Абдулова Е.А.

Об одном подходе к управлению рисками критической инфраструктуры

Аннотация: В работе рассматривается подход к управлению рисками критической инфраструктуры. Предлагается пятиэтапный подход, включающий конкретизацию целей и задач процесса, определение инфраструктуры, оценку и анализ риска, мероприятия по управлению рисками и измерения.

Ключевые слова: критическая инфраструктура, риск, управление рисками, оценка и анализ риска, угрозы, последствия

Критические инфраструктуры (КИ) играют жизненно важную роль в обществе, обеспечивая выполнение многих ключевых функций и услуг [1]. Концепция «критической инфраструктуры» постоянно развивается, отражает текущие проблемы и реагирует на новые вызовы, особенно с точки зрения кибербезопасности и устойчивости. Критические инфраструктуры, включая энергетические, коммуникационные и банковские сети, механизмы общественного здравоохранения и безопасности, как правило, представляют собой совокупность функций, выполняемых широким кругом заинтересованных сторон. Поэтому управление рисками для этих инфраструктур является общей ответственностью, требующей тесного и постоянного сотрудничества между заинтересованными сторонами.

Эффективное управление рисками КИ фокусируется на повышении устойчивости на основе оценки критичности или важности данной инфраструктуры, а также характера и уровня рисков, с которыми она сталкивается. Заинтересованные стороны совместно определяют наиболее важные для них активы, а затем совместно оценивают, расставляют приоритеты и управляют соответствующими рисками.

Риск определяется как вероятность нежелательного исхода в результате инцидента, события или происшествия, определяемая его вероятностью и соответствующими последствиями [2]. На нее влияют характер и величина угрозы или опасности, уязвимости от

этой угрозы или опасности и возможные последствия. Информация о рисках позволяет заинтересованным сторонам, от владельцев объектов и операторов до федеральных агентств, определять приоритеты действия по управлению.

Особенно важное значение имеют критические информационные инфраструктуры (КИИ), т.е. обширные и пересекающиеся сети информационно-коммуникационных технологий, которые связывают и эффективно обеспечивают надлежащее функционирование других ключевых инфраструктур [3-6]. Фактически, КИИ не только поддерживают все другие критические инфраструктуры, но и способствуют наступлению «информационной эпохи».

В отличие от физических активов КИ, таких как здания, плотины или электростанции, критические информационные инфраструктуры являются виртуальными или «логическими» по своей природе. То есть они состоят из сложных, распределенных систем программного обеспечения, оборудования и услуг, функционирующих вместе для достижения желаемого результата.

В работе представлен подход к управлению рисками критической инфраструктуры, который имеет структуру, представленную на рисунке 1. Такая структура позволяет интегрировать стратегии, возможности и структуры управления, для принятия решений с учетом рисков, связанных с критической инфраструктурой. Данный подход к управлению рисками критической инфраструктуры может применяться ко всем угрозам и опасностям, включая киберинциденты, стихийные бедствия, антропогенные угрозы безопасности и террористические акты, хотя для понимания каждого из них могут использоваться разная информация и методологии.

Рисунок 1 – Структура подхода к управлению рисками КИ

Кроме того, подход к управлению рисками критической инфраструктуры дополняет и поддерживает процесс выявления и оценки угроз и опасностей. Этот процесс включает в себя идентификацию угроз и опасностей и то, как они могут повлиять на сообщество, и определение того, как лучше всего смягчить эти угрозы и опасности, исходя из текущих возможностей и требований к ресурсам.

Предлагаемый подход к управлению рисками критической инфраструктуры не предназначен для замены уже используемых моделей или процессов. Скорее, он поддерживает общий, унифицирующий подход к управлению рисками, который все заинтересованные стороны могут использовать, связывать и согласовывать со своими собственными моделями и действиями управления рисками.

Предлагаемый подход к управлению рисками критической инфраструктуры может быть адаптирован и применен к активу, системе, сети и т.д., в зависимости от фундаментальных характеристик решений, которые он призван поддерживать, и характера соответствующей инфраструктуры. Представленный ниже подход к управлению рисками критической инфраструктуры включает следующие этапы.

– Цели и задачи. На этом этапе необходимо определить результаты, условия, конечные точки или целевые показатели эффективности, которые в совокупности описывают эффективное и желаемое состояние управления рисками.

