УДК 656.2.08

П. М. БУЙ, кандидат технических наук, Белорусский государственный университет транспорта, г. Гомель,
С. Г. КУЛЬГАВИК, инженер, Барановичская дистанция сигнализации и связи

МЕТОДИКА ПЕРЕКРЕСТНОЙ ОЦЕНКИ УГРОЗ И УЯЗВИМОСТЕЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Обоснована необходимость обеспечения как информационной, так и функциональной безопасности объектов информатизации железнодорожного транспорта. Даны понятия угрозы и уязвимости безопасности объекта информатизации, а также индивидуальные подходы к оценке их опасности. Предложен совокупный подход для оценки опасности угроз и уязвимостей. Приведены необходимые критерии и система выставления экспертами баллов. Представлена методика перекрестной оценки угроз и уязвимостей объектов информатизации железнодорожного транспорта.

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 объектов информатизации, так и для среды их функционирования.

Объект информатизации, согласно [1] – это средства электронной вычислительной техники (автоматизированные системы различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, а также копировально-множительные средства, в которых для обработки информации применяются цифровые методы) вместе с программным обеспечением, которые используются для обработки информации.

В системах железнодорожного транспорта довольно часто объекты информатизации используются не только для обработки информации, но и для организации автоматизированных систем управления технологическими процессами (АСУ ТП), в ряде из которых может отсутствовать информация, подлежащая защите.

Безопасность объекта информатизации – это защищенность такого объекта от случайного или преднамеренного вмешательства в штатный процесс его функционирования. В общем случае речь идет о функциональной безопасности объекта информатизации, когда важным является выполнение объектом поставленных перед ним задач. Если же эти задачи связаны с хранением и обработкой информации, предоставление и/или распространение которой ограничено, то в этом случае речь идет об информационной безопасности, для которой важным является защита информации от попыток хищения, изменения или разрушения компонентов объекта информатизации.

Функциональная безопасность – это совокупность таких условий функционирования объекта информатизации, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных воздействий, приводящих к нарушению процесса штатного его функционирования.

Именно нарушение функциональной безопасности становится более опасным для систем управления на железнодорожном транспорте. Информационная безопасность, безусловно, так же важна, но при отсутствии у объекта информатизации информации, предоставление которой должно быть ограничено, мероприятия по обеспечению информационной безопасности фактически сводятся к функциям разграничения доступа и контроля выполняемых пользователем операций на этом объекте.

В реальной среде функционирования любого объекта информатизации независимо от него существует множество угроз его безопасности. Угроза безопасности объекта – возможное воздействие на объект, которое прямо или косвенно может нанести ущерб его безопасности. Следует разделять угрозы функциональной и информационной безопасности исходя из функций объекта информатизации, на которые они нацелены.

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

Источники угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы без-

опасности. Таким образом, источником угрозы могут являться [2]:

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

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

– стихийные явления – стихийные бедствия, частично или полностью препятствующие функционированию объекта информатизации.

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], можно выбрать возможность возникновения источника угрозы (K_1), степень его готовности произвести атаку (K_2), а также фатальность для объекта от реализации угрозы (K_3). Коэффициент опасности угрозы вычисляется на основании баллов, выставленных экспертом по трем критериям от 1 до 10, по следующей формуле:

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

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

$$K_{\text{оп.уг}N} = \frac{\sum_{i=1}^{N} K_{1i} \cdot \sum_{i=1}^{N} K_{2i} \cdot \sum_{i=1}^{N} K_{3i}}{(10N)^3}, \qquad (2)$$

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 конкретного объекта информатизации перечень наиболее опасных.

Сами по себе угрозы не опасны для объекта информатизации. Сосуществуя совместно с ним, угрозы могут вовсе не причинять ущерба его безопасности. Опасность для объекта информатизации представляют только те угрозы, для которых объект информатизации является уязвимым, или, иными словами, обладает определенными уязвимостями, через которые источники угроз могут реализовать свои угрозы и нанести ущерб данному объекту.

Уязвимость объекта – это присущие объекту причины, приводящие к нарушению безопасности его функционирования или безопасности информации на объекте.

