УДК 656.2.08

П. М. БУЙ, кандидат технических наук, Белорусский государственный университет транспорта, г. Гомель.

ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Приведены особенности обеспечения кибербезопасности инфокоммуникационных систем железнодорожного транспорта. Обоснована необходимость обеспечения как информационной, так и функциональной безопасности инфокоммуникационных систем. Даны понятия угрозы кибербезопасности, уязвимости инфокоммуникационной системы, кибератаки, риска и киберзащищенности. Предложен метод оценки рисков кибербезопасности инфокоммуникационных систем железнодорожного транспорта. Приведены необходимые критерии и рекомендации по баллам, выставляемым экспертами. Представлена методика оценки киберзащищенности инфокоммуникационных систем железнодорожного транспорта.

Белорусская железная дорога призвана обеспечивать потребности государства, юридических и физических лиц в железнодорожных перевозках, а также работах и услугах, оказываемых железнодорожным транспортом. В связи с этим железнодорожный комплекс Республики Беларусь имеет особое стратегическое значение, являясь связующим звеном единой экономической системы и обеспечивая стабильную деятельность промышленных предприятий. Кроме того, это еще и самый доступный вид транспорта для граждан Республики Беларусь.

В последнее время в рамках стремительной информатизации и компьютеризации на Белорусской железной дороге вводятся в эксплуатацию современные инфокоммуникационные системы. Инфокоммуникационная система – это совокупность технических средств, обеспечивающих сбор, хранение, обработку, распределение, передачу и прием информации. В сфере железнодорожного транспорта довольно часто инфокоммуникационные системы используются не только для передачи и обработки информации, но и для организации автоматизированных систем управления технологическими процессами (АСУ ТП).

Концепция информационной безопасности Республики Беларусь указывает на то, что повсеместное функционирование объектов транспорта с автоматизированными системами управления ставит в прямую зависимость от их надежности и защищенности жизнь и здоровье населения, экологическую и социальную безопасность [1].

Вместе с тем процессы информатизации и компьютеризации, а также использование современных сетевых технологий при организации управления на Белорусской железной дороге таят в себе множество потенциальных опасностей, область реализации которых касается исключительно сферы высоких технологий. При отсутствии адекватной системы защиты опасности такого рода могут привести к нарушению штатной работы систем управления и, как следствие, ухудшению уровня безопасности движения поездов.

В таких условиях обязательным является проведение анализа этих опасностей, характерных как для самих инфокоммуникационных систем, так и для среды их функционирования.

Безопасность инфокоммуникационных систем железнодорожного транспорта – это их защищенность от случайного или преднамеренного вмешательства в штатный процесс их функционирования. В общем случае речь идет о функциональной безопасности инфокоммуникационной системы, когда важным является выполнение системой поставленных перед ней задач. Если же в инфокоммуникационной системе содержится информация, предоставление и (или) распространение которой ограничено, то в таком случае речь идет также и об информационной безопасности.

В соответствии с [1] кибербезопасность – это состояние защищенности инфокоммуникационной системы и содержащейся в ней информации от внешних и внутренних угроз.

Понятие кибербезопасности включает в себя защищенность информации, которая обрабатывается инфокоммуникационной системой (информационная безопасность), так и защищенность процесса функционирования самой инфокоммуникационной системы (функциональная безопасность). Причем для железнодорожного транспорта вторая составляющая кибербезопасности является более актуальной. Это связано с тем, что часть АСУ ТП железнодорожного транспорта вообще может не использовать информацию, предоставление и (или) распространение которой ограничено, и при этом выполнять задачи, связанные с безопасностью движения поездов. Для таких систем мероприятия по обеспечению информационной безопасности фактически сводятся к функциям разграничения доступа и аудита выполняемых пользователем АСУ ТП операций.

В реальной среде функционирования любой инфокоммуникационной системы независимо от нее существует множество угроз ее кибербезопасности. Угроза кибербезопасности – возможное воздействие на инфокоммуникационную систему, которое прямо или косвенно может нанести ущерб ее кибербезопасности.

