УДК 656.2.08

ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

П.М. БУЙ

Белорусский государственный университет транспорта, Республика Беларусь

Поступила в редакцию 29 марта 2020

Аннотация. Предложена методика оценки рисков кибербезопасности инфокоммуникационных систем железнодорожного транспорта. Методика использует совокупность угроз и уязвимостей при первостепенном значении функциональной безопасности.

Ключевые слова: угроза, уязвимость, риски, кибербезопасность.

Введение

Для Республики Беларусь железнодорожный комплекс 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. Все это способствует тому, что Белорусская железная дорога обязана обеспечить потребности государства, юридических и физических лиц в железнодорожных перевозках, а также работах и услугах, оказываемых железнодорожным транспортом.

В рамках стремительной информатизации и компьютеризации общества Белорусская железная дорога не в состоянии качественно выполнять поставленные перед ней задачи, не прогрессируя вместе с обществом. Внедрение передовых и вместе с тем надежных инфокоммуникационных технологий является одной из ее первостепенных задач.

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).

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 грузо- и пассажироперевозок.

В Концепции информационной безопасности сказано, что повсеместное функционирование объектов транспорта с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности [1].

Безопасность таких инфокоммуникационных систем – 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.

Однако ни в глобальном, ни в региональных масштабах пока не удается эффективно воспрепятствовать разработкам и распространению средств, заведомо предназначенных для

уничтожения, блокирования, модификации, похищения информации в сетях и ресурсах или нейтрализации мер по ее защите [1].

В таких условиях обязательным является анализбезопасности инфокоммуникационных систем и среды их функционирования.

Угрозы кибербезопасности инфокоммуникационных систем и их уязвимости

Кибербезопасность – состояние защищенности инфокоммуникационной системы и содержащейся в ней информации от внешних и внутренних угроз. Состояние защищенности нарушается посредством кибератак. Кибератака – 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.

Таким образом, 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 могут не использовать информации предоставление и (или) распространение которой ограничено, и при этом выполнять задачи связанные с безопасностью грузо- и пассажироперевозок. 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 любойинфокоммуникационной системы независимо от нее существует множество угроз ее безопасности. Угроза безопасности инфокоммуникационной системе – возможное воздействие на нее, которое прямо или косвенно может нанести ущерб ее безопасности. Следует разделять угрозы функциональной и информационной безопасности исходя из функций, на которые они нацелены.

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

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

– субъекты, потенциальные неумышленные или преднамеренные действия которых могут нанести ущерб функциональной или информационной безопасности инфокоммуникационной системы;

– технические средства – аппаратные, программные или аппаратно-программные средства и комплексы, отказы которых или наличие в их реализации логических ошибок может привести к нарушению безопасности инфокоммуникационной системы;

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

Оптимальным методом оценки угроз является метод экспертных оценок, при котором экспертам предлагается оценить возможность реализации некоторого перечня угроз. В качестве критериев оценки опасности конкретной угрозы, согласно [3], следует выбрать возможность возникновения источника угрозы (K_1), степень его готовности произвести атаку (K_2), а также фатальность для инфокоммуникационной системы от реализации угрозы (K_3). Коэффициент опасности угрозы вычисляется на основании баллов (дискретно от 1 до 10), выставленных экспертом по трем критериям, по следующей формуле:

$$K_{\text{опуг}} = \frac{K_1 K_2 K_3}{10^3}. \qquad (1)$$

Для N экспертов общий коэффициент опасности угрозы вычисляется как произведение средних баллов, выставленных экспертами по каждому критерию:

$$K_{\text{опуг}N} = \frac{\sum_{i=1}^{N} K_{1i} \cdot \sum_{i=1}^{N} K_{2i} \cdot \sum_{i=1}^{N} K_{3i}}{(10N)^3}, \quad (2)$$

где K_{1i}, K_{2i}, K_{3i} – баллы, выставленные i-м экспертом трем указанным выше критериям соответственно.

При таком расчете максимальное значение коэффициента опасности угрозы при выставлении экспертами максимальных баллов по всем критериям будет равно единице. Анализируя коэффициенты опасности совокупности угроз, можно произвести их ранжирование и определить для конкретнойинфокоммуникационной системы перечень наиболее опасных из них.

Сами по себе угрозы не представляют опасности инфокоммуникационных систем. Сосуществуя совместно с ним, угрозы могут вовсе не причинять ущерба их безопасности. Опасность для инфокоммуникационной системы представляют только те угрозы, для которых она является уязвимой, или, иными словами, обладает определенными уязвимостями, через которые источники угроз могут реализовать свои угрозы и нанести ущерб данному объекту.

Уязвимость инфокоммуникационной системы – это присущие инфокоммуникационной системе причины, приводящие к нарушению безопасности ее функционирования или безопасности информации, которая в ней обрабатывается.

