ОБЕСПЕЧЕНИЕ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ ЗА СЧЕТ СНИЖЕНИЯ РИСКОВ ОТ КИБЕРУГРОЗ


Б.Ф. Безродный


Л.В. Любимова

Рассмотрен подход к обеспечению техносферной безопасности с точки зрения снижения рисков возникновения опасных воздействий на человека и окружающую среду посредством киберугроз. Описана методика количественной оценки эффективности стратегий защиты автоматизированных систем управления железнодорожным транспортом от киберугроз.

Ключевые слова: безопасность, снижение рисков, ущерб, АСУЖТ, киберугроза, оценка эффективности

EDN: DXYAEA

Техносферная безопасность обеспечивается уменьшением воздействия на человека и окружающую среду вредных и опасных производственных факторов. На сегодняшний день с учетом цифровизации железной дороги одним из наиболее очевидных опасных внешних воздействий являются киберугрозы. Это – возможность проникновения извне в автоматизированные системы управления железнодорожным транспортом (далее – АСУЖТ) с целью нарушения их штатного функционирования. При этом особое значение имеют организационные и технические меры, которые используются на железной дороге для противодействия киберугрозам. В связи с этим, в настоящей статье рассмотрена методика оценки эффективности средств защиты АСУЖТ от киберугроз.

Различные применяемые комбинации организационных и технических мер можно назвать стратегиями защиты АСУЖТ. Оценка, в том числе, количественная, результативности применения стратегий защиты необходима для дальнейшего анализа с целью поддержки и улучшения систем обеспечения кибербезопасности. Для оценки эффективности информационной и кибербезопасности существует множество методик, основанных на сложных математических моделях [1]. Применительно к АСУЖТ авторы статьи предлагают в качестве критерия оценки использовать размер снижения величины прогнозируемого ущерба, наносимого инфраструктуре и подвижному составу ОАО «РЖД», регионам и территориям, по которым пролегают железнодорожные магистрали, а также перевозимым пасса-

Безродный Борис Федорович, доктор технических наук, профессор, начальник Отдела обеспечения кибербезопасности – заместитель начальника Центра кибербезопасности Научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте (АО «НИИАС»), заведующий кафедрой «Прикладная математика» Московского автомобильно-дорожного государственного технического университета (МАДИ). Область научных интересов: кибербезопасность автоматизированных систем управления железнодорожным транспортом. Автор 300 научных работ, в том числе двух монографий. Имеет один патент на изобретение.

Любимова Лариса Владимировна, главный специалист по информационной безопасности Отдела обеспечения кибербезопасности Центра кибербезопасности Научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте (АО «НИИАС»). Область научных интересов: кибербезопасность автоматизированных систем управления железнодорожным транспортом. Автор 10 научных работ.

жирам и грузам по причине форс-мажорных (не страхуемых) событий, вызванных кибератаками.

Чтобы оценить эффективность применения той или иной стратегии защиты АСУЖТ через размер снижения величины прогнозируемого ущерба от нарушений штатного функционирования этих систем, необходимо рассчитать указанный ущерб для трех случаев:

1. Кибератаки на АСУЖТ отсутствуют.

2. На АСУЖТ направлены кибератаки, но никакие стратегии защиты не применяются.

3. На АСУЖТ направлены кибератаки и применяются стратегии защиты, эффективность которых рассчитывается.

При этом средний ущерб от кибератак на АСУЖТ следует рассчитывать как оценку математического ожидания величины ущерба [2] с учетом распределения нежелательных событий, вызванных реализацией киберугроз, по четырем категориям исходя из возможных негативных последствий. Согласно принятой на железнодорожном транспорте классификации такими категориями являются:

- опасный отказ;
- защитный отказ;
- отказ технических (программно-аппаратных) средств;
- событие, не нарушающее штатное функционирование системы.

