DOI:

ВЕРИФИКАЦИЯ И КИБЕРБЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМ ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ АЭС

Жарко Е.Ф.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65
zharko@ipu.ru

Аннотация: Верификация программного обеспечения является фундаментальным и наиболее распространенным видом деятельности для обеспечения качества программных систем. В статье предлагается применение методологии верификации для обеспечения кибербезопасности систем важных для безопасности АЭС.

Ключевые слова: атомная электростанция, кибербезопасность, верификация, валидация, жизненный цикл програмного обеспчения.

Введение

Цифровизация автоматизированных систем управления технологическим процессом (АСУ ТП) атомных электростанций (АЭС) обратила внимание на новую задачу – обеспечение кибербезопасности АЭС. В первую очередь это связано с тем, что атомная энергетика в виду своей инерционности в части внедрения цифровых технологий в настоящее время находится на ранней стадии решения задачи обеспечения кибербезопасности. До последнего времени в атомной энергетике уделялось мало внимания задачам кибербезопасности по сравнению с другими вопросами безопасности, и одновременно стоит отметить закрытость информации по инцидентам и аварийным ситуациям [1]. 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 [2-4]. 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 АСУ ТП и большое количество средств управления кибербезопасностью затрудняют верификацию и применение средств управления кибербезопасностью на всех этапах жизненного цикла от проектирования до эксплуатации [5]. В связи с этим для усилия направлены на разработку методологии оценки и выбора средств управления кибербезопасностью. Данный подход применяется при разработке систем верхнего уровня АСУ ТП АЭС [6, 7].

Однако применение мер безопасности в АСУ ТП АЭС 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 [8]. Поэтому особую важность приобретает безопасное управление конфигурацией при интеграции ядерной безопасности и защищенности [9], при этом производительность и надежность АСУ ТП не должны ухудшаться средствами управления кибербезопасностью.

Фактически, 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 [2]. Для обеспечения объективного контекста для субъективных суждений экспертов, в статье предлагается систематический и количественный метод.

1 Анализ влияния средств управления кибербезопасности

В атомной энергетике, в соответствии с нормативными документами, надежность цифровых систем важных для безопасности должна быть не ниже чем у аналоговых систем. В связи с внедрением новых технологий (таких как искусственный интеллект и кибербезопасность), разработчиков программного обеспечения (ПО) для систем АСУ ТП внимание привлекли новые типы программных сбоев и неисправностей. В области атомной энергетики был предложен безопасный процесс управления конфигурацией программного обеспечения в части защиты от сбоев ПО и уязвимостей АСУ ТП [10], а также предложена модель вероятностной оценки безопасности с учетом влияния ошибок ПО [11]. Обнаруживаемость программных ошибок в АСУ ТП может быть оценена путем расчета зон необнаружения цифровых датчиков [12, 13]. Была разработана модель байесовской сети

доверия для оценки потенциального риска, связанного с ошибками программного обеспечения, и оценки качества цифровых систем контроля и управления [14].

Однако из-за присущих характеристик и практических ограничений программного обеспечения систем, обеспечивающих безопасность или важных для безопасности, 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 ПО. С этой точки зрения был предложен метод оценки надежности программного обеспечения на основе процесса верификации и валидации (ВиВ) [15], позволяющий моделировать процесс внесения и устранения ошибок на кажом этапе разработки.

Разработка программного обеспечения для систем важных для безопасности АЭС обычно адаптируется к одному из классических жизненных циклов ПО [16]. 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 рис. 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.

