телеуправления ТУ16-1 диспетчерской централизации «Нёман», блоки телеуправления ТУ-8Б и телесигнализации и телесигнализации ТС-16Б, применяемых в микропроцессорных централизациях «Ипуть» и «Днепр». В 2017 году *Formal Time Verifier* зарегистрировано в реестре компьютерных программ Национального центра интеллектуальной собственности, г. Минск.

УДК 621.38

ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МЕТОДИКИ ПЕРЕКРЕСТНОЙ ОЦЕНКИ ИХ УЯЗВИМОСТЕЙ И ПОТЕНЦИАЛЬНЫХ УГРОЗ

П. М. БУЙ
Белорусский государственный университет транспорта, г. Гомель

С. Г. КУЛЬГАВИК
Белорусская железная дорога, г. Барановичи

Риск для безопасности информационной системы – возможность нарушения ее функциональной и/или информационной безопасности в результате реализации угрозы с негативными последствиями, имеющими определенную цену в денежном эквиваленте (размер ожидаемого ущерба).

Оценка рисков занимает центральное место в системе управления информационной безопасностью, позволяет идентифицировать и оценить существующие активы, определить необходимость внедрения и эффективность уже внедренных средств защиты информации.

Активы информационной системы – это всё то, что необходимо для ее штатного функционирования и находится в ее распоряжении, например, аппаратные средства, программное обеспечение, хранимая и/или обрабатываемая информация и т. п. Ущерб, нанесенный организации, в собственности которой находится информационная система, в результате нарушения безопасности актива определяется аналитически в зависимости от его свойств [1].

При количественной оценке рисков безопасности информационной системы помимо ущерба необходимо учитывать вероятности появления угроз и их реализации через конкретные уязвимости отдельных активов или информационной системы в целом. При этом для адекватной оценки рисков важно охватить существенное количество угроз и соответствующих им уязвимостей. Такой подход дополнительно усложняется, если принять во внимание, что несколько угроз могут реализовываться через одну и ту же уязвимость и аналогично несколько уязвимостей могут быть причиной реализации одной и той же угрозы. В таких обстоятельствах целесообразно будет воспользоваться методикой перекрестной оценки угроз безопасности информационных систем и их уязвимостей [2]. 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.

Проведение методики перекрестной оценки угроз и уязвимостей предполагает определение совокупностей угроз и уязвимостей безопасности информационной системы. После этого необходимо определить, через какие уязвимости могут быть реализованы угрозы, т. е. связать уязвимости с угрозами, причинами реализации которых они могут стать.

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: C_1 – возможность возникновения источника угрозы в достаточном окружении от информационной системы для реализации угрозы через уязвимость; C_2 – степень готовности источника угрозы воспользоваться уязвимостью информационной системы и реализовать угрозу; C_3 – распространенность уязвимости по информационной системе или частота ее появления; C_4 – доступность уязвимости для реализации угрозы ее источником; 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 в таблице 1 значения баллов и соответствующие им уровни нарушения безопасности информационных систем исходя из соображений первостепенной важности обеспечения функциональной безопасности.

Таблица 1 – **Значения баллов критерия фатальности реализации угрозы через уязвимость**

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					+

Затем для каждой из уязвимостей необходимо определить коэффициент ее опасности по следующей формуле [3]:

$$K_{\text{опуяз}NZ} = \frac{\sum_{j=1}^{Z}\sum_{i=1}^{N} C_{1ij} \sum_{j=1}^{Z}\sum_{i=1}^{N} C_{2ij}}{(10N)^2} \cdot \frac{\sum_{j=1}^{Z}\sum_{i=1}^{N} C_{3ij} \sum_{j=1}^{Z}\sum_{i=1}^{N} C_{4ij}}{(10NZ)^2} \cdot \frac{\max\limits_{j=1..Z}\left(\sum_{i=1}^{N} C_{5ij}\right)}{10N},$$

где Z – количество угроз, которые могут реализоваться через выбранную уязвимость; N – количество привлеченных к оценке экспертов; C_{1ij}, C_{2ij}, C_{3ij}, C_{4ij}, C_{5ij} – баллы, выставленные i-м экспертом пяти указанным выше критериям соответственно в процессе оценки одной уязвимости объекта информатизации при реализации через нее j-й угрозы.