Совокупность всех угроз $T = \{T_1, T_2, \dots T_m\}$ (от англ. *threat*), которые в той или иной степени могут нанести ущерб безопасности инфокоммуникационной системе, формируют реальную среду ее функционирования. Именно на такое функционирование следует рассчитывать при эксплуатации инфокоммуникационной системы. Любая угроза не может существовать сама по себе – у нее должен быть источник.

Источники угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы кибербезопасности. Таким образом, источником угрозы могут являться [2]:

– субъекты, потенциальные неумышленные или преднамеренные действия которых могут нанести ущерб кибербезопасности инфокоммуникационной системы;

– технические средства – аппаратные, программные или аппаратно-программные средства и комплексы, от-

казы которых или наличие в их реализации логических ошибок может привести к нарушению кибербезопасности инфокоммуникационной системы;

– стихийные явления – стихийные бедствия, частично или полностью препятствующие функционированию инфокоммуникационной системы.

Сами по себе угрозы не опасны для инфокоммуникационной системы. Сосуществуя совместно с ней, угрозы могут вовсе не причинять ущерба ее кибербезопасности. Опасность для инфокоммуникационной системы представляют только те угрозы, для которых инфокоммуникационная система является уязвимой, или, иными словами, обладает определенными уязвимостями, через которые источники угроз могут реализовать свои угрозы в обход системы защиты информации и нанести ущерб владельцу инфокоммуникационной системы.

Уязвимость инфокоммуникационной системы – это присущая ей причина, приводящая к нарушению ее кибербезопасности.

Совокупность уязвимостей инфокоммуникационной системы $V = \{V_1, V_2, \ldots V_k,\}$ (от англ. *vulnerability*) ограничивает сферу ее эксплуатации и режимы функционирования. Максимально полное представление об уязвимостях инфокоммуникационной системы позволяет применить адекватные меры по их минимизации и тем самым устранить возможные последствия от воздействия угроз.

При наличии множества уязвимостей инфокоммуникационной системы и множества угроз ее кибербезопасности в реальных условиях функционирования велика вероятность реализации одной из таких угроз через какую-либо уязвимость.

В соответствии с [1] кибератака – это целенаправленное воздействие программных и (или) программно-аппаратных средств на инфокоммуникационную систему в целях нарушения и (или) прекращения ее функционирования и (или) создания угрозы безопасности обрабатываемой такой системой информации. Для того, чтобы произошла кибератака, необходимо, чтобы реализовалась конкретная угроза при взаимодействии источника данной угрозы с конкретной уязвимостью инфокоммуникационной системы в обход системы защиты информации (рисунок 1). Для каждой из угроз кибербезопасности инфокоммуникационной системы можно определить подмножество уязвимостей $VT \subseteq V$, через которые данная угроза может реализоваться.

Риск – это мера, определяющая возможность нанесения ущерба владельцу инфокоммуникационной системы посредством реализации угроз кибербезопасности через установленные уязвимости инфокоммуникационной системы [3].

Для количественной оценки риска используется следующая формула:

$$R = P_A U, \tag{1}$$

где R – риск от реализации угрозы; P_A – вероятность реализации угрозы; U – величина ущерба.

Вероятность реализации угрозы состоит из вероятности появления источника угрозы и его готовности атаковать, а также включает вероятности наличия у инфокоммуникационной системы подходящей уязвимости и ее доступность для угрозы:

$$P_A = P_{уг} P_{уяз}, \tag{2}$$

где $P_{уг}$ – вероятность появления источника угрозы и его готовности атаковать; $P_{уяз}$ – вероятность наличия у инфокоммуникационной системы подходящей уязвимости и ее доступность для угрозы.