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

В качестве критериев оценки опасности уязвимости источник [3] предлагает: фатальность наличия у объекта информатизации уязвимости (K_4), доступность уязвимости для источников угроз (K_5), а также количество уязвимостей на объекте или частота их появления (K_6). Аналогично с процессом оценки опасности угроз один или N экспертов выставляют баллы от 1 до 10 по каждому из критериев. Для одного эксперта коэффициент опасности уязвимости вычисляется по схожей с (1) формулой:

$$K_{\text{оп.уяз}} = \frac{K_4 K_5 K_6}{10^3}. \qquad (3)$$

Для N независимых экспертов расчет общего коэффициента опасности уязвимости производится аналогично формуле (2):

$$K_{\text{оп.уяз}N} = \frac{\sum_{i=1}^{N} K_{4i} \cdot \sum_{i=1}^{N} K_{5i} \cdot \sum_{i=1}^{N} K_{6i}}{(10N)^3}. \qquad (4)$$

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

При наличии множества уязвимостей объекта информатизации и множества угроз его безопасности в реальных условиях функционирования велика вероятность реализации одной из угроз, нацеленной на процесс функционирования объекта или безопасность информации, которая в нем используется.

Атака – это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющуюся уязвимость. Таким образом, атака – это обязательное сочетание угрозы, реализуемой источником угрозы, и уязвимости, которое приводит к нарушению функциональной или информационной безопасности объекта информатизации (рисунок 1).

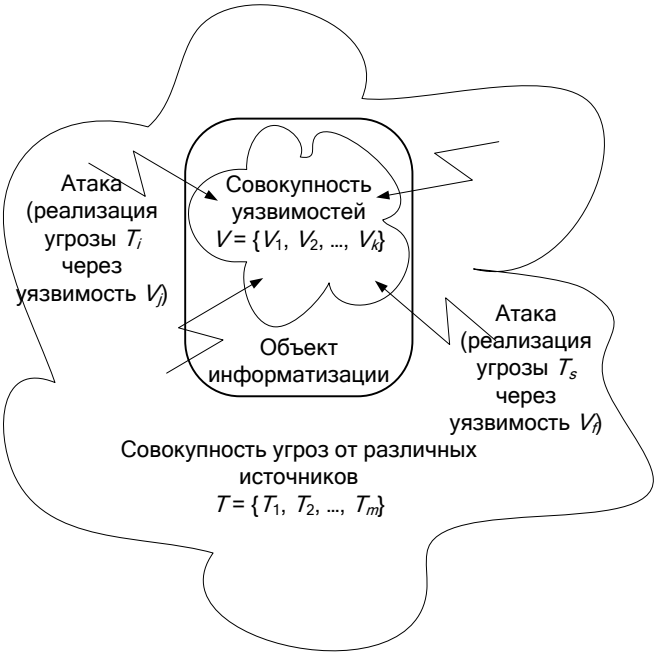

Рисунок 1 – Совокупности угроз и уязвимостей безопасности объекта информатизации

Для защиты объектов информатизации от атак разрабатываются специальные мероприятия по обеспечению их безопасности, часть из которых обеспечивает их надежное функционирование в условиях воздействия угроз, часть направлено на обеспечение информационной безопасности, т. е. сохранению таких свойств защищаемой информации, как конфиденциальность, доступность и целостность.

Учитывая многообразие угроз современного информационного мира, построить абсолютно адекватную систему защиты не представляется возможным, ведь 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 выбрать наиболее опасные для исследуемого объекта информатизации угрозы и защищаться только от них. Также важным является определение наиболее опасных для объекта информатизации уязвимостей, устранение которых позволит существенно повысить уровень безопасности объекта.

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 безопасности объекта, если нет угроз, которые могут ими воспользоваться. Следовательно, оценку угроз и уязвимостей следует производить совокупно, оценивая критерии опасности угрозы и уязвимости исходя из того, что первая будет реализована через вторую. При этом следует использовать подкорректированные критерии, соответствующие указанной совокупной оценке «угроза – уязвимость»:

– критерий C_1 (от англ. *Criterion*) – возможность возникновения источника угрозы в достаточном окружении от объекта информатизации для реализации угрозы через уязвимость;

– критерий C_2 – степень готовности источника угрозы воспользоваться уязвимостью объекта информатизации и реализовать угрозу;

– критерий C_3 – распространенность уязвимости по объекту информатизации 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 объекта информатизации.

