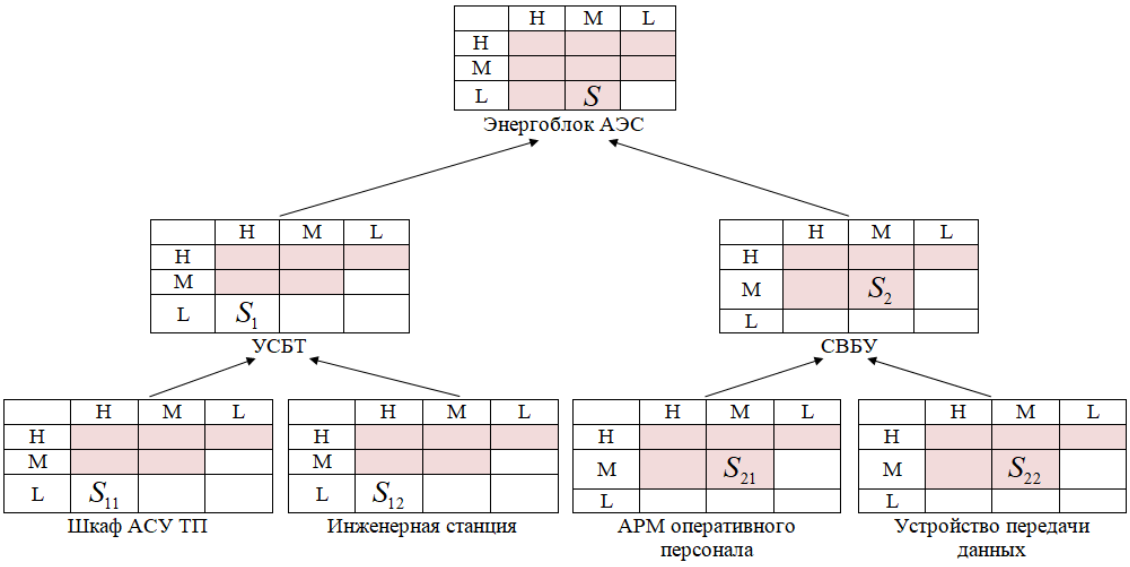

Рис. 2. Иерархия матриц критичности на этапе проектного анализа
Fig. 2. Criticality matrix hierarchy at the stage of design analysis

Рассмотрим сценарий компьютерной атаки, произошедшей в результате внедрения вредоносного программного обеспечения в системное программное обеспечение устройства передачи данных СВБУ. При наступлении отказа (получения несанкционированного доступа) устройства передачи данных в соответствии с матрицей влияния повышается критичность отказов S_2, S_{21}. Последующее получение несанкционированного терминального доступа к АРМ оперативного персонала (отказ S_{21}) повышает критичность отказов S_2, S_{12} (рис. 3).