Нейтрализацией угрозы безопасности при этом является перевод нежелательного события, наступающего в результате ее реализации, в более низкую, с точки зрения величины ущерба, категорию (вплоть до категории, не наносящей ущерб).

Размер ущерба С, наносимого по причине кибератак на АСУЖТ, можно оценить (рассчитать) по формуле:

$$C \approx (\lambda_{ОО} C_{ОО} + \lambda_{ОЗ} C_{ОЗ} + \lambda_{ТС} C_{ТС} + \lambda_{БУ} C_{БУ}) \Delta t, \qquad (1)$$

где $C_{ОО}$ – средний ущерб от одного опасного отказа АСУЖТ;

$C_{ОЗ}$ – средний ущерб от одного защитного отказа АСУЖТ;

$C_{ТС}$ – средний ущерб от одного отказа технических (программно-аппаратных) средств АСУЖТ;

$C_{БУ}$ – средний ущерб от одного события, не приводящего к нарушению штатного функционирования АСУЖТ;

$\lambda_{ОО}$ – интенсивность потоков опасных отказов АСУЖТ;

$\lambda_{ОЗ}$ – интенсивность потоков защитных отказов АСУЖТ;

$\lambda_{ТС}$ – интенсивность потоков отказов технических (программно-аппаратных) средств АСУЖТ;

$\lambda_{БУ}$ – интенсивность потоков событий, не приводящих к нарушению штатного функционирования АСУЖТ;

Δt – время наблюдения.

Так как события, не приводящие к нарушению штатного функционирования АСУЖТ, не наносят ущерб, то $C_{БУ}=0$. И, следовательно, учитывать интенсивность потоков таких событий в предлагаемой авторами методике нецелесообразно.

Размер интенсивности потоков нежелательных событий является величиной переменной и в зависимости от рассматриваемой ситуации (в части влияния на АСУЖТ различных сценариев кибератак и стратегий защиты) принимает разные значения. Интенсивность потоков нежелательных событий λ, для каждой из четырех категорий, включает в себя эталонную интенсивность потока нежелательных событий λ^0 (в случае отсутствия кибератак на АСУЖТ) и величины $\Delta\lambda$ и $\Delta\lambda'$, на которые изменяется λ^0, когда на АСУЖТ направлены кибератаки без применения стратегий защиты и с применением таковых соответственно.

Эталонные значения интенсивности потоков нежелательных событий определяются из технических условий, ГОСТ 33432-2015, а также нормативных документов, конструкторской и проектной документации на АСУЖТ.

В случае, когда кибератаки на АСУЖТ отсутствуют, интенсивности потоков нежелательных событий равны своим эталонным значениям, т.е. $\lambda=\lambda^0$. Тогда величину ущерба обозначим C_0 и рассчитаем по формуле (1)

$$C_0 \approx (\lambda^0_{ОО} C_{ОО} + \lambda^0_{ОЗ} C_{ОЗ} + \lambda^0_{ТС} C_{ТС}) \Delta t. \qquad (2)$$

Кибератаки, осуществляемые по разным сценариям, являются событиями несовместными. В случае, когда на АСУЖТ направлены кибератаки, но никакие стратегии защиты не применяются, интенсивность потоков нежелательных событий увеличивается на величину $\Delta\lambda$, т.е.

$$\lambda = \lambda^0 + \Delta\lambda. \qquad (3)$$

Найти величину $\Delta\lambda$ можно, зная вероятности успешной реализации кибератаки на АСУЖТ, полученные на основании экспертных оценок, либо по результатам экспериментальных исследований по оценке актуальных для АСУЖТ киберугроз. С учетом реальной статистики за исследуемые несколько лет известно, что кибератаки на АСУЖТ, являются редкими событиями, а их поток можно считать простейшим, т.е. пуассоновским

$$P_{ОО} = 1 - e^{-\Delta\lambda_{ОО}\Delta t}, \qquad (4)$$

$$P_{ОЗ} = 1 - e^{-\Delta\lambda_{ОЗ}\Delta t}, \quad (5)$$

$$P_{ТС} = 1 - e^{-\Delta\lambda_{ТС}\Delta t}, \quad (6)$$

$$P_{БУ} = 1 - e^{-\Delta\lambda_{БУ}\Delta t}, \quad (7)$$

где $P_{ОО}$ – вероятность успешной реализации кибератаки, приводящей к опасному отказу АСУЖТ;

