Жарко Е.Ф.

Некоторые вопросы процесса верификации и валидации управления кибербезопасностью

Аннотация: В работе рассматриваются процессы обеспечения качества программного обеспечения для средств управления кибербезопасностью. В связи с тем, что системы управления могут быть модифицированы, то для обеспечения выполнения функций безопасности, необходимых для управления кибербезопасностью предложено использовать расширенный жизненный цикл разработки ПО. Также в работе предложена качественная модель процесса верификации и валидации управления кибербезопасностью.

Ключевые слова: программное обеспечение, верификация, валидация, кибербезопасность, критическая информационная инфраструктура

Цифровизация систем управления объектов критической информационной инфраструктуры (КИИ) обратила внимание на новую задачу – обеспечение их кибербезопасности. В первую очередь это связано с тем, что объекты КИИ в виду своей инерционности в части внедрения цифровых технологий в настоящее время находятся на ранней стадии решения задачи обеспечения кибербезопасности [1]. До последнего времени уделялось мало внимания задачам кибербезопасности по сравнению с другими вопросами безопасности, и одновременно стоит отметить закрытость информации по инцидентам и аварийным ситуациям [2]. Для обеспечения предоставления необходимой информации о имеющихся проблемах кибербезопасности были разработаны нормативные документы, руководства и стандарты, в том числе в части оценки и выбора средств управления кибербезопасностью. Управление кибербезопасностью в первую очередь – это меры безопасности или контрмеры, которые позволяют избегать, обнаруживать, минимизировать риски кибербезопасности для физического имущества, информации, компьютерных систем и других активов.

Необходимо учитывать, что сложная структура объектов КИИ и большое количество средств управления кибербезопасностью

затрудняют верификацию и применение средств управления кибербезопасностью на всех этапах жизненного цикла от проектирования до эксплуатации. В связи с этим для усилия направлены на разработку методологии оценки и выбора средств управления кибербезопасностью. Данный подход применяется при разработке систем верхнего уровня объектов КИИ.

Однако применение мер безопасности в системах управления объектов КИИ является не только проблемой защищенности, но и проблемой безопасности системы в целом. Это связано с тем, что функции безопасности и защищенности могут влиять друг на друга и вызывать проблемы безопасности. Поэтому особую важность приобретает безопасное управление конфигурацией при интеграции, при этом производительность и надежность систем управления объектов КИИ не должны ухудшаться средствами управления кибербезопасностью. Стоит отметить, что в существующих руководствах по кибербезопасности подчеркивается, что некоторые средства контроля защищенности, которые могут оказать негативное влияние на функции обеспечения безопасности и защиты, должны быть верифицированы для подтверждения отсутствия неблагоприятного влияния.

В связи с внедрением новых технологий (таких как искусственный интеллект и кибербезопасность), разработчиков программного обеспечения (ПО) для систем управления объектов КИИ внимание привлекли новые типы программных сбоев и неисправностей. Однако из-за присущих характеристик и практических ограничений программного обеспечения систем управления объектов КИИ подходы количественного измерения надежности программного обеспечения имеют некоторые ограничения в демонстрации требуемого уровня надежности. Одним из наиболее перспективных альтернативных подходов является использование информации о качестве разработки программного обеспечения. С этой точки зрения предложен метод оценки надежности программного обеспечения на основе процесса верификации и валидации [3], позволяющий моделировать процесс внесения и устранения ошибок на каждом этапе разработки.

Разработка программного обеспечения обычно адаптируется к одному из классических жизненных циклов ПО [4]. В классическом жизненном цикле процесс разработки ПО можно рассматривать как

эволюцию ПО, которая проходит через упорядоченную последовательность переходов от одной фазы к другой в порядке очередности. Ошибки ПО вносятся и устраняются в ходе переходного процесса на каждом этапе разработки, и количество внесенных в процессе разработки ошибок сильно зависит от качества процесса разработки ПО. Ошибки, внесенные разработчиками или средствами разработки ПО, устраняются проведением верификации и валидации. На рисунке 1 представлена упрощенная модель внесения и устранения ошибок на этапе разработки. Используя байесовскую сеть доверия, число оставшихся отказов может быть оценено с учетом факторов, имеющих отношение к надежности, таких как качество управления процессом разработки, сложность процесса и т.д.

