МЕТОДИКА ПЕРЕКРЕСТНОЙ ОЦЕНКИ УЯЗВИМОСТЕЙ И УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Буй П. М., Кульгавик С. Г.
Кафедра «Автоматика, телемеханика и связь», Белорусский государственный университет транспорта
Гомель, Республика Беларусь
E-mail: pashabuoy@rambler.ru, kalashnikovn27.sk@gmail.com

В статье обоснована необходимость обеспечения как информационной, так и функциональной безопасности информационных систем железнодорожного транспорта, предложена методика перекрестной оценки угроз и уязвимостей, приведены необходимые критерии и система выставления баллов экспертами.

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 технологий по ее информатизации является одной из первостепенных задач. 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 таких условиях обязательным является проведение анализа этих опасностей характерных как для самих информационных систем, так и для среды их функционирования. В сфере железнодорожного транспорта довольно часто информационные системы используются не только для обработки информации, но и для организации автоматизированных систем управления технологическими процессами (АСУ ТП), в некоторых из которых может вообще отсутствовать информация, предоставление и/или распространение которой ограничено. Безопасность таких информационных систем – это их защищенность от случайного или преднамеренного вмешательства в штатный процесс их функционирования. В общем случае речь идет о функциональной безопасности информационной системы, когда важным является выполнение системой поставленных перед ней задач. Если же эти задачи связаны с хранением и обработкой информации, предоставление и/или распространение которой ограничено, то в таком случае речь идет об информационной безопасности. Для систем управления на железнодорожном транспорте именно нарушение функциональной безопасности становится более опасным.

I. Критерии оценки

Для адекватной оценки уровня безопасности информационной системы важно проводить анализ ее уязвимостей и потенциальных угроз ее безопасности. При этом следует охватить существенное их количество. Такой подход дополнительно усложняется, если принять во внимание, что несколько угроз могут быть реализованы через одну и ту же уязвимость и аналогично несколько уязвимостей могут стать причиной реализации одной и той же угрозы. В таких обстоятельствах целесообразно использовать методику перекрестной оценки угроз безопасности информационных систем и их уязвимостей [1]. Это позволит учесть очевидную взаимосвязь угроз и уязвимостей, являющуюся обязательным условием реализации любой угрозы, а также вопросы не только информационной, но и функциональной безопасности, которые зачастую остаются в «тени» при использовании существующих методов, ориентированных на оценку исключительно информационной безопасности. Методика перекрестной оценки угроз безопасности информационных систем и их уязвимостей опирается на методику экспертных оценок. В связи с этим квалифицированные эксперты должны определить и выставить баллы следующим специальным критериям для каждой пары «угроза-уязвимость» дискретно в диапазоне от 1 до 10 [2]:

– критерий C_1 (от англ. Criterion) – возможность возникновения источника угрозы в достаточном окружении от информацион-

ной системы для реализации угрозы через уязвимость;
- критерий C_2 – степень готовности источника угрозы воспользоваться уязвимостью информационной системы и реализовать угрозу;
- критерий C_3 – распространенность уязвимости по информационной системе или частота ее появления;
- критерий C_4 – доступность уязвимости для реализации угрозы ее источником;
- критерий C_5 – фатальность от реализации угрозы источником угрозы через уязвимость информационной системы.

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 на рисунке 1 значения баллов и соответствующие им уровни нарушения безопасности информационных систем исходя из соображений первостепенной важности обеспечения функциональной безопасности.

II. Методика перекрестной оценки

При проведении перекрестной оценки уязвимостей и угроз безопасности информационной системы необходимо:

1. Определить совокупности угроз и уязвимостей безопасности информационной системы;
2. Увязать между собой угрозы и уязвимости, установив потенциальную реализацию первых через вторые;
3. Перевести в резерв несвязанные уязвимости и угрозы;
4. Вычислить коэффициенты опасности реализации каждой угрозы через каждую связанную с ней уязвимость (формула расчета коэффициента опасности приведена в источнике [1]);
5. Для каждой угрозы определить коэффициент опасности с учетом возможной ее реализации через некоторые уязвимости из перечня уязвимостей, определенного в пункте 1 (формула расчета коэффициента опасности угрозы приведена в источнике [2]);
6. Для каждой уязвимости определить коэффициент опасности с учетом возможной реализации через нее некоторых угроз из перечня угроз, определенного в пункте 1 (формула расчета коэффициента опасности уязвимости также приведена в источнике [2]);
7. Произвести ранжирование угроз и уязвимостей, определив тем самым наиболее опасные из них.

1. Буй, П. М. Методика перекрестной оценки угроз безопасности информационных систем и их уязвимостей / П. М. Буй, С. Г. Кульгавик // Комплексная защита информации: материалы XXIII Международной научно-практической конференции, Суздаль, 22-24 мая 2018г. – Суздаль: НИИ ТЗИ, 2018.
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.

Балл, выставляемый экспертом	Уровни нарушения безопасности информационных систем				
	нарушение доступности информации	нарушение конфиденциальности информации	нарушение целостности информации	частичное нарушение функциональной безопасности	выход из строя информационной системы
1	+				
2		+			
			+		
3		+	+		
	+	+			
	+		+		
4	+	+	+		
5				+	
6	+			+	
7		+		+	
			+	+	
8		+	+	+	
	+	+		+	
	+		+	+	
9	+	+	+	+	
10					+

Рис. 1 – Значения баллов критерия фатальности реализации угрозы через уязвимость