$P_{ОЗ}$ – вероятность успешной реализации кибератаки, приводящей к защитному отказу АСУЖТ;

$P_{ТС}$ – вероятность успешной реализации кибератаки, приводящей к отказу технических (программно-аппаратных) средств АСУЖТ;

$P_{БУ}$ – вероятность успешной реализации кибератаки, приводящей к событию, не нарушающему штатного функционирования АСУЖТ.

При оценке вероятностей успешной реализации кибератаки на АСУЖТ должна учитываться ее реализуемость. Т.е. каждая вероятность $P_{ОО}$, $P_{ОЗ}$, $P_{ТС}$, $P_{БУ}$ – это произведение вероятности выбора конкретного сценария кибератаки из всего набора возможных на вероятность достижения цели конкретного воздействия.

$$P = P^a \cdot P^y, \quad (8)$$

где P^a – вероятность выбора сценария кибератаки;

P^y – вероятность успеха кибератаки.

Вероятности P^a и P^y можно определить на основе экспертного опроса опытных сотрудников службы информационной безопасности и специалистов-железнодорожников, соответственно, либо по результатам экспериментальных исследований, а именно серии пентестов, реализующих различные сценарии кибератак на АСУЖТ. Рекомендованное количество пентестов для каждого сценария кибератаки составляет 100 и более.

Используя зависимость интенсивности потока нежелательных событий от вероятности успешной реализации кибератаки, из формул (4–8) получаем

$$\Delta\lambda_{ОО} \approx \frac{\ln\left(1 - P^a_{ОО} \cdot P^y_{ОО}\right)}{\Delta t}; \quad (9)$$

$$\Delta\lambda_{ОЗ} \approx \frac{\ln\left(1 - P^a_{ОЗ} \cdot P^y_{ОЗ}\right)}{\Delta t}; \quad (10)$$

$$\Delta\lambda_{ТС} \approx \frac{\ln\left(1 - P^a_{ТС} \cdot P^y_{ТС}\right)}{\Delta t}; \quad (11)$$

$$\Delta\lambda_{БУ} \approx \frac{\ln\left(1 - P^a_{БУ} \cdot P^y_{БУ}\right)}{\Delta t}. \quad (12)$$

Тогда формула (1) примет вид

$$C \approx ((\lambda^0_{ОО} + \Delta\lambda_{ОО})C_{ОО} + (\lambda^0_{ОЗ} + \Delta\lambda_{ОЗ})C_{ОЗ} + (\lambda^0_{ТС} + \Delta\lambda_{ТС})C_{ТС})\Delta t. \quad (13)$$

Для третьего случая, когда на АСУЖТ направлены кибератаки и применяются стратегии защиты, интенсивность потоков нежелательных событий будет изменяться на величину $\Delta\lambda'$, т.е.

$$\lambda = \lambda^0 + \Delta\lambda'. \quad (14)$$

Величина $\Delta\lambda'$ определяется из данных об изменении категории нежелательного события после применения различных стратегий защиты АСУЖТ. Для каждой конкретной АСУЖТ киберугрозы распределяются на группы от 1 до 4 в зависимости от последствий их реализации. Величина $\Delta\lambda$ – это интенсивность потоков нежелательных событий для группы. Она сохраняется, но при противодействии киберугрозам различными мерами и средствами защиты может перераспределяться, так как киберугрозы могут переходить из одной группы в другую. Как правило, при эффективном применении мер и средств защиты киберугрозы из группы событий, приводящих к опасным отказам, переходят в группу событий, приводящих к защитным отказам, а киберугрозы из группы событий, приводящих к отказам технических (программно-аппаратных) средств, переходят в группу событий, не нарушающих штатное функционирование системы. Внутри групп у каждой кибератаки появляется своя величина $\overline{\Delta\lambda}^i$, сумма всех $\overline{\Delta\lambda}^i$ равна $\Delta\lambda$.

