ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Иваненко В. Г.[1], Иванова Н. Д.[2]

DOI: 10.21681/2311-3456-2024-1-116-123

Цель работы: *формирование методики количественной и качественной оценки рисков информационной безопасности автоматизированных систем управления технологическим процессом как объектов критической информационной инфраструктуры и предложений об ее внедрении в проводимый процесс категорирования объектов критической информационной инфраструктуры с целью адаптации базового набора мер защиты.*

Метод исследования: *анализ существующих подходов к оценке рисков информационной безопасности. Анализ отечественных и зарубежных нормативно-правовых и методических документов на предмет применимости для оценки рисков информационной безопасности автоматизированных систем управления технологическим процессом. Построение блок-схем процессов оценки рисков.*

Результаты: *в исследовании обоснована необходимость проведения оценки рисков информационной безопасности автоматизированных систем управления технологическим процессом с целью адаптации базового набора мер защиты. Проведен анализ методов количественной и качественной оценки рисков информационной безопасности, определен смешанный подход к оценке рисков как компромиссный между ними. На основании национальных и международных нормативно-методических документов и практики обеспечения информационной безопасности были определены факторы и характеристики рисков информационной безопасности, а также возможность их количественной оценки. Сформированы предложения к алгоритму количественной и качественной оценки рисков информационной безопасности автоматизированных систем управления технологическим процессом и к его внедрению в проводимый процесс категорирования объектов критической информационной инфраструктуры. Составлены блок-схема соответствующих процессов.*

Практическая ценность: *практическая ценность работы заключается в предложении метода оценки рисков, согласованного с существующей практикой обеспечения информационной безопасности автоматизированных систем управления технологическим процессом, методами управления рисками информационной безопасности и требованиями регулирующих органов. Результаты проведенного анализа и выработанные рекомендации по адаптации базового набора мер защиты могут быть используемы для повышения информационной безопасности автоматизированных систем управления технологическим процессом.*

Ключевые слова: *угрозы информационной безопасности, уязвимости, базовый набор мер защиты, CVSS, количественные, качественные, смешанные (гибридные) методы оценки рисков.*

INFORMATION SECURITY RISK ASSESSMENT OF INDUSTRIAL CONTROL SYSTEMS

Ivanenko V. G.[3], Ivanova N. D.[4]

Purpose: *development of a methodology for quantitative and qualitative assessment of information security risks of industrial control systems as objects of critical information infrastructure and development of proposals*

1 Иваненко Виталий Григорьевич, доктор технических наук, профессор Института Интеллектуальных Кибернетических Систем (ИИКС) Национального исследовательского ядерного университета «МИФИ», г. Москва, Россия. E-mail: VGIvanenko@mephi.ru

2 Иванова Нина Дмитриевна, аспирант кафедры «Управление и защита информации» Российского университета транспорта (МИИТ), г. Москва, Россия. E-mail: IvanovaND.Nina@yandex.ru, ORCID 0000-0001-5942-8050

3 Vitaly G. Ivanenko, Dr.Sc., Associate Professor of the Institute of Intelligent Cybernetic Systems of the National Research Nuclear University «MEPhI», Moscow, Russia. E-mail: VGIvanenko@mephi.ru

4 Nina D. Ivanova, assistant of the Department of Management and Information Security, Russian University of Transport (MIIT), Moscow, Russia. Email: IvanovaND.Nina@yandex.ru, ORCID 0000-0001-5942-8050

for its implementation in addition to the process of categorizing objects of critical information infrastructure in order to adapt the basic set of protection measures.