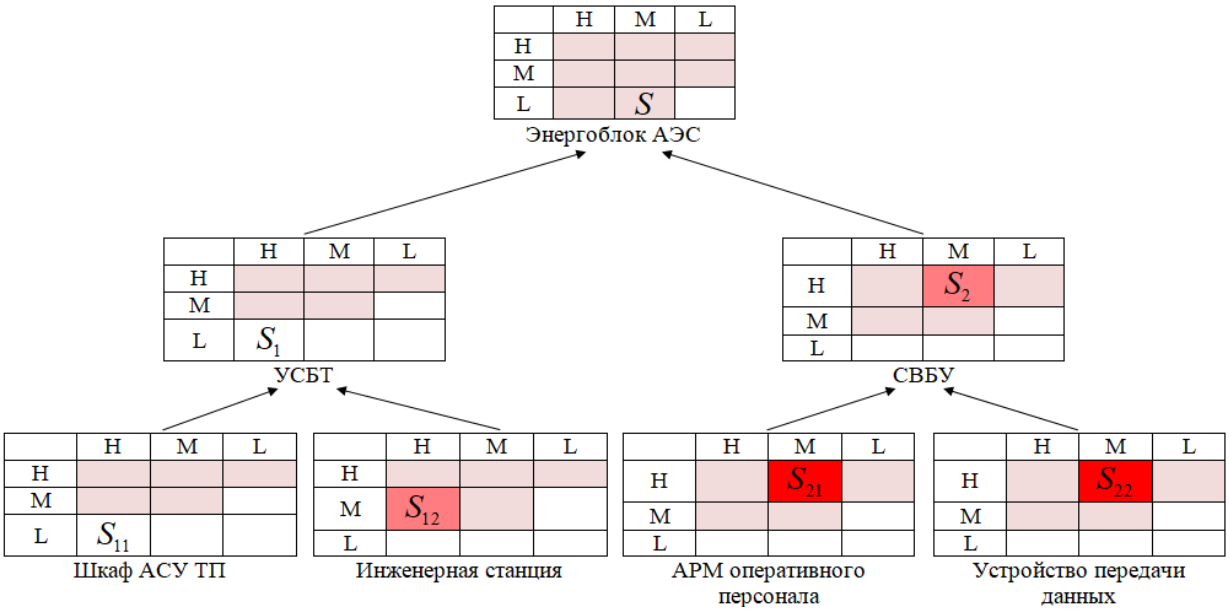

Рис. 3. Иерархия матриц критичности на этапе получения несанкционированного доступа к АРМ оперативного персонала СВБУ

Fig. 3. Criticality matrix hierarchy at the stage of obtaining unauthorized access to the workstation of operating personnel

В результате отправки видеокадра в УСБТ с АРМ оперативного персонала наступает отказ СВБУ S_2 и повышается критичность отказа энергоблока S. На инженерной станции УСБТ инициируется управляющий сигнал, из-за чего повышается критичность отказа технических средств шкафа АСУ ТП S_{12} и УСБТ S_1. Уточненная ИМК представлена на рис. 4.

Средства управления в составе шкафа АСУ ТП формируют и отправляют управляющий сигнал (отказ S_{11}), в результате чего наступает отказ УСБТ S_1, что приводит к исходному событию аварии S.

Представленный выше сценарий компьютерной атаки невозможно составить без учета принципа взаимовлияния, который в рамках анализа был учтен через матрицы влияния отказов (табл. 1). Путем использования матриц влияния представляется возможным прогнозировать поведение злоумышленника, а уточненные иерархии матриц критичности позволят наглядно иллюстрировать состояние системы на каждом этапе компьютерной атаки.

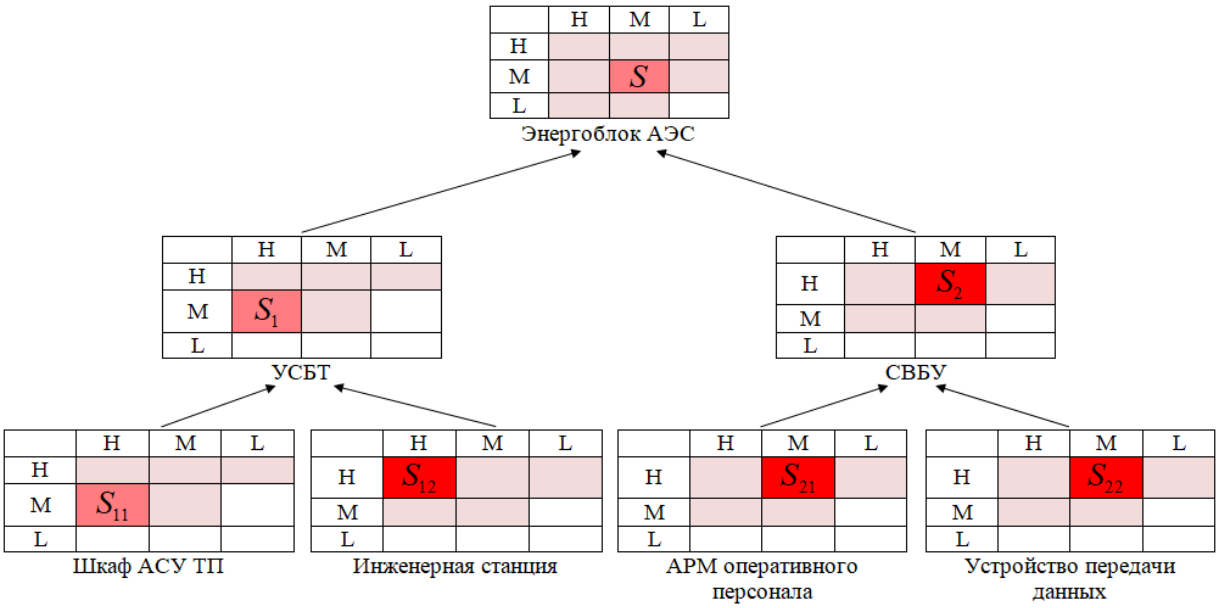

Рис. 4. Иерархия матриц критичности на этапе отказа инженерной станции УСБТ
Fig. 4. Criticality matrix hierarchy at the stage of failure of the engineering workstation