$$\Delta\lambda = \sum_{i=1}^{n} \overline{\Delta\lambda}^i, \quad (15)$$

где n – количество киберугроз в группе.

Тогда

$$\Delta\lambda' = \Delta\lambda \pm \sum_{j=1}^{m} \overline{\Delta\lambda}^{ij}, \text{ для } m \le n, \quad (16)$$

где m – количество киберугроз, перешедших из одной группы в другую.

Величина ущерба C' в таком случае будет равна

$$C' = ((\lambda^0_{ОО} + \Delta\lambda'_{ОО})C_{ОО} + (\lambda^0_{ОЗ} + \Delta\lambda'_{ОЗ})C_{ОЗ} + (\lambda^0_{ТС} + \Delta\lambda'_{ТС})C_{ТС})\Delta t. \quad (17)$$

Рассчитав значения величины ущерба для трех разных случаев наличия или отсутствия кибератак и стратегий защиты, можно сделать вывод об эффективности применяемых стратегий защиты АСУЖТ. Для этого необходимо рассчитать величины ΔC_A и ΔC_B

$$\Delta C_A = C - C', \quad (18)$$

$$\Delta C_B = C' - C_0, \quad (19)$$

где ΔC_A – это величина, которая показывает разницу между величиной ущерба в случае, когда на АСУЖТ направлены кибератаки, но никакие стратегии защиты не применяются, и величиной ущерба, когда на АСУЖТ направлены кибератаки и применяются стратегии защиты;

ΔC_B – это величина, которая показывает разницу между величиной ущерба в случае, когда на АСУЖТ направлены кибератаки и применяются стратегии защиты, и величиной ущерба, когда кибератаки на АСУЖТ отсутствуют.

Стратегию защиты от кибератак, направленных на АСУЖТ, следует считать более эффективной по сравнению с другой стратегией защиты, если величина ΔC_A для нее больше, чем у альтернативной стратегии, а ΔC_B наоборот меньше. Поэтому наиболее предпочтительной следует считать стратегию защиты от кибератак, у которой параметр ΔC_A максимален среди всех комплексов защитных мер, а параметр ΔC_B – минимален.

Заключение

Обеспечение техносферной безопасности за счет снижения опасных воздействий на человека и окружающую среду возможно при эффективном применении стратегий защиты АСУЖТ от киберугроз. Для количественной оценки эффективности целесообразно выбрать в качестве ее критерия размер снижения величины ущерба от форс-мажорных (нестрахуемых) событий, вызванных кибератаками. Такой подход дает возможность определить наиболее эффективную стратегию защиты АСУЖТ от кибератак, опираясь на экспертную оценку вероятности реализации этих кибератак и (или) результаты экспериментальных исследований киберзащищенности АСУЖТ, что позволит сократить опасные воздействия и обеспечить техносферную безопасность.

Литература

1. Хайретдинов, Р. Оценка эффективности информационной безопасности / Р. Хайретдинов. –Текст: непосредственный // Information Security / Информационная безопасность. –2014. –№2. –С. 48–49.

2. Безродный, Б.Ф. Оценка эффективности решений по повышению киберзащищенности объектов ЖАТ / Б.Ф. Безродный, Л.В. Любимова. –Текст: непосредственный // Интеллектуальные транспортные системы: материалы Международной научно-практической конференции, Москва, 26 мая 2022 года. –Москва: Российский университет транспорта, 2022. –С. 487–489.