Research method: *analysis of existing approaches to assessing information security risks. Analysis of national and international regulatory and methodological documents for applicability for assessing the information security risks of industrial control systems. Drawing up flowcharts of risk assessment processes.*

Results: *the study substantiates the need to conduct an assessment of the information security risks of industrial control systems in order to adapt a basic set of protection measures. An analysis of methods for quantitative and qualitative assessment of information security risks was carried out, and a hybrid approach to risk assessment was determined as a compromise between them. Based on national and international regulatory and methodological documents and information security practices, the factors and characteristics of information security risks of industrial control systems were identified, as well as the possibility of their quantitative assessment. Proposals have been formulated for an algorithm for quantitative and qualitative risk assessment of industrial control systems and for its implementation in addition to the process of categorizing objects of critical information infrastructure. Flowcharts of the relevant processes have been drawn up.*

Practical value: *the practical value of the work lies in the proposal of a risk assessment method consistent with the existing practice of ensuring the information security of industrial control systems, information security risk management methods and the requirements of regulatory authorities. The results of the analysis and recommendations developed for adapting a basic set of protection measures can be used to improve the information security of industrial control systems.*

Keywords: *information security threats, vulnerabilities, basic set of protection measures, CVSS, qualitative, qualitative, hybrid risk assessment methods.*

Введение

До сравнительно недавнего времени обеспечение информационной безопасности (ИБ) не являлось приоритетной задачей для автоматизированных систем управления технологическим процессом (АСУ ТП) [1]. Безопасность ранних АСУ ТП достигалась за счет контроля физического доступа к компонентам системы – специализированным программно-аппаратным комплексам, использующим проприетарные протоколы связи.

Современные системы АСУ ТП сложны и основаны на передовых технологиях. Возрастающая сложность и модернизация, а также непрерывная работа в режиме реального времени и распределенная многокомпонентная архитектура лежат в основе роста компьютерных атак на АСУ ТП. АСУ ТП подвержены широкому спектру компьютерных атак, в том числе из-за стандартизации коммуникационных протоколов и аппаратных компонентов, растущей взаимосвязи и наследия [2].

В 2010 году компьютерный червь Stuxnet поразил иранский ядерный объект, вызвав отказ почти пятой части всех центрифуг [3]. В 2014 украинские электросети были атакованы с помощью вредоносного программного обеспечения Black Energy 3, что привело к временному обесточиванию большей части Украины [4]. В 2017 году в системах противоаварийной защиты саудовского нефтехимического предприятия была обнаружена вредоносная программа Triton/Triconex [5]; последствием успешной реализации компьютерной атаки с использованием Triton/Triconex могла стать гибель людей. В начале 2022 года группой хакеров Hackers-Arise были реализованы многочисленные нападения на объекты промышленной инфраструктуры Российской Федерации [6]. В 2010 году в Репозитории инцидентов промышленной безопасности (The Repository of Industrial Security Incidents – RISI) был зарегистрирован 161 компьютерный инцидент, причем каждый квартал добавлялось около 10 новых инцидентов. В 2013 году база данных RISI содержала уже 240 инцидентов. Начиная с января 2015 года, RISI перестал обновляться, содержа в своей базе более 300 инцидентов компьютерной безопасности. Неуклонный рост компьютерных атак на объекты промышленной автоматизации стал причиной появления соответствующих нормативных документов и требований к ИБ АСУ ТП [7].

Необходимость обеспечения ИБ АСУ ТП как объектов критической информационной инфраструктуры (КИИ) обусловлена требованиями приказов ФСТЭК России № 239[5] и 31[6]. Данные приказы содержат требования к применяемым мерам защиты информации АСУ ТП КИИ в соответствии с присвоенной категорией значимости объекта КИИ и классом защищенности АСУ. В случае пересечения требований необходимо применять наиболее строгое.

5 Приказ ФСТЭК России от 25.12.2017. № 239. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31

6 Приказ ФСТЭК России от 14.03.2014. № 31. URL:https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

Оценка рисков безопасности АСУ ТП КИИ является основой для принятия решений, связанных с предотвращением аварий или минимизацией их негативных последствий. В соответствии с приказами ФСТЭК России базовый набор мер защиты информации (по обеспечению безопасности) должен быть адаптирован, если он не позволяет обеспечить блокирование всех угроз ИБ. Критерии для адаптации базового набора мер в приказах ФСТЭК России отсутствуют, что обуславливает необходимость разработки методики оценки рисков АСУ ТП КИИ.

