УДК 004.41:004.056

Метод управления рисками разработки программного обеспечения на основе алгоритмов анализа уязвимостей

Смирнов А.А., д.т.н., професор; Коваленко А.В., к.т.н., доцент;
Коваленко А.С., к.т.н.
Центральноукраинский национальный технический университет, м. Кропивницький

В настоящее время в большинстве организаций и предприятий различных форм собственности все больше внимания уделяется вопросам анализа и оценки рисков. Но, несмотря на это проблемы и вопросы, относящиеся к общей теории и методологии анализа, оценки и управления рисками требуют адаптации к подходам и положениям современного менеджмента, учета новых факторов становления и развития технологий, объединения известных «устоявшихся» положений теории рисков с новыми, прогрессирующими подходами анализа и синтеза. Всеобщие процессы глобализации экономических, финансовых, социальных и информационных отношений способствовали развитию направления риск-менеджмента. Однако общемировые финансовые кризисы показали недостаточно внимательное отношение к управлению рисками со стороны большинства представителей руководства организаций, в том числе и в Украине. Несмотря на достаточно глубокую историю развития понятия «риск» и попытки ряда известных авторов сконцентрировать свои разработки в область управления рисками отдельных отраслей и направлений деятельности, разработка новых, перспективных научных положений в этой области все же несколько «заужена» финансовой деятельностью. В то же время широкое использование в нашей работе информационных технологий требует повышенного внимания к этому направлению, и соответственно, более глубокого освещения вопросов риск-менеджмента IT-индустрии. Для управления рисками разработки программного обеспечения, в частности предлагается использовать следующие методы.

Алгоритм анализа DOM XSS уязвимости. Уязвимость DOM XSS представляет собой подвид XSS, в случае которой результат атаки находится не в ответе сервера и, соответственно, не в HTML коде, а в DOM структуре HTML страницы. Результаты атак посредством таких уязвимостей можно обнаружить только в процессе выполнения или анализе DOM структуры. Сам механизм атаки, а именно инъекция Javascript кода в уязвимый сегмент, остается неизменным.

Алгоритм анализа уязвимости к атакам SQL Injection. SQL инъекция возможна, если входные данные используются в запросах к БД без предварительной валидации. В данной реализации выполняется анализ параметров GET запроса на предмет наличия уязвимости.