На следующем этапе нужно произвести ранжирование уязвимостей по уменьшению коэффициента их опасности, определив тем самым наиболее опасные из них. Затем для каждого из активов из общего списка уязвимостей необходимо выбрать присущие ему уязвимости, сохраняя порядок их ранжирования. Таким образом для каждого актива формируется индивидуальный ранжированный по степени опасности перечень уязвимостей.

Для определения риска безопасности по каждому из активов необходимо умножить величину ущерба, нанесенного организации, в случае нарушения безопасности актива и, следовательно, информационной системы на коэффициент опасности самой высокой по рангу уязвимости для данного актива.

Определение суммарного риска безопасности информационной системы в целом производится путем суммирования рисков безопасности каждого из активов.

Список литературы

1 **Белоусова, Е. С.** Политика безопасности информационных систем : учеб.-метод. пособие / Е. С. Белоусова, П. М. Буй. – Гомель : БелГУТ, 2016. – 38 с.

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 **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 2018 г. – Суздаль : НИИ ТЗИ, 2018.

УДК 656.212.5

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ДЛЯ ПОВЫШЕНИЯ РИТМИЧНОСТИ РАБОТЫ ТЕРМИНАЛЬНЫХ КОМПЛЕКСОВ

Н. А. ГОНЧАРОВА
Петербургский государственный университет путей сообщения Императора Александра I, Российская Федерация

Проблема обеспечения ритмичности процессов грузовой и коммерческой работы на терминальных комплексах на данном этапе развития логистических систем приобретает всё большую актуальность. Это связано с тем, что возможности экстенсивного развития транспортной и складской инфраструктуры в Москве и Санкт-Петербурге практически исчерпаны. Сглаживанию неравномерности процессов транспортировки и обработки грузов в значительной мере способствовало создание сети тыловых логистических терминалов, но в последнее время в связи со спадом в экономике всё сложнее становится найти финансовые ресурсы для этого. Это делает актуальным исследование логистических технологий, позволяющих организовать эффективную работу терминала при минимальной площади зоны обмена с магистральными видами транспорта. Развитие таких технологий возможно на основе внедрения автоматизированных систем управления на терминальных комплексах.

На начальном этапе внедрения автоматизированных систем в процессы терминальной обработки грузов основной целью было ускорение процессов документооборота. Снижение доли бумажных документов позволило в разы повысить скорость обработки грузопотоков и снизить влияние человеческого фактора. Дальнейшее развитие данного направления предполагает широкое использование QR-кодирования, технологий pick-by-voice и pick-by-light.

Следующим значимым направлением развития автоматизированных систем в терминальной деятельности является развитие систем мониторинга груза в режиме реального времени. К сожалению, до сих пор на ряде российских терминалов возникают ситуации, когда на поиск определенной единицы груза, находящейся на территории терминального комплекса, тратится по несколько часов. В европейских странах широко применяется RFID-технология, постепенно начинается ее внедрение на передовых российских терминальных комплексах [1].

Третьим направлением развития автоматизированных систем в транспортной и складской логистике является интеграция всех участников перевозочного процесса. Данное направление включает в себя реализацию следующих возможностей:

– разработка согласованных контактных графиков работы взаимодействующих видов транспорта, грузоотправителей и грузополучателей, а также логистических посредников;

– составление взаимоувязанных с интересами грузоотправителей и грузополучателей графиков прибытия и отправления разных видов транспорта;

– организация комплексных технологических процессов работы в крупных узлах.

В России на данном этапе это направление развивается с большим трудом, поскольку крупные участники рынка транспортно-логистических услуг нацелены на дальнейшее использование собственных информационных систем, крайне сложно организовать их согласованную работу. Современный транспортный комплекс не может представлять собой множество разрозненных транспортных систем, при взаимодействии друг с другом снижающих эффективность технологических процессов [2]. Наибольшие усилия предпринимаются сейчас в организации эффективного взаимодействия морского и железнодорожного транспорта [3]. В повышении качества взаимодействия железнодорожного и автомобильного транспорта также есть определенные успехи. Наиболее значимыми из них являются:

– применение централизованных систем завоза и вывоза грузов силами крупных специализированных автотранспортных предприятий;