DOI: 10.25728/mlsd.2022.1020

О СВОЙСТВЕ ДОСТУПНОСТИ И ЕГО МЕТРИКЕ ДЛЯ АСУ ТП АЭС

Байбулатов А.А., Промыслов В.Г.
Институт проблем управления им. В.А. Трапезникова РАН
Россия, г. Москва, ул. Профсоюзная, д.65
ipu31@mail.ru

Аннотация: рассмотрена проблема оценки кибербезопасности АСУ ТП АЭС. Представлена более реалистичная, чем общепринято, триада безопасности и показано, что свойство доступности является в ней наиболее важным. Приведены результаты анализа определений доступности в международных стандартах. Предложена референтная модель доступности. Выведена метрика доступности и предложена идея для ее расчета.

Ключевые слова: доступность, метрика, кибербезопасность, АСУ ТП, АЭС.

Введение

В настоящее время энергетические системы меняются. Происходит переход от углеродной энергетики к возобновляемым источникам воды, солнца и ветра, что делает системы более сложными и взаимосвязанными. Декарбонизация ведет к созданию умных энергетических систем, децентрализации объектов и распространению умных сетей.

С каждым годом возобновляемые источники играют все большую роль в энергетике: производстве электричества, отоплении, на транспорте. По некоторым данным в 2020 году, несмотря на пандемию, годовой прирост возобновляемых источников увеличился на 45 %, в то время как употребление других источников сократилось [1].

С другой стороны, потребление электричества продолжает расти, и, хотя в наши дни возобновляемая энергетика сделала значительный скачок, и несомненно является будущим энергетических систем, она не может успеть за растущими энергетическими потребностями. Более того, возобновляемая энергетика имеет свои недостатки, наиболее существенные из них это ненадежность и непостоянство. Простыми словами, ветер дует не всегда и солнце светит не постоянно, особенно по утрам и вечерам, когда люди потребляют максимальное количество электричества. Сезонные изменения делают этот проблему еще более острой. Существует даже мнение, что солнце и ветер – это слабые источники энергии, и проблемы, связанные с ними, не технические, а скорее естественные [2].

В этой ситуации для борьбы с влиянием разрушительных углеродных источников необходимо переосмыслить атомную энергетику, которая после катастрофы на Чернобыльской АЭС находится в несколько застойном состоянии [3].

В 2019 году в мировом распределении производства электричества атомная энергетика составляла 10,4% после 15,7% гидро и 10,8% остальных не гидро-источников и отходов. В 2020 году мировое производство атомной энергии сократилось.

Что касается декарбонизации, этот процесс обычно означает переход от ископаемого топлива к возобновляемым источникам. Хотя атомная энергия не является возобновляемой, парниковые газы, которые она выделяет, чрезвычайно малы по сравнению со сжигаемым топливом. Поэтому использование атомной энергии сокращает выбросы CO_2 и является важным элементом в декарбонизации.

Другое важное преимущество атомной энергии – высокая эффективность использования пространства: любая АЭС генерирует значительное количество энергии на крошечной территории.

Однако при использование атомной энергии возникает ряд вопросов. Одна из главных проблем: как сделать атомные объекты безопасными. Большую тревогу вызывают АСУ ТП АЭС, так как чрезвычайные ситуации и аварии в управлении АЭС могут приводить к серьезным последствиям для окружающей среды и человека. Поскольку в настоящее время АСУ ТП реализованы с использованием цифровых технологий, наиболее острой становится проблема кибербезопасности.

Представляемый доклад посвящен исследованию кибербезопасности АСУ ТП АЭС и, в частности, решению задачи оценки доступности. Рассмотрен вопрос о моделирование кибербезопасности в контексте АСУ ТП АЭС и представлена более реалистичная, чем общепринято, триада кибербезопасности. Приведены результаты анализа определений доступности в международных стандартах и показано, что для АСУ ТП АЭС определение МЭК 62443 является наиболее подходящим. Предложена референтная модель доступности. Выведена метрика доступности функционирования АСУ ТП АЭС и предложен способ ее расчета.