Согласно [8] каждый новый разработанный нормативно-правовой акт или методический документ способствует появлению новых потенциальных рисков для защищаемой организации. Поэтому для оценки рисков ИБ АСУ ТП КИИ предлагается исследовать применимость существующих нормативно-правовых актов, государственных стандартов и методических документов. Анализ применимости этих документов и их учет в контексте управления рисками ИБ может послужить основой для разработки рекомендаций по поддержанию актуальности рисков ИБ АСУ ТП КИИ.

Целью настоящей статьи является формирование методики количественной и качественной оценки рисков ИБ (установления значения рисков ИБ) АСУ ТП КИИ как одного из этапов процесса оценки рисков ИБ, а также формирование предложений по внедрению разработанной методики в процесс категорирования объектов КИИ с целью уточнения базового набора мер защиты.

Количественные и качественные методы оценки рисков ИБ АСУ ТП КИИ

В области оценки рисков ИБ имеют широкое распространение два основных направления [9]: количественная оценка рисков (риск измеряется, например, в возможных финансовых потерях) и качественная оценка рисков (риск задается значениями лингвистической переменной).

Качественные методы оценки рисков не оперируют числовыми данными, представляя результат в виде описаний, сценариев угроз ИБ и рекомендаций. К основным недостаткам качественных методов оценки рисков можно отнести отсутствие числового представления результатов, невысокую точность и приближенный характер результатов [10]. С применением качественного подхода возможно учесть те риски, которые нельзя характеризовать количественно, с другой стороны, качественная оценка усложняет принятие точных решений по снижению рисков.

Методы количественной оценки рисков ИБ используют фактические данные, которые можно измерить математически или с помощью других вычислительных методов. Количественные методы оценки рисков учитывают только те риски, что могут быть количественно выражены (например, риски функциональных компонентов и конфигурации системы) [11]. Благодаря измеримости и воспроизводимости данных количественная оценка рисков является надежным и эффективным методом, но его недостатком является возможность игнорирования рисков, возникающих из нетехнических аспектов.

Как качественная, так и количественная оценка являются ключевыми факторами успешной деятельности по управлению рисками, и обычно их используют совместно. Например, на этапе установления контекста риска первым используют качественный подход, выявляя приоритетные риски, которые после будут уточнены с помощью количественного подхода.

Компромиссом между подходами качественной и количественной оценки может быть смешанный подход [12] к оценке рисков, также называемый гибридной оценкой рисков [13]. Смешанный подход объединяет качественный и количественный методы: например, путем перевода качественно определенного значения риска в количественный по соответствующей числовой шкале или наоборот (сопоставление значениям лингвистических переменных числовых шкал). С использованием смешанного подхода к оценке рисков сохраняются достоинства обоих методов (точность оценок, полученных из количественного метода и возможность всестороннего анализа, получаемого с использованием качественного метода оценки) и нивелируются их недостатки.

Формирование перечня факторов и характеристик рисков ИБ АСУ ТП КИИ

Под угрозой информационной безопасности следует понимать потенциальное нежелательное опасное событие, когда как риск информационной безопасности определяет степень опасности воздействия нежелательного события на систему или объект системы [14]. В определениях государственных и международных стандартов и руководств понятие риск чаще всего характеризуется как сочетание тяжести и вероятности наступления опасного события. Стандарты, определяющие риск ИБ, характеризуют его как потенциальную возможность успешно использовать уязвимость с целью создания угрозы активу, приводящей к нежелательным последствиям для организации. Следовательно, важнейшими факторами риска являются тяжесть последствий и вероятность наступления опасного события. Вероятность наступления опасного события ИБ может быть характеризована исходной защищенностью системы (уязвимостями системы и ее компонентов) и потенциалом (возможностями) нарушителя.

В результате риск ИБ определяется следующими факторами:

- величина тяжести возможных последствий от реализации опасного события;
- вероятность наступления опасного события, определяемая уязвимостями системы и ее компонентов и потенциалом нарушителя.