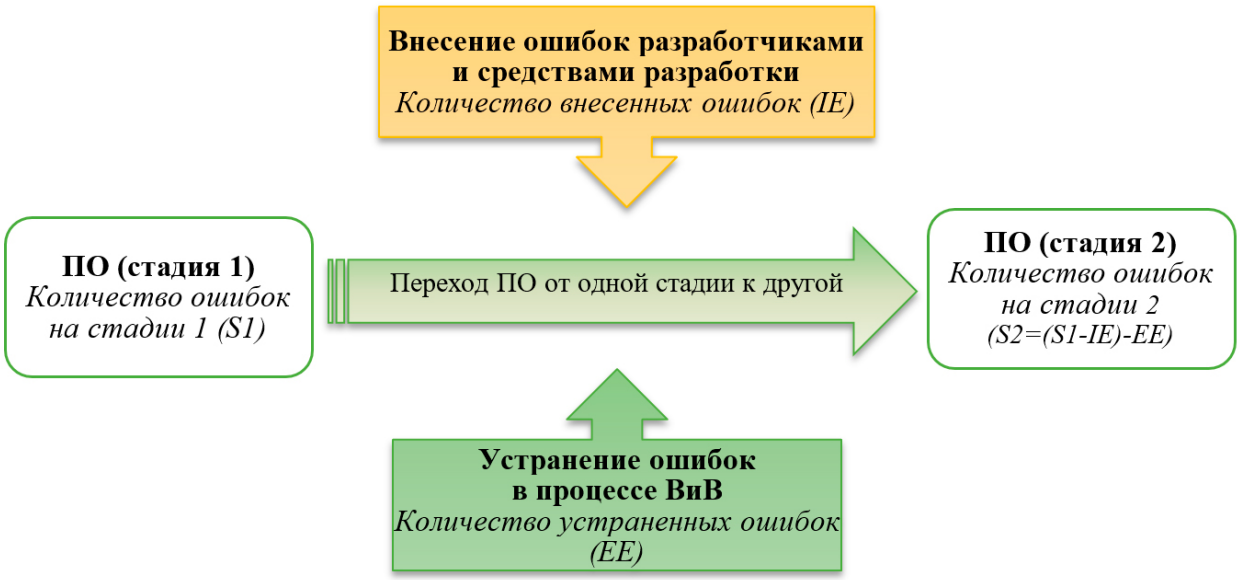

Рис. 1. Схема внесения/устранения ошибок на каждом этапе разработки ПО.

В перспективе АСУ ТП АЭС 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 АСУ ТП АЭС могут быть модифицированы с целью обеспечения выполнения функций безопасности, необходимых для управления кибербезопасностью, на основе расширенного жизненного цикла разработки ПО [17] (см. рис. 2). 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 [18]. 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. В работе сбои в работе ПО и оставшиеся ошибки, вызванные применением мер безопасности, рассматриваются как серьезная проблема, влияющая на безопасность.

Для надежного управляния процессом применения средств управления кибербезопасностью, необходимо обеспечивать качество ПО, используя различные методы проверки и тестирования [19]. В области разработки систем для АСУ ТП АЭС могут потребоваться дополнительные мероприятия по обеспечению качества средств управления кибербезопасностью.

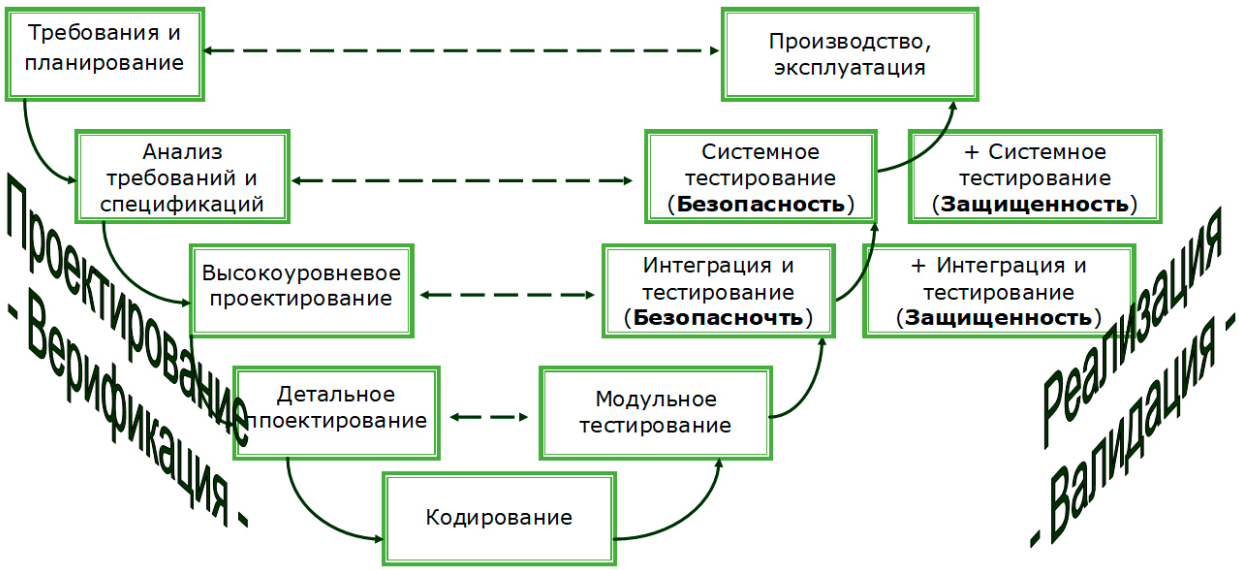

Рис. 2. Расширенная V-образная модель жизненного цикла программного обеспечения для обеспечения качества программного обеспечения систем, важных для безопасности АЭС.