Совокупность уязвимостей инфокоммуникационной системы $V = \{V_1, V_2, ..., V_k\}$ (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 возможных последствий от воздействия угроз.

В качестве критериев оценки опасности уязвимости источник [3] предлагает: фатальность наличия у инфокоммуникационной системы уязвимости (K_4), доступность уязвимости для источников угроз (K_5), а также количество уязвимостей выбранного рода в инфокоммуникационной системе или частота их появления (K_6). Аналогично с процессом оценки опасности угроз эксперты выставляют баллы от 1 до 10 по каждому из критериев. Для одного эксперта коэффициент опасности уязвимости вычисляется по формуле:

$$K_{\text{опуяз}} = \frac{K_4 K_5 K_6}{10^3}. \quad (3)$$

Анализируя коэффициенты опасности совокупности уязвимостей, можно произвести их ранжирование и определить те из них, устранением которых необходимо заняться в первую очередь.

Критерии оценки угроз кибербезопасности

Для оценки рисков кибербезопасности инфокоммуникационной системы необходимо в первую очередь выделить ее активы. Совокупность активов инфокоммуникационной системы – это все то, что необходимо для ее штатного функционирования и находится в ее распоряжении (аппаратные средства, программное обеспечение, хранимая и (или) обрабатываемая информация.

Процесс оценки рисков для каждого из активов должен учитывать стоимость самого актива и вероятностную характеристику возможности нарушения его кибербезопасности. При этом важно учитывать, как всю совокупность угроз, так и всю совокупность уязвимостей (рис. 1). Процесс изменения совокупности угроз в процессе функционирования инфокоммуникационной системы является гораздо более динамичным по сравнению с процессом изменения совокупности ее уязвимостей. В связи с этим для оценки рисков целесообразно первостепенное внимание уделять именно угрозам кибербезопасности инфокоммуникационных систем.

В связи с тем, что неуклонно растет количество киберпреступлений, инфокоммуникационные системы становятся как предметом таких преступлений, так и средством их совершения, в перспективе намечается формирование тотальной зависимости транспортной отрасли от защищенности инфокоммуникационных систем, построить абсолютно адекватную систему защиты не представляется возможным. Особенно, если затраты на ее организацию и сопровождение не должны превышать предполагаемый ущерб от ее нарушения в результате реализации угроз. Таким образом, необходимо выбрать методику, которая позволит определить опасность угроз для инфокоммуникационной системы, сравнить угрозы между собой и провести ранжирование. А выбрав наиболее опасные угрозы для исследуемой инфокоммуникационной системы можно по ним оценивать риски и конфигурировать систему защиты, вписываясь по ее стоимости в уровень предполагаемого ущерба.

В реальных условиях функционирования одна и та же угрозакибербезопасности инфокоммуникационной системы может реализоваться через нескольких уязвимостей. На рисунке 2, для примера, такими уязвимостями из множества уязвимостей V для угрозы T_4 являются уязвимости V_2, V_3 и V_4. Важно для каждой угрозы составить совокупность уязвимостей конкретного актива или инфокоммуникационной системы в целом, через которые данная угроза может реализоваться $V_S = \{V_{S1}, V_{S2}, ..., V_{Sk}\}; V_S \subseteq V$.

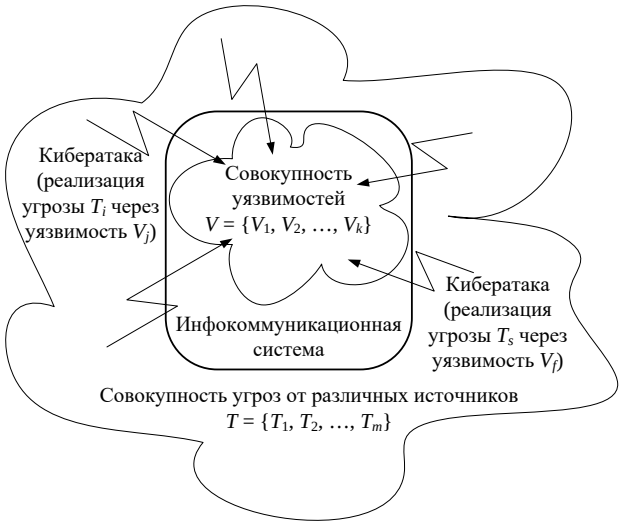

Рис. 1. Совокупности угроз и уязвимостей кибербезопасности инфокоммуникационной системы