Согласно требованиям приказов ФСТЭК России, величину тяжести ущерба для обеспечения ИБ АСУ ТП КИИ характеризуют значения показателей критериев значимости объектов КИИ РФ и степень возможного ущерба от нарушения свойств конфиденциальности, целостности и доступности информации.

Уязвимости АСУ ТП КИИ могут быть определены с использованием стандарта Common Vulnerability Scoring System (CVSS)[7] – открытого стандарта, используемого для оценки уязвимостей, в том числе, и для уязвимостей из базы данных угроз (БДУ) ФСТЭК России. Для определения характеристик потенциала нарушителя может быть использован стандарт ГОСТ Р ИСО/МЭК 18045-2013[8], который предлагает методику определения потенциала нападения нарушителя, ориентированную на имеющиеся в системе уязвимости (и, следовательно, объекты защиты, что согласуется с определенным в [15] подходом к обеспечению ИБ АСУ ТП КИИ).

Ниже представлены факторы и характеристики рисков ИБ АСУ ТП КИИ, включая возможность их количественной оценки (табл. 1). Если количественную оценку рисков реализовать не представляется возможным, следует провести смешанную оценку рисков: качественно определенные характеристики перевести в количественные с помощью соответствующей числовой шкалы, сопоставляющей значения лингвистических переменных числовым показателям.

Большинство из предложенных характеристик определяются на основании отечественных или зарубежных методических документов, что позволяет проводить оценку рисков с использованием результатов уже проведенных исследований при их наличии.

Формирование предложений к алгоритму количественной и качественной оценки рисков ИБ АСУ ТП КИИ

Целью этапа количественной и качественной оценки рисков ИБ в процессе управления рисками ИБ является формирование количественных и качественных показателей факторов рисков для дальнейшей сравнительной оценки. Ниже приведена блок-схема процесса количественной и качественной оценки рисков ИБ АСУ ТП КИИ (рис. 1).

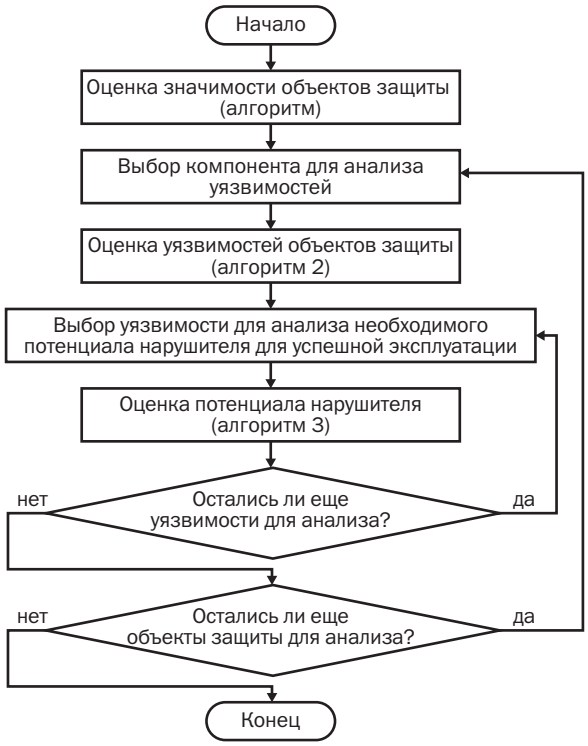


Рис. 1. Блок-схема процесса количественной и качественной оценки рисков ИБ АСУ ТП КИИ

Оценка значимости объектов защиты (рис. 2) производится на основании ранее проведенного категорирования и определения класса защищенности АСУ. В рамках анализа ущерб из-за отказов компонентов определяется тяжестью ущерба отказа соответствующей системы согласно положениям Постановления Правительства № 127[9] в части категорирования объектов КИИ, заключающимся в присвоении определенной категории значимости объектам по результатам анализа «сверху-вниз».