Все критерии оцениваются экспертами по десятибалльной шкале (дискретно от 1 до 10). Принцип выставления баллов для первых четырех критериев прост: чем в большей степени появляется критерий, тем большего балла он заслуживает. Критерии C_1 и C_2 в паре «угроза – уязвимость» в большей степени имеют отношение к угрозе, а критерии C_3 и C_4 – к уязвимости. Критерий C_5 в одинаковой степени зависит как от угрозы, так и от уязвимости, и для него целесообразно использовать более конкретизированную систему оценивания.

При оценке фатальности от реализации угрозы для объектов информатизации железнодорожного транспорта, специфика которых была указана выше, важно не только принимать во внимание нарушение информационной безопасности, но также учитывать и функциональную безопасность. Ниже представлены баллы и соответствующие им уровни нарушения безопасности объектов информатизации исходя из соображений первостепенной важности обеспечения функциональной безопасности для объектов железнодорожного транспорта:

1 – нарушение доступности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

2 – нарушение конфиденциальности или целостности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

3 – нарушение конфиденциальности и целостности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

4 – нарушение конфиденциальности, целостности и доступности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

5 – частичное нарушение функциональной безопасности объекта информатизации;

6 – нарушение доступности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

7 – нарушение конфиденциальности или целостности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

8 – нарушение конфиденциальности и целостности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

9 – нарушение конфиденциальности, целостности и доступности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

10 – нарушение функциональной безопасности объекта информатизации – полный его выход из строя.

При таком подходе оценивается опасность реализации угрозы через уязвимость объекта информатизации. Общий коэффициент опасности реализации угрозы через уязвимость ($K_{\text{оп.уг.уз}N}$) оценивается N экспертами по следующей формуле:

$$K_{\text{оп.уг.уз}N} = \frac{\sum_{i=1}^{N} C_{1i} \cdot \sum_{i=1}^{N} C_{2i} \cdot \sum_{i=1}^{N} C_{3i} \cdot \sum_{i=1}^{N} C_{4i} \cdot \sum_{i=1}^{N} C_{5i}}{(10N)^5}. \qquad (5)$$

В реальных условиях функционирования одна и та же уязвимость безопасности объекта информатизации может стать причиной реализации сразу нескольких угроз. На рисунке 2 такими уязвимостями из множества уязвимостей V являются уязвимости V_1 и V_k. Вместе с тем одна и та же угроза может быть реализована через разные уязвимости. На рисунке 2 угроза T_4 может быть реализована через уязвимости V_2 и V_3, а T_5 – через V_4 и V_k.

Для перекрестной оценки опасности угроз и уязвимостей в таких условиях необходимо учитывать все сочетания пар «угроза – уязвимость», для которых были проведены индивидуальные оценки по формуле (5).

Оценка опасности угрозы, которая может быть реализована через S уязвимостей, каждая из которых по отдельности была оценена группой из N экспертов по методике, указанной выше, рассчитывается следующим образом:

$$K_{\text{оп.уг}NS} = \frac{\sum_{j=1}^{S}\sum_{i=1}^{N} C_{1ij} \cdot \sum_{j=1}^{S}\sum_{i=1}^{N} C_{2ij}}{(10NS)^2} \times \times \frac{\sum_{j=1}^{S}\sum_{i=1}^{N} C_{3ij} \cdot \sum_{j=1}^{S}\sum_{i=1}^{N} C_{4ij}}{(10N)^2} \cdot \frac{\max\limits_{j=1..S}\left(\sum_{i=1}^{N} C_{5ij}\right)}{10N}, \quad (6)$$

где C_{1ij}, C_{2ij}, C_{3ij}, C_{4ij}, C_{5ij} – баллы, выставленные i-м экспертом пяти указанным выше критериям соответственно в процессе оценки реализации одной угрозы через j-ю уязвимость объекта информатизации.