1 О моделирование кибербезопасности и доступности для АСУ ТП АЭС

При изучении кибербезопасности обычно рассматривают три атрибута или свойства: конфиденциальность, целостность и доступность, которые вместе образуют триаду кибербезопасности. Атрибуты имеют следующий смысл. Конфиденциальность: только авторизованные пользователи или процессы должны иметь доступ к данным. Целостность: никто не должен недопустимо модифицировать данные. Доступность: авторизованные пользователи должны всегда иметь доступ к данным. Согласно триаде, обеспечение кибербезопасности означает поддержку всех этих трех свойств. Существуют также другие альтернативные более сложные модели, например, шестиэлементная модель Паркера, но обычно они основаны на тех же трех базовых принципах, более того, они не пользуются популярностью [4].

Исторически, кибербезопасность, как и информационная безопасность начиналась с конфиденциальности. Причина заключается в том, что большая часть широко использующейся информации имеет коммерческое, корпоративное или частное значение и, несомненно, должна быть конфиденциальной. Также, корректность или целостность – это свойство, которое традиционно должно поддерживаться для этого типа информации. Про доступность часто забывают. В результате, в большинстве практических приложений конфиденциальность играет ведущую роль в триаде, целостность – вторую, а доступность – последнюю.

Рассматривая геометрически классическую триаду, можно заметить, что она имеет форму равностороннего треугольника, каждая сторона которого представляет одно из свойств, которые считаются одинаково ценными. Однако, на самом деле, существует зависимость конфиденциальности и целостности от доступности [5], которая может быть объяснена следующим образом. Для того, чтобы информация была доступной, т.е., для существования свойства доступности нет необходимости поддерживать свойства конфиденциальности и целостности. Но если информация недоступна, т.е. свойство доступности не существует, то свойства конфиденциальности и целостности не имеют никакого смысла. Таким образом, более реалистичная форма триады кибербезопасности далека от равностороннего треугольника (рис. 1).

Рис. 1. Реалистичная триада кибербезопасности

Если рассматривать триаду в контексте промышленного управления, то приоритет доступности становится еще более очевидным. Действительно, АСУ ТП должна функционировать в любое время, постоянно. Даже в случае утечки или изменения информации, что означает нарушение конфиденциальности и целостности, доступность функционирования должна поддерживаться.

Тем не менее, в специальных документах, посвященных обеспечению и оценке кибербезопасности – политиках безопасности, свойства конфиденциальности и целостности обычно представлены довольно подробно, а свойство доступности лишено внимания. Рассматривая модель фундаментальных требований к промышленной кибербезопасности [6] интересно отметить, что только седьмое, последнее, требование относится к доступности.

2 Свойство доступности

2.1 Понятие доступности в международных стандартах

При исследовании доступности для АСУ ТП АЭС важно выбрать подходящее определение, поскольку разные источники дают различные определения понятию доступности. При этом следует руководствоваться специализированными стандартами ИСО, МЭК, МАГАТЭ.

В самом общем случае под доступностью понимают «свойство быть доступным и готовым к использованию по запросу авторизованного субъекта» [7].

Другое классическое определение, пришедшее из теории надежности, трактует доступность как «отрезок времени, в течение которого система способна выполнять поставленную задачу» [8].

Но что касается задачи обеспечения кибербезопасности АСУ ТП АЭС, то наиболее подходящим здесь определением можно считать следующее: «свойство, гарантирующее своевременный и надежный доступ к информации и функциям, относящимся к системе управления, и их использование» [9].

Преимущества этого определения для кибербезопасности над классическим определением теории надежности заключается в следующем. Во-первых, в случае с кибератаками невозможно набрать необходимую статистику. Во-вторых, не важно сколько времени система была работоспособной, а важно, как она будет себя вести во время и после кибератаки.

Подходя к вопросу выбора определения более формально, можно отметить, что наиболее важными характеристиками, которые следует рассматривать, являются количественная измеримость и соответствие системам важным для безопасности. В таблице 1 представлены результаты анализа определений доступности в некоторых стандартах ИСО, МЭК, МАГАТЭ.

Таблица 1. Анализ определений доступности

Стандарт	**Количественная измеримость**	**Соответствие системам важным для безопасности**
ИСО/МЭК 27000 [7]	-	+
МАГАТЭ № NP-T-1.13 [8]	+	-
МАГАТЭ № SSG-39 [10]	-	+
МЭК 62645 [11]	-	+
МЭК 62443 [9]	+	+

Формальный анализ определений [12] также подтверждает, что наиболее подходящим является определение доступности согласно МЭК 62443 [9].