Рис. 2. Блок-схема оценки значимости объектов защиты АСУ ТП КИИ (алгоритм 1)

7 Common Vulnerability Scoring System version 3.1: Specification Document. – URL: https://www.first.org/cvss/specification-document/

8 ГОСТ Р ИСО/МЭК 18045–2013 (введ. 28.08.2013). URL: https://gostexpert.ru/data/files/18045-2013/65454.pdf

9 Постановление Правительства Российской Федерации от 08.02.2018 № 127. URL:http://publication.pravo.gov.ru/Document/View/0001201802130006

Таблица 1.

Факторы и характеристики рисков ИБ АСУ ТП КИИ

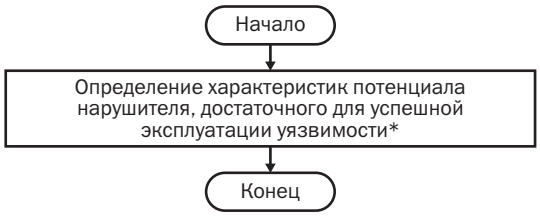
Фактор риска		Характеристики риска	Возможность количественной оценки
Величина тяжести возможных последствий от реализации опасного события		экономические последствия, вызванные нарушением критических процессов	математическое ожидание случайной величины материального ущерба
		социальные последствия, вызванные нарушением критических процессов	математическое ожидание случайной величины смертельного поражения определенного числа людей
		экологические последствия, вызванные нарушением критических процессов	математическое ожидание случайной величины аварийных выбросов в окружающую среду
		последствия угроз политической значимости объекта КИИ	—
		последствия угроз обеспечению обороны страны, безопасности государства и правопорядка	—
		степень возможного ущерба от нарушения целостности/доступности/конфиденциальности обрабатываемой в АСУ ТП информации	—
Вероятность наступления опасного события	Уязвимости системы и ее компонентов	возможная удаленность нарушителя для использования уязвимости (локальный доступ/соседняя сеть/сетевой доступ)	—
		сложность использования уязвимости	—
		требуемые привилегии для использования уязвимости	—
		необходимость взаимодействия с пользователем (необходимость действий со стороны пользователя для использования нарушителем уязвимости)	—
		возможность использования уязвимости (наличие или отсутствие кода или техники эксплуатации)	—
		уровень исправления уязвимости	—
		степень достоверности отчета о существовании уязвимости, известных технических деталей	—
	Потенциал нарушителя	время, затрачиваемое на идентификацию уязвимости и ее использование	математическое ожидание случайной величины времени обнаружения и использования уязвимости
		требующаяся техническая компетентность нарушителя для эксплуатации уязвимости	—
		знание нарушителем проекта системы и ее функционирования	—
		возможность доступа к исследуемой системе для нарушителя	—
		аппаратные средства/программное обеспечение ИТ или другое оборудование, необходимое для эксплуатации уязвимости	—

Для каждого объекта защиты АСУ ТП КИИ на основании ранее проведенной идентификации рисков ИБ АСУ ТП КИИ формируется перечень уязвимостей и проводится их анализ на основании стандарта CVSS (рис. 3).

* на основании стандарта ГОСТ Р ИСО/МЭК 18045-2013

Рис. 3. Блок-схема оценки значимости объектов защиты АСУ ТП КИИ (алгоритм 2)

Далее для каждой уязвимости оцениваются необходимые возможности нарушителя для ее успешной эксплуатации в соответствии со стандартом ГОСТ Р ИСО/МЭК 18045-2013 (рис. 4) такие как: требуемые привилегии для использования уязвимости, наличие или отсутствие кода или техники эксплуатации уязвимости, возможная удаленность нарушителя для использования уязвимости и другие.



* на основании стандарта ГОСТ Р ИСО/МЭК 18045-2013

Рис.4. Блок-схема оценки значимости объектов защиты АСУ ТП КИИ (алгоритм 3)

В результате формируется сопоставление активов, уязвимостей и возможностей нарушителей, а также определяются их характеристики, что позволяет на этапе сравнительной оценки рисков сопоставить каждой уязвимости компенсирующие меры защиты для дальнейшего снижения риска до минимального остаточного.