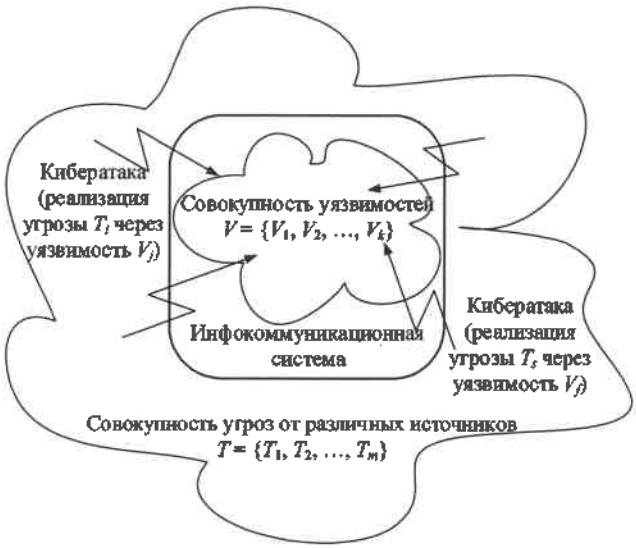

Рисунок 1 – Совокупности угроз и уязвимостей кибербезопасности инфокоммуникационной системы

Уровень киберзащищенности инфокоммуникационной системы – это мера, которая определяет возможность предотвращения ущерба, наносимого владельцу инфокоммуникационной системы, вследствие использования конкретного комплекса средств защиты информации при реализации угроз кибербезопасности через установленные уязвимости инфокоммуникационной системы.

Уровень киберзащищенности определяется по следующей формуле:

$$Z = \frac{1}{P_A U P_{ПСЗ}}, \tag{3}$$

где Z – киберзащищенность инфокоммуникационной системы от воздействия конкретной угрозы; $P_{ПСЗ}$ – вероятность преодоления средства защиты информации инфокоммуникационной системы в процессе реализации угрозы.

При анализе киберзащищенности инфокоммуникационной системы от нескольких угроз оценка уровня киберзащищенности будет рассчитываться по следующей формуле:

$$Z = \frac{N}{\sum_{i=1}^{N} \left(P_{Ai} U_i P_{ПСЗi} \right)}, \tag{4}$$

где N – количество угроз.

Существует **четыре метода оценки эффективности кибербезопасности**, основанных на анализе рисков [3]:

– *базовый метод* основан на использовании стандартов информационной безопасности;

– *метод детального анализа рисков* предполагает систематический анализ исходных данных для конкретной инфокоммуникационной системы с целью оценки рисков нарушения ее кибербезопасности и выбора средств защиты, соответствующих заданным требованиям;

– *экспертный метод* основан на проведении неформального анализа рисков, результат которого основан на знаниях и опыте экспертов;

– *комбинированный метод* предполагает использование в различных сочетаниях трех предыдущих методов.

Первые три метода имеют свои преимущества и недостатки. Первый метод прост и надежен, однако опирается на базовый набор требований, предполагает использование штатных методов защиты информации и, в основном, рассматривает угрозы информационной безопасности. Второй метод достаточно сложен в реализации, требует максимальных затрат времени и усилий. Третий метод достаточно субъективен и не систематичен.

В связи с этим для инфокоммуникационных систем железнодорожного транспорта будет оптимальным использовать комбинированный метод оценки эффективности кибербезопасности. При этом, опираясь на действующие стандарты информационной безопасности (базовый метод), детально прорабатываются риски кибербезопасности инфокоммуникационной системы с учетом множества угроз ее кибербезопасности (метод детального анализа рисков), а для оценки вероятностей реализации угроз через конкретные уязвимости в обход системы защиты, а также величины возможного ущерба, который будет при этом нанесен, используется экспертная оценка (экспертный метод).

Оценку рисков кибербезопасности инфокоммуникационной системы железнодорожного транспорта следует начать с определения множества угроз кибербезопасности. Для каждой из угроз экспертам предлагается дать оценку по двум критериям:

– критерий C_1 (от англ. *Criterion*) – возможность возникновения источника угрозы в достаточном окружении от инфокоммуникационной системы для реализации угрозы (если возможность возникновения источника угрозы высока, то эксперт ставит высокую оценку, если мала – низкую);

– критерий C_2 – степень готовности источника угрозы реализовать угрозу.