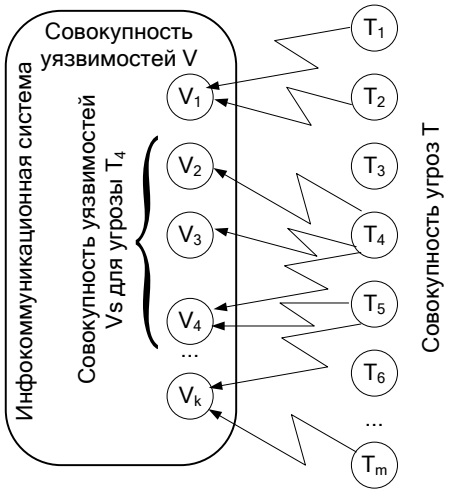

Рис. 2. Реализация угроз кибербезопасности через разные уязвимости

Существующие методы ранжирования угроз и уязвимостей производят их оценку независимо друг от друга [3]. Однако, как было указано выше, угрозы не представляют опасности для объекта без наличия соответствующих им уязвимостей. Также и уязвимости не подрывают уровень кибербезопасности инфокоммуникационной системы, если нет угроз, которые могут ими воспользоваться. Следовательно, оценку угроз и уязвимостей следует производить совокупно. При этом следует использовать следующие критерии:

– критерий C_1 (от англ. *criterion*) – возможность возникновения источника угрозы в достаточном окружении от инфокоммуникационной системы для реализации угрозы;

– критерий C_2 – степень готовности источника угрозы реализовать угрозу;

– критерий C_3 – распространенность в инфокоммуникационной системе уязвимостей из совокупности уязвимостей (V_S), через которые может реализоваться угроза;

– критерий C_4 – доступность для реализации угрозы уязвимостей из совокупности уязвимостей (V_S), через которые может реализоваться данная угроза;

– критерий C_5 – фатальность для инфокоммуникационной системы от реализации угрозы.

Коллектив независимых экспертов по каждому из критериев выставляет баллы (дискретно от 1 до 10). Принцип выставления баллов для первых четырех критериев прост: чем в большей степени появляется критерий, тем большего балла он заслуживает. Для учета вопросов как информационной, так и функциональной безопасности для пятого критерия рекомендуются представленные втаблице 1 значения баллов и соответствующие им уровни нарушения кибербезопасности инфокоммуникационных систем исходя из соображений первостепенной важности обеспечения функциональной безопасности.

Таблица 1. **Значения баллов критерия фатальности реализации угрозы**

Балл, выставляемый экспертом	Уровни нарушения кибербезопасности инфокоммуникационных систем				
	нарушение доступности информации	нарушение конфиден-циальности информации	нарушение целостности информации	частичное нарушение функциональной безопасности	выход из строя инфоком-муникационной системы
1	+				
2		+			
			+		
3		+	+		
	+	+			
	+		+		
4	+	+	+		
5				+	
6	+			+	
7		+		+	
			+	+	
8		+	+	+	
	+	+		+	
	+		+	+	
9	+	+	+	+	
10					+

Тогда для N экспертов общий коэффициент опасности угрозы с учетом указанного выше перечня критериев вычисляется по следующей формуле:

$$K_{\text{опуг}N} = \frac{\sum_{i=1}^{N} C_{1i} \cdot \sum_{i=1}^{N} C_{2i} \cdot \sum_{i=1}^{N} C_{3i} \cdot \sum_{i=1}^{N} C_{4i} \cdot \sum_{i=1}^{N} C_{5i}}{(10N)^5}, \quad (4)$$

где C_{1i}, C_{2i} и т. д. – баллы, выставленные i-м экспертом по пяти указанным выше критериям соответственно.

Заключение

Оценка рисков кибербезопасности инфокоммуникационных систем производится следующим образом:

1. Определяется перечень активов инфокоммуникационной системы.
2. Для каждого из активов определяется совокупность угроз его кибербезопасности.
3. Для каждой из угроз определяется совокупность уязвимостей, через которые она может реализоваться.
4. Группой экспертов производится оценка коэффициента опасности каждой из угроз (формула 4).
5. Производится ранжирование угроз по уменьшению коэффициента их опасности. Таким образом, для каждого актива формируется индивидуальный ранжированный по степени опасности список угроз.
6. Для каждого из активов определяются риски кибербезопасности по его стоимости и максимальному для актива значению коэффициента опасности угрозы.

ASSESSING RISKS OF INFOCOMMUNICATION SYSTEMS' CYBERSECURITY

P.M. BUI

Abstract. A methodology for assessing the risks of railway transport's infocommunication systems' cybersecurity is proposed. The methodology uses an aggregate of threats and vulnerabilities with the paramount importance of functional security.

Keywords: threat, vulnerability, risks, cybersecurity.

Списоклитературы

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : Постановление Совета безопасности Республики Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ.Беларусь. – Минск, 2019.
2. Вихорев С.В., Кобцев Р.Ю. // Защита информации. Конфидент. 2002. № 2. С. 44–49.
3. Вихорев С.В., Кобцев Р.Ю. // Защита информации. Конфидент. 2002. № 3. С. 80–84.