Согласование предлагаемого подхода к оценке рисков с практикой категорирования объектов КИИ

Согласно приказам ФСТЭК России решение о применении базовых мер обработки рисков на данный момент основывается на результатах категорирования объектов КИИ (присвоения класса защищенности АСУ). Результаты оценки рисков объектов КИИ характеризуются необходимостью согласования с результатами ранее проведенного категорирования. Например, риски объекта с третьей категорией

Таблица 2.

Сопоставление этапов управления рисками ИБ и категорирования объектов КИИ

Процесс управления рисками ИБ		Процесс категорирования объектов КИИ	
№ п/п	Этап управления рисками ИБ	№ п/п	Этап категорирования объектов КИИ
1	Установление контекста, идентификация рисков.	1	Идентификация процессов, реализующих функционирование организации.
		2	Идентификация критических процессов (которые могут привести к опасным последствиям согласно перечню показателей критериев значимости).
		3	Идентификация объектов, используемых для обработки информации, для реализации критических процессов (выделение потенциальных объектов КИИ).
		4	Формирование модели нарушителя.
		5	Формирование модели угроз (в том числе, идентификация уязвимостей).
2	Количественный и качественный анализ рисков.	6	Оценка возможных последствий в случае реализации угроз ИБ (согласно перечню показателей критериев значимости).
3	Обработка рисков.	7	Присвоение объекту КИИ определенной категории значимости или принятие решения об отсутствии такой необходимости.
4	Принятие рисков.		
5	Мониторинг и переоценка рисков.	8	Пересмотр в случае изменений значений показателей критериев значимости. Плановый пересмотр не реже, чем раз в 5 лет.

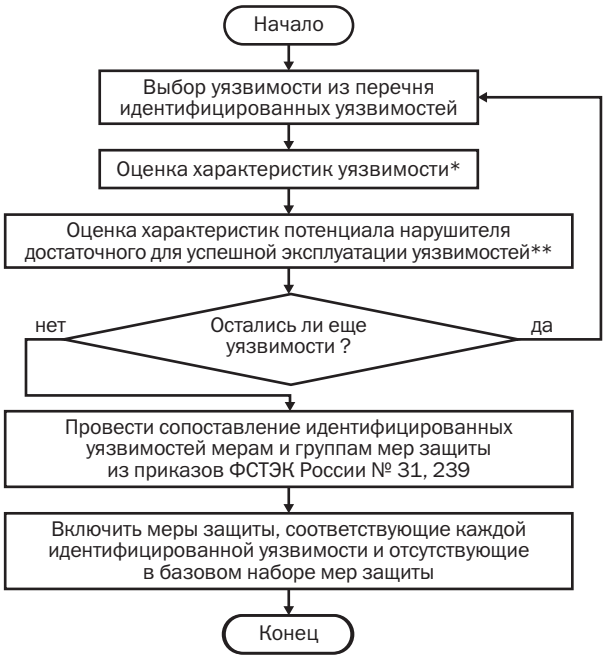
значимости не должны быть более критичными, чем риски объекта КИИ первой категории значимости. Это влечет за собой необходимость сопоставления правил категорирования с международным стандартом управления рисками ИБ. На основе анализа, проведенного в [8], ниже представлено сопоставление этапов проведения категорирования объектов КИИ согласно Постановлению Правительства № 127 и управления рисками в соответствии с ГОСТ Р ИСО/МЭК 27005-2010[10] (и проектом 2022 года[11]) (табл. 2).

Правилами категорирования определяются лишь сроки пересмотра в случае изменения значений показателей критериев значимости, которые не всегда охватывают все происходящие с системой изменения. Переоценку рисков ИБ необходимо проводить в случае модернизации и автоматизации новых процессов, применения искусственного интеллекта или биометрических технологий. Данные изменения могут не повлиять на значения показателей критериев значимости АСУ ТП КИИ, из-за чего категория значимости, а вместе с ней и применяемый базовый набор мер защиты изменены не будут, что приведет к неактуальности рисков (модели нарушителя и угроз ИБ) и нанесению ущерба субъекту КИИ.