Заключение

Традиционно в атомной энергетике для анализа безопасности АЭС разрабатываются соответствующие документы, обосновывающие безопасность: вероятностный анализ безопасности, предварительный и окончательный отчеты по обоснованию безопасности. В рамках отмеченных документов рассматриваются влияния непреднамеренных отказов оборудования АЭС, включая АСУ ТП, на безопасность АЭС. Однако полученные подобным образом результаты в большинстве случаев недостаточны для анализа стойкости АСУ ТП к воздействию угроз безопасности информации, включая компьютерные атаки. Такое положение дел обусловлено тем, что в рамках существующей практики анализа безопасности АЭС не рассматривается фактор антропогенных угроз безопасности информации, в том числе целенаправленные компьютерные атаки; не учитывается зависимость отказов систем и их компонентов.

Таким образом, существует острая необходимость в разработке методов и подходов, позволяющих оценить последствия воздействия компьютерных атак на АСУ ТП энергоблока АЭС и безопасность энергоблока АЭС в целом.

Предложенная в работе методика анализа стойкости АСУ ТП энергоблока АЭС к воздействию целенаправленных компьютерных атак, основанная на применении матриц влияния и иерархии матриц критичности, учитывает принципы динамичности, иерархии и взаимовлияния риск-анализа безопасности энергосистем и применима для моделирования сценариев компьютерных атак. Представленный в статье анализ, основанный на использовании матричных моделей оценивания рисков, ранее не проводился для отечественных АЭС и может быть интегрирован в существующую практику, что позволит обеспечить безопасность АЭС с учетом фактора антропогенных угроз безопасности информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Cherdantseva Y., Burnap P., Blyth A. A review of cyber security risk assessment methods for SCADA systems. Computers & Security. 2016. № 56. P. 1–27. URL:https://www.researchgate.net/publication/283568912_A_Review_of_cyber_security_risk_assessment_methods_for_SCADA_systems (дата обращения: 07.10.2021).