– Определение инфраструктуры. На этом этапе необходимо определить активы, системы и сети, которые вносят вклад в критически важные функции, а также необходимо собрать информацию, относящуюся к управлению рисками, включая анализ зависимостей и взаимозависимостей.

– Оценка и анализ рисков. На этом этапе проводится оценка риска с учетом потенциальных прямых и косвенных последствий инцидента, известных уязвимостей для различных потенциальных угроз или опасностей, а также имеющейся информации об угрозах. Риск для критической инфраструктуры является функцией угрозы, уязвимости и последствий, где: угроза относится к природным и антропогенным источникам, в части и их движущей силы, целей и возможностей, а также к вероятности того, что угроза существует или возникнет; уязвимость – это слабое место или ограничение,

которое может быть использовано угрозой; последствия – выражаются стоимостью для оценки риска. На рисунке 2 показана взаимосвязь между риском, угрозами, уязвимостью и последствиями.

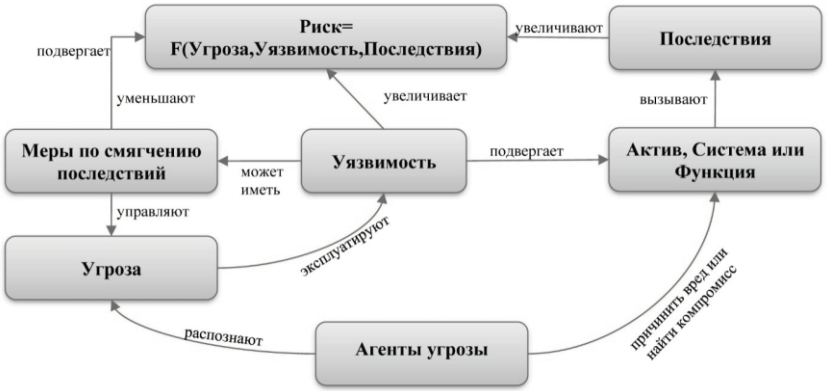

Рисунок 2 – Связь между риском, угрозами, уязвимостью и последствиями

Мероприятия по управлению рисками. На этом этапе принимаются решения и внедряются подходы к управлению рисками для контроля, принятия, передачи или предотвращения рисков. Подходы могут включать меры по предотвращению, защите, смягчению, реагированию и восстановлению.

Измерения. На основе использования метрик проводится определение прогресса и оценки эффективности усилий по обеспечению и повышению устойчивости критической инфраструктуры.

Используя показатели для оценки эффективности усилий заинтересованных сторон по достижению приоритетов в рамках критической инфраструктуры, заинтересованные стороны могут корректировать и адаптировать свои подходы к безопасности и устойчивости с учетом достигнутого прогресса, а также изменений в угрозах и других средах. Метрики используются для сосредоточения внимания на конкретных вопросах безопасности и устойчивости, которые требуют дополнительных.

Метрики также служат механизмом обратной связи для других аспектов подхода к управлению рисками критической инфраструктуры. Они отображают прогресс в достижении целей и предоставляют аналитикам информацию для корректировки оценок рисков. Например, метрики показывают эффективность действий по обеспечению безопасности и устойчивости, а также степень, в которой эти действия снижают риски.

Представленный подход поддерживает интегрированный и непрерывный процесс с циклами обратной связи и повторяющимися шагами, что позволяет лицам, принимающим решения, отслеживать прогресс и реализовывать действия по повышению безопасности и устойчивости критической инфраструктуры с течением времени. Физические, кибернетические (виртуальные) и человеческие элементы критической инфраструктуры следует рассматривать как часть каждого этапа подхода к управлению рисками КИ.

Литература:

1. *Markopoulou D., Papakonstantinou V.* The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular // Computer Law & Security Review. – 2021. – Vol. 41. – Article 105502.

2. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2020. – 20 с.

3. *Калашников А.О., Сакрутина Е.А.* Модель оценки рискового потенциала объектов критической инфраструктуры атомных электростанций / Труды 11-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD’2018) (1-3 октября 2018 г. Москва). – М.: ИПУ РАН, 2018. – Т. 2. – С. 457-461.

4. *Калашников А.О., Сакрутина Е.А.* Модель прогнозирования рискового потенциала значимых объектов критической информационной инфраструктуры // Информация и безопасность. – 2018. – Т. 21. № 4. – С. 465-470.