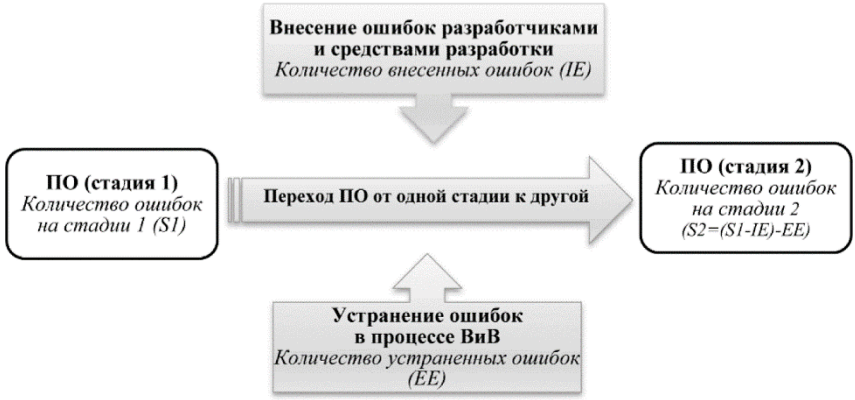

Рисунок 1 – Схема внесения/устранения ошибок на каждом этапе разработки ПО

В перспективе системы управления объектов КИИ будут защищены мерами кибербезопасности, применяемых регулирующими органами, которые будут включать подсистемы безопасности, такие как система обнаружения вторжений, система наблюдения, система контроля доступа и т.д. Системы управления могут быть модифицированы с целью обеспечения выполнения функций безопасности, необходимых для управления кибербезопасностью, на основе расширенного жизненного цикла

разработки ПО (рисунок 2) [1]. Применение мер управления кибербезопасностью повышает уровень связности системы, а также уровень ее безопасности. Уровень связности является активно используемой мерой, которая фиксирует зависимости, существующие между каждым компонентом ПО и каждой системой [5]. По мере увеличения уровня связности, частота программных сбоев имеет тенденцию к увеличению. Поэтому чрезмерные модификации при применении средств управления кибербезопасностью могут привести к увеличению размера и сложности ПО систем, а также увеличить риск программного сбоя. Кроме того, применение средств управления кибербезопасностью без тщательной проверки качества может усложнить не только структуру системы, но также процессы разработки и интеграции программного обеспечения, что в свою очередь увеличит вероятность сбоев программного обеспечения. Сбои в работе ПО и оставшиеся ошибки, вызванные применением мер безопасности, рассматриваются как серьезная проблема, влияющая на безопасность.

Рисунок 2 – Расширенная V-образная модель жизненного цикла программного обеспечения для обеспечения качества программного обеспечения

Для надежного управления процессом применения средств управления кибербезопасностью, необходимо обеспечивать качество ПО, используя различные методы проверки и тестирования. В области разработки систем управления могут потребоваться дополнительные мероприятия по обеспечению качества средств управления кибербезопасностью.

На рисунке 3 приведена качественная модель процесса верификации и валидации управления кибербезопасностью.

Рисунок 3 – Процесс оценки вероятности сбоя ПО

Первым этапом является разработка процесса применения средств управления кибербезопасностью на основе соответствующих цифровых устройств и функций безопасности, необходимых для каждого элемента управления безопасностью. На втором этапе оценивается отказоустойчивость каждого элемента управления безопасностью, и на основе оценки выявляются и расставляются приоритеты для элементов управления кибербезопасностью. На третьем этапе проверочные тесты

проводятся после определения соответствующего объема и уровня проверки в зависимости от предполагаемой отказоустойчивости каждого элемента управления безопасностью. На четвертом этапе в соответствии с результатами проверочного теста происходит принятие каждого элемента управления безопасностью. Только средства управления безопасностью, прошедшие верификационные тесты, могут применяться к цифровым системам и далее подвергаться постоянному мониторингу. Средства управления кибербезопасностью, которые еще не прошли верификационные тесты, должны быть перепроверены и/или пересмотрены.

Литература:

1. *Жарко Е.Ф., Промыслов В.Г., Исхаков А.Ю., Мещеряков Р.В., Семенков К.В., Абдулова Е.А., Байбулатов А.А., Исхаков С.Ю.* Кибербезопасность беспилотных транспортных средств. Архитектура. Методы проектирования. – М.: Радиотехника, 2021. – 160 с.

2. *Baylon C., Brunt R., Livingstone D.* Cyber security at civil nuclear facilities: understanding the risks. – Chatham House, 2016. – 56 p.

3. *Eom H.S., Park G.Y., Jang S.C., Son H.S., Kang H.G.* V&V-based remaining fault estimation model for safety-critical software of a nuclear power plant // Annals of Nuclear Energy. – 2013. – Vol. 51. – P. 38-49.

4. *Жарко Е.Ф.* Сравнение моделей качества программного обеспечения: аналитический подход // Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). – М.: ИПУ РАН, 2014. – С. 4585-4594.

5. *Жарко Е.Ф.* Формализация функций безопасности и обеспечение качества программного обеспечения систем, важных для безопасности АЭС / Материалы 12-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2019) (1-3 октября 2019 г. Москва). – М.: ИПУ РАН, 2019. – С. 844-847.