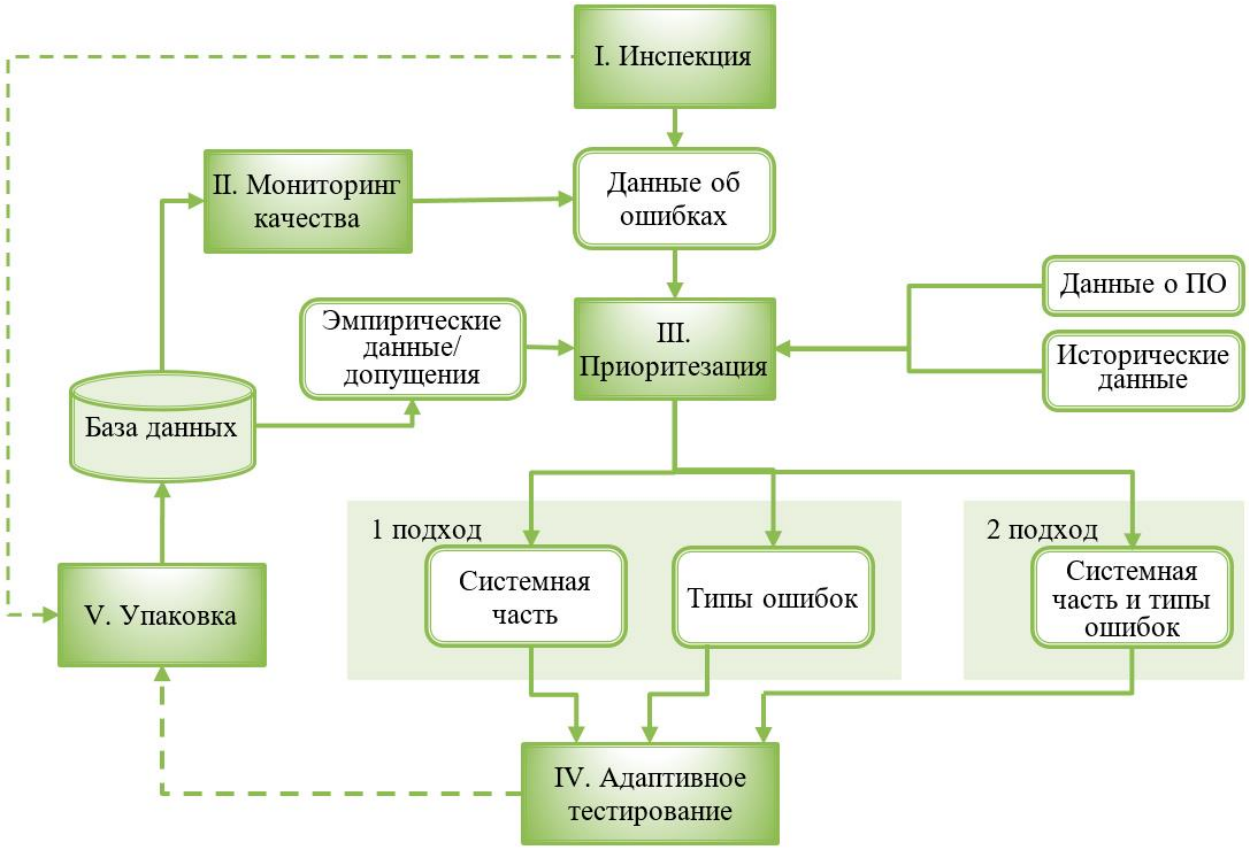

Рис. 3. Адаптивное тестирование и качество ПО.

2 Концепция адаптивного тестирования

В области информационных технологий существует концепция интеграции инспекционных и испытательных мероприятий, называемая адаптивным тестированием и направленная на уменьшение

затрат на обеспечение качества программного обеспечения. Применяя концепцию адаптивного тестирования [20] при тестировании качества ПО можно сосредоточиться в первую очередь на подверженных ошибкам модулях ПО, что сокращает затраты на тестирование. Подход к адаптивному тестированию, его процессам и требуемой информации представлены на рис. 3. В этом подходе необходимы знания о взаимосвязи между результатами инспекций и соответствующими проверочными тестами.

