УДК 004.056

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНЫХ СИСТЕМ

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

Оценка рисков информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ) является основой для принятия решений, направленных на предотвращение отказов или минимизацию их негативных последствий. Растущее количество компьютерных атак на объекты КИИ стало причиной разработки соответствующих нормативных документов и требований к ИБ транспортных систем. В соответствии с приказом ФСТЭК России № 239, базовый набор мер защиты информации должен быть адаптирован, если он не способен предотвратить все угрозы ИБ. Однако в приказах ФСТЭК России отсутствуют критерии для адаптации, что создает необходимость разработки методики оценки рисков ИБ транспортных систем.

Согласно [1] каждый новый нормативно-правовой акт или методический документ может создавать новые потенциальные риски для защищаемой организации. Поэтому для оценки рисков ИБ транспортных систем целесообразно проанализировать применимость существующих нормативно-правовых актов, государственных и международных стандартов и методических документов. Учет этих документов в контексте управления рисками ИБ может стать основой для формирования рекомендаций по поддержанию актуальности результатов оценки рисков ИБ транспортных систем.

Целью настоящего исследования является формирование предложений по внедрению методики оценки рисков ИБ транспортных систем в процесс категорирования объектов КИИ с целью уточнения базового набора мер защиты.

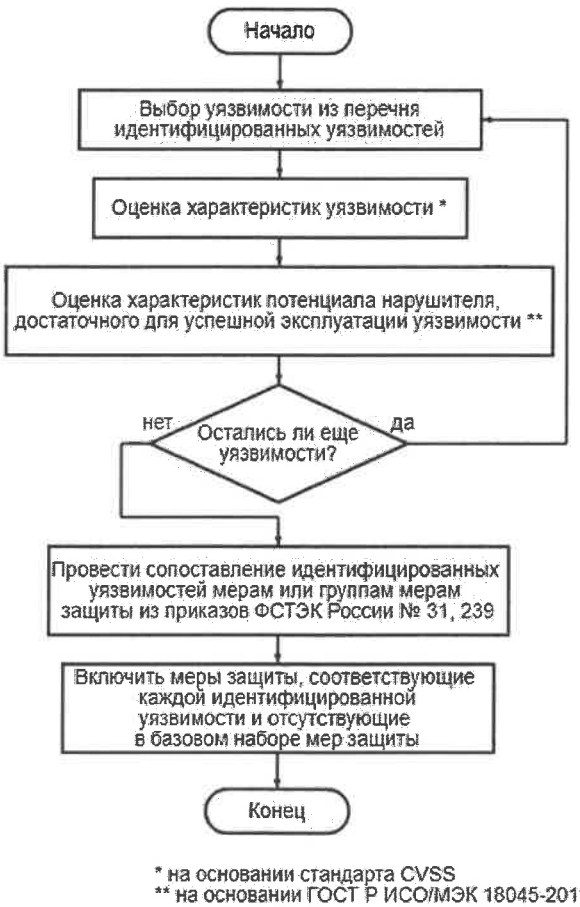

Рисунок 1 – Блок-схема оценки рисков ИБ транспортных систем в дополнение к проводимому категорированию объектов КИИ

Согласно приказу ФСТЭК России № 239, решение о применении базовых мер защиты основано на результатах категорирования объектов КИИ. Результаты оценки рисков объектов КИИ не должны противоречить ранее проведенному категорированию транспортной системы как объекта КИИ. Например, риски объекта КИИ третьей категории значимости не должны быть более критичными по сравнению с рисками объекта первой категории. Вследствие этого возникает необходимость сопоставления правил категорирования с международными стандартами управления рисками ИБ (анализ представлен в [1]). Правилами категорирования определяются лишь сроки пересмотра в случае изменения значений показателей критериев значимости, которые не всегда охватывают все происходящие с системой изменения. Переоценка рисков ИБ должна проводиться при любых изменениях в системе: модернизации и автоматизации процессов, применении искусственного интеллекта или биометрических технологий. Эти изменения могут не повлиять на показатели критериев значимости объектов КИИ, в результате чего категория значимости и применяемый базовый набор мер защиты останутся неизменными, что приведет к потере актуальности модели нарушителя и угроз ИБ и, следовательно, к возможному ущербу субъекту КИИ [2].

На рисунке приведена блок-схема процесса оценки рисков ИБ транспортных систем в дополнение к проведенному категорированию объектов.

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.