2.2 Референтная модель доступности

Рассматривая уровень программного обеспечения АСУ ТП, для решения задач, связанных со свойством доступности в контексте промышленных систем управления, в частности, для количественной оценки доступности функционирования АСУ ТП АЭС удобно использовать референтную модель (рис. 2). Концепции (домены), которые составляют модель, означают следующее. Метрика доступности – это абстрактная величина, основанная на соответствующих мерах доступности, которая служит для количественной оценки доступности. Функция – это набор функций, для реализации которых служит рассматриваемая система управления. Под системой понимается архитектура системы. Платформа – это набор объектов, которые нуждаются в защите. Задержка – это измеряемая или оцениваемая величина времени прохождения сигнала с учетом архитектуры системы. Временны*е* параметры – это параметры, для которых измеряется задержка.

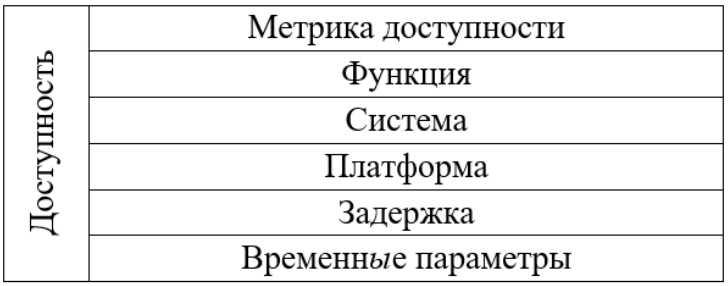

Рис. 2. Референтная модель доступности

В соответствии с референтной моделью доступность может быть выражена как следующая композиция:

$$\text{Доступность} = A \circ F \circ S \circ a \circ D(\boldsymbol{t}),$$

где A – метрика доступности, F – множество функций АСУ ТП, S – архитектура системы, a – платформа, D – множество задержек, t – временной вектор. Причем множества F и D имеют одинаковую мощность:

$$\text{card}(F) = \text{card}(D) = N,$$

где N – число функций АСУ ТП.

3 Метрика доступности

В общем случае метрики – это средство для удобной и наглядной характеристики производительности системы и принятия решений для ее улучшения. В контексте кибербезопасности метрики помогают верифицировать безопасность системы и показывать, что она соответствует заданным политикам и процедурам. Метрики применяются для выявления уязвимостей и трендов поведения системы, для повышения эффективности использования ресурсов и для определения успешности результатов применения решений в области безопасности. Обычно метрики абстрактны и субъективны, но чрезвычайно удобны в использовании. Метрики основаны на мерах – объективных, наблюдаемых и измеряемых прямыми способами показателях [13].

Возвращаясь к доступности и следуя определению МЭК 62443, в качестве меры доступности удобно выбрать время передачи сигнала от источника до приемника или задержку. Важное преимущество задержки – количественная измеримость этого показателя: в условиях нормальной эксплуатации задержка является диагностической функцией и измеряется специальным программным обеспечением [14].

На основе задержки как меры метрика доступности может быть представлена следующим образом:

$$A = 1 - \frac{1}{N}\sum_{i=1}^{N}\frac{d_i}{d_{i\max}},\ d_i \le d_{i\max}, \qquad (1)$$

где di – измеряемое или оцениваемое значение задержки для рассматриваемых временных параметров, dimax – заданное максимальное значение задержки, например, в соответствии с техническим заданием, N – число функций АСУ ТП.

Рассматривая уровень программного обеспечения АСУ ТП АЭС и следуя референтной модели (рис. 2), для расчета метрики необходимо использовать домен Система, т.е. представить систему управления состоящей из совокупности программных компонентов. Для наглядного представления зависимости между программными компонентами удобно использовать матрицу зависимости [15]:

$$\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix}, \qquad (2)$$

где cij=1, если существует переход от компонента i к компоненту j, и cij=0 в противном случае, n – число программных компонентов.

В качестве примера можно рассмотреть прямолинейное выполнение функции или программного комплекса, состоящего из 5 компонентов (рис. 3).