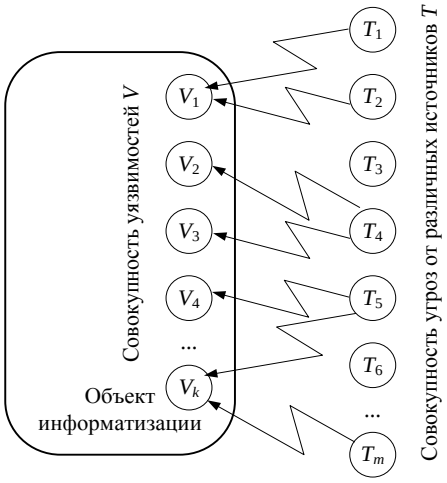

Рисунок 2 – Перекрестный характер угроз и уязвимостей безопасности объекта информатизации

Первый сомножитель в формуле (6), содержащий значения критериев C_1 и C_2, характеризует угрозу, которая является одинаковой во всех используемых парах «угроза – уязвимость». Для всех из S пар эксперты должны были указать одинаковые критерии. Чтобы избежать возможных ошибок экспертов, в формуле (6) принимаются средние для всех S пар значения критериев C_1 и C_2 (в знаменателе присутствует сомножитель S^2).

Второй сомножитель, содержащий значения критериев C_3 и C_4, характеризует уязвимость, которая является уникальной для каждой из используемых пар «угроза – уязвимость». Для того чтобы оценка опасности угрозы учитывала все возможные уязвимости, через которые она может реализоваться, необходимо сложить их значения критериев C_3 и C_4. Чем больше уязвимостей объекта информатизации может использовать угроза для своей реализации, тем больше должен быть коэффициент ее опасности.

Последний сомножитель характеризует фатальность от реализации угрозы. Для оценки опасности угрозы необходимо использовать максимальное значение критерия, определенное экспертами для всех уязвимостей, через которые угроза может быть реализована.

Схожим образом производится расчет коэффициента опасности уязвимости, через которую могут реализоваться Z угроз:

$$K_{\text{оп.уяз}NZ} = \frac{\sum_{j=1}^{Z}\sum_{i=1}^{N} C_{1ij} \cdot \sum_{j=1}^{Z}\sum_{i=1}^{N} C_{2ij}}{(10N)^2} \times \times \frac{\sum_{j=1}^{Z}\sum_{i=1}^{N} C_{3ij} \cdot \sum_{j=1}^{Z}\sum_{i=1}^{N} C_{4ij}}{(10NZ)^2} \cdot \frac{\max\limits_{j=1..Z}\left(\sum_{i=1}^{N} C_{5ij}\right)}{10N}, \quad (7)$$

где 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.

Здесь суммируются значения критериев C_1 и C_2, выставленные экспертами для каждой из угроз, которые могут реализоваться через исследуемую уязвимость, а значения критериев C_3 и C_4 усредняются, т. к. характеризуют одну и ту же уязвимость во всех парах «угроза – уязвимость». Значение критерия C_5 также выбирается максимальным.

Таким образом, при проведении перекрестной оценки угроз и уязвимостей необходимо:

– определить совокупности угроз и уязвимостей безопасности объекта информатизации;

– увязать между собой угрозы и уязвимости, установив потенциальную реализацию первых через вторые;

– перевести в резерв несвязанные уязвимости и угрозы;

– вычислить по формуле (5) коэффициент опасности реализации каждой угрозы через каждую увязанную с ней уязвимость;

– для каждой из угроз и уязвимостей определить соответственно по формулам (6) и (7) коэффициенты их опасностей;

– произвести ранжирование угроз и уязвимостей, определив тем самым наиболее опасные из них.

Список литературы

1 **СТБ 34.101.30-2007.** Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация. – Введ. 2008 –04–1. – Минск : БелГИСС. – 7 с.

2 **Вихорев, С. В.** Как узнать – откуда напасть или откуда исходит угроза безопасности информации / С. В. Вихорев, Р. Ю. Кобцев // Защита информации. Конфидент. – 2002. – № 2. – С. 44–49.

3 **Вихорев, С. В.** Как узнать – откуда напасть или откуда исходит угроза безопасности информации / С. В. Вихорев, Р. Ю. Кобцев // Защита информации. Конфидент. – 2002. – № 3. – С. 80–84.

Получено 30.09.2017

P. M. Bui, S. G. Kulgavik. Methodology of cross-cutting estimation of threats and vulnerabilities of safety of railway informatization objects.

The necessity of providing both informational and functional security of informatization objects of railway transport is grounded. The concepts of the threat and vulnerability of the security of the informatization object are given, as well as individual approaches to assessing their danger. An aggregated approach is proposed for assessing the dangers of threats and vulnerabilities. The necessary criteria and system of experts' points are given. The technique of cross-assessment of threats and vulnerabilities of objects of informatization of railway transport is presented.