Критерии оцениваются экспертами по десятибалльной шкале (дискретно от 1 до 10).

Следующим шагом является определение множества уязвимостей инфокоммуникационной системы. Для каждой уязвимости экспертам предлагается дать оценку также по двум критериям:

– критерий C_3 – распространенность уязвимости по инфокоммуникационной системе или частота ее появления;

– критерий C_4 – доступность уязвимости для реализации через нее угроз.

Затем для каждой из угроз определяется подмножество уязвимостей, через которые угроза может быть реализована (таблица 1). Угрозы, для которых подмножество уязвимостей является пустым, удаляются из списка угроз. Для каждой уязвимости из подмножества экспертами определяется критерий C_5 – фатальность от реализации угрозы источником угрозы через уязвимость инфокоммуникационной системы.

Таблица 1 – **Выбор подмножеств уязвимостей инфокоммуникационной системы для конкретных угроз**

Угрозы кибербезопасности	Уязвимость инфокоммуникационной системы					
	№ 1	№ 2	№ 3	№ 4	№ 5	и т. д.
№ 1	×	×	×			
№ 2		×		×	×	
№ 3						
№ 4	×		×			
и т. д.						

Оценка риска от реализации каждой из угроз при использовании оценок экспертов производится по следующей формуле:

$$R_i = \frac{\sum_{j=1}^{M} C_{1j} \sum_{j=1}^{M} C_{2j} \sum_{j=1}^{M} C_{3j} \sum_{j=1}^{M} C_{4j} \sum_{j=1}^{M} C_{5j}}{M^5}, \qquad (5)$$

где M – количество экспертов; C_{ij} – значение i-го критерия, выставленного j-м экспертом.

В формуле (5) в отличие от формул (1) и (2) применяются не значения вероятностей и величины ущерба, а оценки экспертов, что не позволит получить уровень ущерба в единицах, в которых измеряется ущерб. Однако это позволит сопоставлять уровень нанесенного ущерба владельцу инфокоммуникационной системы посредством реализации разного набора угроз кибербезопасности. В формуле (5) критерии C_1 и C_2 соответствуют $P_{уг}$ из формулы (2), C_3 и C_4 – $P_{уяз}$ из этой же формулы, а C_5 – U из формулы (1).

При наличии M экспертов для упрощения формулы (5) критерии C_1 и C_2 удобно представить параметром $C_{уг}$:

$$C_{уг} = \sum_{j=1}^{M} C_{1j} \cdot \sum_{j=1}^{M} C_{2j}. \qquad (6)$$

Критерии C_3, C_4 и C_5 выбираются только для одной из уязвимостей подмножества. Эта уязвимость имеет максимальное значение произведения данных критериев, выставленных всеми экспертами и для удобства представляется параметром $C_{уяз}$:

$$C_{уяз} = \sum_{j=1}^{M} C_{3j} \cdot \sum_{j=1}^{M} C_{4j} \cdot \sum_{j=1}^{M} C_{5j} \to \max. \qquad (7)$$

При таком расчете максимальное значение риска реализации угрозы при выставлении экспертами только максимальных баллов по всем критериям будет равно 10^5. Минимальное значение риска (все эксперты выставили только минимальные баллы) – 1.

При оценке фатальности (критерий C_5) от реализации угрозы для инфокоммуникационных систем железнодорожного транспорта, специфика которых была указана выше, важно не только принимать во внимание нарушение информационной безопасности, но также учитывать и функциональную безопасность. В таблице 2 представлены рекомендации для экспертов при выставлении баллов по данному критерию исходя из соображений первостепенной важности обеспечения функциональной безопасности для объектов железнодорожного транспорта.