Рис. 3. Пример графа выполнения функции

Тогда матрица (2), соответствующая графу рис. 3, будет иметь следующий вид:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

С использованием матрицы зависимости (2) каждая задержка d_i в формуле (1) может быть выражена следующим образом:

$$d = \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}\, d_{ij}, \qquad (3)$$

где dij означает время передачи сигнала от компонента i до компонента j, если if i ≠ j, и время выполнения компонента i, если i = j.

Таким образом, метрика доступности (1) с учетом выражения для задержки (3) основана на знаниях о структуре системы и заданных максимальных значениях задержек и позволяет проводить расчеты с использованием измеряемых или оцениваемых временны*х* интервалов прохождения сигналов.

Заключение

Для того, чтобы подтвердить безопасность объектов атомной энергетики, важно исследовать и оценить кибербезопасность АСУ ТП АЭС. Поскольку для АСУ ТП АЭС свойство доступности является наиболее важным в триаде безопасности, а свойства конфиденциальности и целостности, как правило, достаточно исследованы и всесторонне представлены в политиках безопасности, наиболее острой становится проблема оценки доступности.

Определение доступности по МЭК 62443 является наиболее подходящим, поскольку оно позволяет установить количественную измеримость и проводить прямые вычисления, а также совместимо с системами важными для безопасности. Следуя этому определению, удобно выбрать время передачи сигнала от источника до приемника или задержку в качестве меры доступности.

Для всестороннего исследования свойства доступности целесообразно использовать референтную модель доступности, содержащую такие домены как Метрика доступности, Функция, Система, Платформа, Задержка, Временны*е* параметры.

С использованием референтной модели на основе задержки как меры выводится метрика доступности. Проводить расчет метрики необходимо с использованием знаний о структуре системы.

Результаты, полученные в данной работе, будут полезны для оценки свойства доступности и кибербезопасности в целом не только АСУ ТП АЭС, но и других промышленных систем управления. Дальнейшие исследования могут быть посвящены разработке более детальных методов для практического расчета метрики доступности.

Литература

1. Statistics report. Key World Energy Statistics 2021. France: IEA. 2021. – 80 p.
2. *Shellenberger M.* Apocalypse Never: Why Environmental Alarmism Hurts Us All. New York: HarperCollins Publishers. 2020. – 432 p.
3. *Brand S.* Whole Earth Discipline: An Ecopragmatist Manifesto. Viking Penguin. 2009. – 336 p.
4. *Andress J.* The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Oxford: Syngress, 2014. – 217+xxii p.
5. *Qadir S., Quadri S.M.K.* Information Availability: An Insight into the Most Important Attribute of Information Security // Journal of Information Security, vol. 7. 2016. – P. 185-194.
6. IEC 62443-1-1 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models. Geneva: IEC. 2009. – 81 p.
7. ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO. 2018. – 32 p.
8. IAEA Nuclear Energy Series No. NP-T-1.13 «Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants». Vienna: IAEA. 2015. – 68+iv+viii p.
9. IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Geneva: IEC. 2013. – 170 p.
10. IAEA Safety Standards Series № SSG-39 «Design of Instrumentation and Control Systems for Nuclear Power Plants». Vienna: IAEA. 2016. – 166+xvi p.
11. IEC 62645 Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems. Geneva: IEC. 2014. – 93 p.
12. *Baybulatov A.A., Promyslov V.G.* Industrial Control System Availability Assessment with a Metric Based on Delay and Dependency // IFAC-PapersOnLine. Elsevier, Amsterdam, vol. 54, issue 13. 2021. – P. 472-476.
13. *Black P.E., Scarfone K., Souppaya M.* Cyber Security Metrics and Measures // Voeller, J.G. (ed.), Wiley Handbook of Science and Technology for Homeland Security. John Wiley & Sons. 2008. – P. 1-8.
14. *Promyslov V.G., Masolkin S.I.* NPP APCS diagnostics implementation as a routine task of APCS // IFAC Proceedings Volumes, vol. 42, no. 2. 2009. – P. 221-225.
15. *Qadir S., Quadri S.M.K.* Information Availability: An Insight into the Most Important Attribute of Information Security // Journal of Information Security, vol. 7. 2016. – P. 185-194.