Идентифицированные и сопоставленные с угрозами ИБ в процессе категорирования уязвимости оцениваются по метрикам Common Vulnerability Scoring System (CVSS) – открытого международного стандарта, используемого для оценки уязвимостей. Дополнительно оцениваются возможности нарушителя (согласно стандарту ГОСТ Р ИСО/МЭК 18045–2013), достаточные для эксплуатации каждой из уязвимостей, такие как требуемые привилегии для использования уязвимости, наличие или отсутствие кода или техники эксплуатации уязвимости, возможная удаленность нарушителя для использования уязвимости и другие. Каждой угрозе сопоставляются используемые уязвимости, а каждой уязвимости – минимизирующие их меры защиты. Согласно предложенному методу оценки рисков ИБ транспортных систем в набор мер защиты включаются те меры защиты из требований приказа ФСТЭК России № 239, которые соответствуют выявленным уязвимостям и не включены в базовый набор мер защит.

Возможность интеграции оценки рисков ИБ в процесс категорирования объектов КИИ с целью адаптации базового набора мер защиты способствует оптимизации и улучшению обеспечения ИБ транспортных систем. В качестве факторов и характеристик риска используются известные метрики и характеристики, что исключает необходимость проведения дополнительного анализа, если аналогичная работа уже была выполнена ранее. Разработанные рекомендации по адаптации базового набора мер защиты могут быть применены для повышения уровня защиты транспортных систем как объектов КИИ.

Список литературы

1 **Кидяева, С. М.** Вопросы организации менеджмента рисков значимых объектов критической информационной инфраструктуры / С. М. Кидяева, А. В. Шабурова, В. В. Селифанов // Интерэкспо Гео-Сибирь. – 2022. – № 6. – С. 82–87.

2 **Иваненко, В. Г.** Оценка рисков информационной безопасности автоматизированных систем управления технологическим процессом / В. Г. Иваненко, Н. Д. Иванова // Вопросы кибербезопасности. – 2024. – № 1 (59). – С. 116–123.

УДК 004.056

ФАКТОРЫ И ХАРАКТЕРИСТИКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНЫХ СИСТЕМ

Н. Д. ИВАНОВА
Российский университет транспорта (МИИТ), г. Москва

До относительно недавнего времени задача обеспечения информационной безопасности (ИБ) не считалась приоритетной для транспортных систем [1]. ИБ таких систем обеспечивалась за счет контроля физического доступа к компонентам – специализированным программно-аппаратным комплексам, использующим проприетарные протоколы. Современные транспортные системы представляют собой сложные многокомпонентные системы, использующие новейшие технологии. Увеличение сложности таких систем, их модернизация, распределенная многокомпонентная архитектура приводят к росту угроз ИБ на транспортные системы.

Целью настоящего исследования является формирование перечня факторов и характеристик рисков ИБ транспортных систем как объектов критической информационной инфраструктуры (КИИ).

Под угрозой ИБ понимается потенциальное опасное событие, риск ИБ определяет степень опасности влияния нежелательного события на систему или ее компоненты. Согласно государственным и международным стандартам, риск чаще всего характеризуется как сочетание тяжести и вероятности опасного события. Стандарты, касающиеся риска ИБ, рассматривают его как потенциальную возможность использования уязвимости для создания угрозы, что может привести к негативным последствиям для организации. Следовательно, основными факторами риска являются тяжесть последствий и вероятность опасного события. Вероятность возникновения события ИБ может быть охарактеризована исходной защищенностью системы (уязвимостями системы и ее компонентов) и потенциалом нарушителя.

Таким образом, риск ИБ можно определить следующими основными факторами:

– величина тяжести возможных последствий от наступления опасного события;

– вероятность наступления опасного события, в свою очередь определяемая факторами «степень опасности уязвимостей системы и ее компонентов»; «потенциал нападения нарушителя».

Согласно требованиям приказа ФСТЭК России № 239, величину тяжести возможных последствий от наступления опасного события для обеспечения ИБ транспортных систем характеризуют значения показателей критериев значимости объектов КИИ РФ и степень возможного ущерба от нарушения свойств конфиденциальности, целостности и доступности информации.

Оценка опасности уязвимостей транспортных систем реализуется с помощью стандарта Common Vulnerability Scoring System (CVSS), представляющего собой открытый международный стандарт для оценки уязвимостей, который используется, в том числе, в банке данных угроз (БДУ) ФСТЭК России.

Для оценки потенциала нарушителя может применяться ГОСТ Р ИСО/МЭК 18045-2013, который предлагает методику оценки потенциала нападения нарушителя, ориентированную на имеющиеся в системе уязвимости, что согласуется с определенным в [2] подходом к обеспечению ИБ транспортных систем.

В таблице 1 приведены факторы и характеристики рисков ИБ транспортных систем, включая возможные методы количественной оценки.

Таблица 1 – **Факторы и характеристики рисков ИБ транспортных систем**

Фактор		Характеристика	Количественная оценка
Величина тяжести возможных последствий от наступления 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	–	–
		–	–
		–	–
		–	–
		–	–
		–	–
		–	–
	Потенциал нападения 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 или другое оборудование, необходимое для эксплуатации уязвимости	–

Если количественная оценка рисков невозможна, следует провести смешанную оценку: качественно определенные характеристики переводить в количественные с использованием числовых шкал, сопоставляющих значения лингвистических переменных с числовыми показателями. Большинство предложенных характеристик основываются на отечественных или зарубежных методических материалах, что дает возможность оценивать риски ИБ транспортных систем, опираясь на результаты ранее проведенных исследований, если таковые имеются.

Список литературы

1 **Kavallieratos, G.** Managing Cyber Security Risks of the Cyber-Enabled Ship / G. Kavallieratos, S. Katsikas // Marine Science and Engineering. – 2020. – No. 8 (768). – P. 19. – DOI : 10.3390/jmse8100768/.

2 **Михалевич, И. Ф.** Управление рисками информационной безопасности интеллектуальных транспортных систем внутреннего водного транспорта управления на транспорте [Электронный ресурс] / И. Ф. Михалевич, Н. Д. Иванова, В. В. Якунчиков // Транспорт России: проблемы и перспективы-2023 : материалы Междунар. науч.-практ. конф. – СПб., 2023. – Режим доступа : https://www.elibrary.ru/item.asp?id=65700396. – Дата доступа : 20.08.2024.