2. Лукацкий А. В. Кибербезопасность ядерных объектов // Индекс Безопасности. 2015. № 4 (115). С. 113–126. URL: https://pircenter.org/media/content/files/13/14758399062.pdf (дата обращения: 07.10.2021).
3. Бабаев Д.И., Полетыкин А.Г., Промыслов В.Г., Тимофеев М.Ю. Управление архитектурой кибербезопасности АСУТП атомных электростанций // Информационные технологии в управлении. 2018. № 3. С. 47–55. URL: http://m.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=pu&paperid=1082&option_lang=rus (дата обращения: 07.10.2021).
4. Whitehead, D., Owens, K., Gammel, D., Smith, J. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies. Proceedings of the 70th Annual Conference for Protective Relay Engineers (CPRE), 2017. – 9 p. URL: https://www.researchgate.net/publication/320829833_Ukraine_cyber-induced_power_outage_Analysis_and_practical_mitigation_strategies (дата обращения: 07.10.2021).
5. Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г. Кибернетические угрозы и принципы обеспечения кибербезопасности в цифровых системах управления // Энергетик. 2012. № 7. С. 18–23. URL: http://cybersafety.sicpro.org/doc/polet_plenary.pdf (дата обращения: 07.10.2021).
6. Kim Y., Kim I. Involvers' Behavior-based Modeling in Cyber Targeted Attack. Proceedings of the eighth International Conference on Emerging Security Information, Systems and Technologies, 2014. P. 132–137. URL: https://www.researchgate.net/publication/282756823_Involvers'_behavior-based_modeling_in_cyber_targeted_attack (дата обращения: 07.10.2021).
7. Zhou X., Xu Z., Wang L., Wang K., Chen C., Zhang W. APT Attack Analysis in SCADA Systems. Proceedings of MATEC Web of Conferences, 2018. – 5 p. URL: https://www.researchgate.net/publication/325852668_APT_Attack_Analysis_in_SCADA_Systems (дата обращения: 07.10.2021).
8. G.C. Chittester and Y.Y. Haimes. Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures. Journal of Homeland Security and Emergency Management. 2004. № 1(4). – 39 p. URL:https://www.researchgate.net/publication/242556907_Risks_of_Terrorism_to_Information_Technology_and_to_Critical_Interdependent_Infrastructures (дата обращения: 07.10.2021).
9. Barnes K., Johnson B. Introduction to SCADA protection and vulnerabilities. Idaho, Idaho National Engineering and Environmental Laboratory. 2004. – 41 p. URL:https://www.researchgate.net/publication/255532764_Introduction_To_SCADA_Protection_And_Vulnerabilities (дата обращения: 07.10.2021).
10. Teixeira A., Pérez D., Sandberg H., Johansson K.H. Attack Models and Scenarios for Networked Control Systems. Proceedings of the 1st international conference on High Confidence Networked Systems, 2012. P. 55–64. URL: https://www.researchgate.net/publication/254008495_Attack_models_and_scenarios_for_networked_control_systems (дата обращения: 07.10.2021).
11. Полетыкин А.Г., Промыслов В.Г., Менгазетдинов Н.Э. Концепция обеспечения защиты от несанкционированного доступа АСУ ТП АЭС Бушер-1 // Автоматизация в промышленности. 2005. № 5. – 6 с. URL: https://www.ipu.ru/sites/default/files/page_file/secure1.pdf (дата обращения: 07.10.2021).
12. Харченко В.С. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения // Харьков, Министерство образования и науки, молодежи и спорта Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2011. С. 151–173.
13. Брежнев Е.В. Метод оценивания рисков каскадных аварий (отказов) с использованием динамических матриц критичности // Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 1(18). С. 187–190. URL: http://www.hups.mil.gov.ua/periodic-app/article/775/nitps_2015_1_42.pdf (дата обращения: 07.10.2021).
14. Новожилов Е.О. Принципы построения матрицы рисков // Надежность. 2015. № 3. С. 43–80. URL: https://www.dependability.ru/jour/article/view/98 (дата обращения: 07.10.2021).
15. Pickering A., Cowley S.P. Risk Matrices: implied accuracy and false assumptions. Journal of Health & Safety Research & Practice. 2010. № 2(1). P. 11–18. URL:https://www.researchgate.net/publication/285484045_Risk_matrices_Implied_accuracy_and_false_assumptions (дата обращения: 07.10.2021).
16. Cox L. Whats wrong with risk matrices? Risk analysis. 28(2), 2008. P. 497–511. URL:https://www.researchgate.net/publication/310802191_What's_Wrong_with_Risk_Matrices_Decoding_a_Louis_Anthony_Cox_paper (дата обращения: 07.10.2021).

REFERENCES:

[1] Cherdantseva Y., Burnap P., Blyth A. A review of cyber security risk assessment methods for SCADA systems. Computers & Security. 2016. 56, P. 1–27. URL:https://www.researchgate.net/publication/283568912_A_Review_of_cyber_security_risk_assessment_methods_for_SCADA_systems (accessed: 07.10.2021).

[2] Lukackij A. V. Cybersecurity of nuclear facilities. Indeks Bezopasnosti. 2015. № 4 (115). P. 113–126. URL: https://pircenter.org/media/content/files/13/14758399062.pdf (accessed: 07.10.2021) (in Russian).

[3] Babaev D.I., Poletykin A.G., Promyslov V.G., Timofeev M.YU. Management of the cybersecurity architecture of the process control systems of nuclear power plants. Informacionnye tekhnologii v upravlenii. 2018. № 3. P. 47–55. URL: http://m.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=pu&paperid=1082&option_lang=rus (accessed: 07.10.2021) (in Russian).

[4] Whitehead, D., Owens, K., Gammel, D., Smith, J. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies. Proceedings of the 70th Annual Conference for Protective Relay Engineers (CPRE), 2017. – 9 p. URL: https://www.researchgate.net/publication/320829833_Ukraine_cyber-induced_power_outage_Analysis_and_practical_mitigation_strategies (accessed: 07.10.2021).