Таблица 2 – **Значения баллов критерия фатальности от реализации угрозы**

Балл	Уровень нарушения кибербезопасности инфокоммуникационной системы					
	нарушение конфиденциальности информации	нарушение доступности информации	нарушение сохранности информации	нарушение целостности и подлинности информации	частичное нарушение функциональной безопасности	выход из строя инфокоммуникационной системы
1	+					
2		+				
			+			
3				+		

Окончание таблицы 2

Балл	Уровень нарушения кибербезопасности инфокоммуникационной системы					
	нарушение конфиденциальности информации	нарушение доступности информации	нарушение сохранности информации	нарушение целостности и подлинности информации	частичное нарушение функциональной безопасности	выход из строя инфокоммуникационной системы
4	+			+		
		+		+		
			+	+		
	+	+		+		
		+	+	+		
	+		+	+		
5	+	+	+	+		
6			+		+	
		+			+	
	+				+	
7	+	+			+	
		+	+		+	
	+		+		+	
8	+			+	+	
		+		+	+	
			+	+	+	
	+	+		+	+	
		+	+	+	+	
	+		+	+	+	
9	+	+	+	+	+	
10						+

Для оценки уровня киберзащищенности инфокоммуникационной системы необходимо ввести дополнительный критерий C_6 – степень преодоления средства защиты информации в процессе реализации угрозы. Для оценки эффективности киберзащищенности можно выбирать отдельные средства защиты информации или их комбинации. Для каждого средства защиты информации эксперты также по десятибалльной шкале (дискретно от 1 до 10) определяют критерий C_6. При комбинировании средств защиты информации используется только одно максимальное значение данного критерия из его значений для каждого из средств защиты информации по отдельности. При наличии M экспертов для упрощения данный критерий удобно представить параметром $C_{СЗИ}$:

$$C_{СЗИ} = \sum_{j=1}^{M} C_{6j}. \quad (8)$$

Используя формулы (3) и (5)–(8), значение уровня киберзащищенности инфокоммуникационной системы от одной из угроз определим по формуле

$$Z = \frac{M^6}{C_{уг} C_{уяз} C_{СЗИ}}. \quad (9)$$

Тогда при анализе киберзащищенности инфокоммуникационной системы от нескольких угроз оценка уровня киберзащищенности будет рассчитываться по следующей формуле:

$$Z = \frac{NM^6}{\sum_{i=1}^{N} \left(C_{угi} C_{уязi} C_{СЗИi} \right)}. \quad (10)$$

Такой подход позволяет количественно сравнить уровень киберзащищенности инфокоммуникационных систем железнодорожного транспорта при использовании различных систем защиты информации и их комбинаций. При оценке уровня киберзащищенности инфокоммуникационной системы без использования средств защиты информации параметр $C_{СЗИ}$ в формуле (9) и $C_{СЗИi}$ в формуле (10) следует принять равными 10.

Список литературы

1 О Концепции информационной безопасности Республики Беларусь : постановление Совета безопасности Республики Беларусь, 18 марта 2019 г. № 1 // ЭТАЛОН. Законодательство Республики Беларусь [Электронный ресурс] / Нац. центр правовой информации Респ. Беларусь. – Минск, 2019.

2 **Буй, П. М.** Методика перекрестной оценки угроз и уязвимостей безопасности объектов информатизации железнодорожного транспорта / П. М. Буй, С. Г. Кульгавик // Вестник БелГУТа: Наука и транспорт. – 2017. – № 2 (35). – С. 40–43.

3 **Анищенко, В. В.** Методы оценки эффективности защиты активов в объектах информационных технологий / В. В. Анищенко, А. М. Криштофик // Информатика. – 2004. – № 3. – С. 95–105.

Получено 30.09.2020

P. M. Bui. Assessment of the cybersecurity risks infocommunication's systems of railway transport.

The features of ensuring the cybersecurity of infocommunication systems of railway transport are given. The necessity of ensuring both information and functional security of infocommunication systems has been substantiated. The concepts of cybersecurity threat, vulnerability of infocommunication system, cyberattack, risk and cyber security are given. A method for assessing the risks of cybersecurity infocommunication's systems of railway transport is proposed. The necessary criteria and recommendations for the points given by the experts are presented. Presents a methodic for assessing the cyber security of infocommunication systems of railway transport.