Предложенную методику количественной и качественной оценки рисков ИБ можно включить в процесс категорирования АСУ ТП КИИ. Ниже приведена блок-схема процесса оценки рисков ИБ АСУ ТП КИИ в дополнение к проведенному категорированию объектов КИИ (рис. 5).

Идентифицированные и сопоставленные с угрозами ИБ в процессе категорирования уязвимости оцениваются по метрикам CVSS. Дополнительно оценивается потенциал нарушителя, достаточного для эксплуатации каждой из уязвимостей. Каждой угрозе сопоставляются используемые уязвимости, а каждой уязвимости – минимизирующие их меры защиты. Согласно предложенному методу оценки рисков ИБ АСУ ТП КИИ в набор мер защиты включаются те меры защиты из требований приказов ФСТЭК России № 239 и 31, что соответствуют выявленным уязвимостям и не включены в базовый набор мер защит.

Предложенная методика оценки рисков ИБ АСУ ТП КИИ может проводиться самостоятельно, так и быть включенной в дополнение к категорированию объектов КИИ. Возможность включения оценки рисков ИБ в дополнение к проводимому категорированию объектов КИИ с целью адаптации базового набора мер защиты позволяет оптимизировать и усовершенствовать обеспечение ИБ АСУ ТП КИИ.



* на основании стандарта CVSS.
** на основании ГОСТ Р ИСО/МЭК 18045-2013

Рис. 5. Оценка рисков ИБ АСУ ТП КИИ в дополнение к проводимому категорированию объектов КИИ

В качестве факторов и характеристик риска используются известные и применяемые метрики и характеристики, что не потребует дополнительного анализа, если аналогичный был уже ранее проведен.

Выводы

В рамках настоящего исследования была сформирована методика оценки рисков ИБ АСУ ТП КИИ. На примере известных инцидентов, направленных на нарушение ИБ АСУ ТП, а также на основании требований приказов ФСТЭК России была обоснована актуальность создания соответствующей методики. По итогам исследования существующих подходов количественной и качественной оценки рисков ИБ были определены достоинства и недостатки каждого из подходов применительно для АСУ ТП КИИ. Смешанный (гибридный) подход определен как компромиссный между ними. С использованием национальных и международных нормативно-методических документов и практики обеспечения информационной безопасности были определены факторы и характеристики рисков и сформированы предложения к методике количественной и качественной оценки рисков ИБ АСУ ТП КИИ. Также было проведено сопоставление процессов категорирования объектов КИИ и управления рисками ИБ и сформированы предложения по внедрению разработанной методики в дополнение к проводимому категорированию объектов КИИ.

Предлагаемый в настоящей работе подход к количественной и качественной оценке рисков ИБ АСУ

10 ГОСТ Р ИСО/МЭК 27005–2010. (введен 12.01.2011). URL: https://docs.cntd.ru/document/1200084141?ysclid=lpr75gcskw446302670

11 ГОСТ Р ИСО/МЭК 27005 (проект, первая редакция). URL: https://fstec.ru/tk-362/standarty/proekty/proekt-natsionalnogo-standarta-gost-r-iso-mek-27005

ТП КИИ ориентирован на объекты защиты и имеющиеся в системе уязвимости. Определение величины тяжести последствий основано на категории значимости объекта защиты и классе защищенности АСУ, а величина вероятности наступления опасного события определяется путем оценки уязвимостей и потенциала нарушителя. В свою очередь, потенциал нарушителя оценивается по характеристикам из ГОСТ Р ИСО/МЭК 18045-2013, предлагающего методику определения потенциала нападения нарушителя, ориентированную на имеющиеся в системе уязвимости.