[5] Mengazetdinov N.E., Poletykin A.G., Promyclov V.G. Cyber Threats and Principles of Cybersecurity in Digital Control Systems. Energetik. 2012. № 7. P. 18–23. URL: http://cybersafety.sicpro.org/doc/polet_plenary.pdf (accessed: 07.10.2021) (in Russian).

[6] Kim Y., Kim I. Involvers' Behavior-based Modeling in Cyber Targeted Attack. Proceedings of the eighth International Conference on Emerging Security Information, Systems and Technologies, 2014. P. 132–137. URL: https://www.researchgate.net/publication/282756823_Involvers'_behavior-based_modeling_in_cyber_targeted_attack (accessed: 07.10.2021).

[7] Zhou X., Xu Z., Wang L., Wang K., Chen C., Zhang W. APT Attack Analysis in SCADA Systems. Proceedings of MATEC Web of Conferences, 2018. – 5 p. URL: https://www.researchgate.net/publication/325852668_APT_Attack_Analysis_in_SCADA_Systems (accessed: 07.10.2021).

[8] G.C. Chittester and Y.Y. Haimes. Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures. Journal of Homeland Security and Emergency Management. 2004. № 1(4). – 39 p. URL:https://www.researchgate.net/publication/242556907_Risks_of_Terrorism_to_Information_Technology_and_to_Critical_Interdependent_Infrastructures (accessed: 07.10.2021).

[9] Barnes K., Johnson B. Introduction to SCADA protection and vulnerabilities. Idaho, Idaho National Engineering and Environmental Laboratory. 2004. – 41 p. URL:https://www.researchgate.net/publication/255532764_Introduction_To_SCADA_Protection_And_Vulnerabilities (accessed: 07.10.2021).

[10] Teixeira, A., Pérez D., Sandberg H., Johansson K.H. Attack Models and Scenarios for Networked Control Systems. Proceedings of the 1st international conference on High Confidence Networked Systems, 2012. P. 55–64. URL: https://www.researchgate.net/publication/254008495_Attack_models_and_scenarios_for_networked_control_systems (дата обращения: 07.10.2021) (accessed: 07.10.2021).

[11] Poletykin A.G., Promyslov V.G., Mengazetdinov N.E. The concept of providing protection against unauthorized access for the automated process control system at Bushehr-1 NPP. Avtomatizaciya v promyshlennosti. 2005. № 5. – 6 p. URL: https://www.ipu.ru/sites/default/files/page_file/secure1.pdf (accessed: 07.10.2021) (in Russian).

[12] Harchenko V.S. Security of critical infrastructures: mathematical and engineering methods of analysis and support. Har'kov, Ministerstvo obrazovaniya i nauki, molodezhi i sporta Ukrainy, Nacional'nyj aerokosmicheskij universitet im. N.E. ZHukovskogo «HAI», 2011. P. 151–173 (in Russian).

[13] Brezhnev E.V. A method for assessing the risks of cascade accidents (failures) using dynamic criticality matrices. Science and technology of the Air Force of the Armed Forces of Ukraine. 2015. № 1(18). P. 187–190. URL: http://www.hups.mil.gov.ua/periodic-app/article/775/nitps_2015_1_42.pdf (accessed: 07.10.2021) (in Russian).

[14] Novozhilov E.O. Principles of building a risk matrix. Nadezhnost'. 2015. № 3. P. 43–80. URL: https://www.dependability.ru/jour/article/view/98 (accessed: 07.10.2021) (in Russian).

[15] Pickering A., Cowley S.P. Risk Matrices: implied accuracy and false assumptions. Journal of Health & Safety Research & Practice. 2010. № 2(1). P. 11–18. URL:https://www.researchgate.net/publication/285484045_Risk_matrices_Implied_accuracy_and_false_assumptions (accessed: 07.10.2021).

[16] Cox L. Whats wrong with risk matrices? Risk analysis. 28(2), 2008. P. 497–511. URL:https://www.researchgate.net/publication/310802191_What's_Wrong_with_Risk_Matrices_Decoding_a_Louis_Anthony_Cox_paper (accessed: 07.10.2021).

Поступила в редакцию – 12 октября 2021 г. Окончательный вариант – 25 ноября 2021 г.
Received – October 12, 2021. The final version – November 25, 2021.