Результаты проведенного анализа и выработанные рекомендации по адаптации базового набора мер защиты могут быть использованы для повышения защищенности АСУ ТП КИИ. Предложенная методика оценки рисков согласована с существующей практикой обеспечения ИБ АСУ ТП, методами управления рисками ИБ и требованиями приказов ФСТЭК России. Оценка рисков, ориентированная на объекты защиты АСУ ТП КИИ и их уязвимости, позволяет реализовать детальную оценку рисков в условиях неопределенности видов возможных нарушителей и их мотивов.

Литература

1. *Durakovskiy A. P., Gavdan G. P., Korsakov I. A., Melnikov D. A. About the cybersecurity of automated process control systems // Procedia Computer Science. 2021. № 190. P. 217–225. DOI: 10.1016/j.procs.2021.06.027.*
2. *Бабенко А. А., Магомедов Д. А. Оценка риска информационной безопасности автоматизированной системы управления технологическим процессом. Международная научно-техническая конференция «Перспективные информационные технологии» (Самара, Российская Федерация, 24–27 мая, 2021 г.). ПИТ 2021. С. 140–145.*
3. *Sembiring Z. Stuxnet Threat Analysis in SCADA (Supervisory Control and Data Acquisition) and PLC (Programmable Logic Controller) Systems // Journal of Computer Science, Information Technology and Telecommunication Engineering (JCoSITTE). 2020. № 1 (2). Pp. 96–103. DOI: 10.30596/jcositte.v1i1.5116.*
4. *Geiger M., Bauer J., Masuch M., Franke J. An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (8–11 Sept., 2020). ETFA'2020. Pp. 1537–1543. DOI: 10.1109/ETFA46521.2020.*
5. *Maynard P., McLaughlin R., Sezer S. Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems // Journal of Cybersecurit. 2020. № 6 (1). 20 p. DOI: 10.1093/cybsec/tyaa020.*
6. *Aljohani T. M. Cyberattacks on Energy Infrastructures: Modern War Weapons // Preprint Arxiv.org (Cornell University Library). 2022. 10 p. DOI: 10.48550/arXiv.2208.14225.*
7. *Chernov D., Sychugov D. Problems of Information Security and Availability of Automated Process Control Systems. 2019 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) (25–29 March 2019). ICIEAM'2019. 5 p. DOI: 10.1109/ICIEAM.2019.8743037.*
8. *Кидяева С. М., Шабурова А. В., Селифанов В. В. Вопросы организации менеджмента рисков значимых объектов критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2022. № 6. С. 82–87.*
9. *Djurayev R. Kh., Jabborov Sh. Yu., Omonov I. I. Methods for assessing the information security of telecommunications networks. // Scientific progress. 2021. № 3. С. 73–77.*
10. *Crotty J., Daniel E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment // Applied Computing and Informatics. 2022. 12 p. DOI: 10.1108/ACI-07-2022-0178.*
11. *Rahmani J. The main approaches to evaluating the effectiveness of applying the risk analysis and management methodology at energy company // T-Comm. 2022. № 9. Pp. 46–55. DOI: 10.36724/2072-8735-2022-16-9-46-55.*
12. *Минаков А. В. Оценка модели рисков информационной безопасности: характеристика, проблемы и перспективы // Экономика и бизнес: теория и практика. 2023. № 10–2 (104). С. 63–69. DOI: 10.24412/2411-0450-2023-10-2-63-69.*
13. *Canbolat S., Elbez G., Hagenmeyer V. A new hybrid risk assessment process for cyber security design of smart grids using fuzzy analytic hierarchy processes // Automatisierungstechnik. 2023. № 71 (9). Pp. 779-788. DOI: 10.1515/auto-2023-0089.*
14. *Харченко А. Ю., Харченко Ю. А. Анализ и определение рисков информационной безопасности // Вестник науки и образования. 2020. № 6–1 (84). С. 18–21.*
15. *Иваненко В. Г., Иванова Н. Д. Методика анализа стойкости автоматизированных систем управления технологическим процессом энергоблока АЭС к воздействию компьютерных атак // Безопасность информационных технологий. 2021. № 28 (4). С. 52–62. DOI: 10.26583/bit.2021.4.04.*