Однако в атомной энергетике такие знания часто зависят от контекста или их трудно получить экспериментальным путем, поскольку системы, важные для безопасности, редко демонстрируют ошибки и сбои во время проведения проверочных испытаний, направленных на подтверждение требований спецификаций. Для решения этой проблемы предлагается интегрированная модель для оценки вероятности сбоя программного обеспечения с учетом необнаруженных ошибок. Эта модель основывается на оценке вероятности сбоя ПО на основе результатов проверок и проверочных испытаний. Поскольку ПО систем, важных для безопасности АЭС, представляет собой комбинацию модуля операционной системы (ОС) и модуля прикладной программы (ППО), который в свою очередь состоит из двух частей: части для нормальной эксплуатации системы и части, предназначенной для отключения системы. Часть, предназначенная для нормальной эксплуатации системы, – это часть, содержащая инструкции, которые периодически выполняются в нормальном состоянии системы, а часть, предназначенная для отключения системы, – это часть, которая содержит инструкции, выполняемые только при условии достижения эксплуатационными параметрами уставок, предусмотренных для отключения системы. Вероятность сбоя ПО системы, важной для безопасности АЭС, можно представить как функцию вероятностей отказов ОС и ППО следующим образом:

(1) $$\boldsymbol{p} = \boldsymbol{f}(\boldsymbol{p}_{\text{ОС}}, \boldsymbol{p}_{\text{ППО}})$$

(2) $$\boldsymbol{p}_{\text{ППО}} = \boldsymbol{f}\left(\boldsymbol{p}_{\text{ППОн}}, \boldsymbol{p}_{\text{ППОа}}\right)$$

где $p_{\text{ОС}}$ и $p_{\text{ППО}}$ – вероятности отказов модулей ОС и ППО, $p_{\text{ППОн}}$ – вероятность отказа части ППО, ответственной за нормальную эксплуатацию, а $p_{\text{ППОа}}$ - вероятность отказа части ППО, отвечающей за отключение системы.

В этой модели предполагается, что оставшиеся ошибки могут быть активированы случайным образом во время выполнения программы, и априорная вероятность сбоя ПО, p, во время выполнения программы может быть оценена на основе биномиального распределения, с учетом числа оставшихся ошибок и вероятности активации ошибки:

(3) $$\boldsymbol{p} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{k}} \left(\frac{\boldsymbol{k}}{\boldsymbol{l}}\right) \boldsymbol{p}_{\boldsymbol{a}}^{\boldsymbol{i}} \left(\boldsymbol{1} - \boldsymbol{p}_{\boldsymbol{a}}\right)^{\boldsymbol{k-i}}$$

где k – количество оставшихся ошибок, а p_a – вероятность случайной активации отдельной оставшейся ошибки. Число оставшихся ошибки может быть оценено с использованием модели, предложенной [15], и вероятность активации ошибки должна выбираться на основе консервативного подхода.

(4) $$\boldsymbol{E}_{\boldsymbol{p}_{\text{ОС}}} = \frac{\boldsymbol{\alpha}_{\text{ОС}}}{\boldsymbol{\alpha}_{\text{ОС}} + \boldsymbol{\beta}_{\text{ОС}}}$$

(5) $$\boldsymbol{D}_{\boldsymbol{p}_{\text{ОС}}} = \frac{\boldsymbol{\alpha}_{\text{ОС}}\boldsymbol{\beta}_{\text{ОС}}}{\left(\boldsymbol{\alpha}_{\text{ОС}} + \boldsymbol{\beta}_{\text{ОС}}\right)^{\boldsymbol{2}}\left(\boldsymbol{\alpha}_{\text{ОС}} + \boldsymbol{\beta}_{\text{ОС}} + \boldsymbol{1}\right)}$$

где параметры бета-распределения $\alpha_{\text{ОС}}$; $\beta_{\text{ОС}}$ оцениваются по предыдущему значению математического ожидания $E_{p_{\text{ОС}}}$, определенного на основе биномиальной модели, и дисперсии $D_{p_{\text{ОС}}}$. Предыдущее значение вероятности сбоя ПО может быть скорректировано следующим образом:

(6) $$\boldsymbol{p}_{\text{ОС}} = \frac{\boldsymbol{\alpha}_{\text{ОС}}}{\boldsymbol{\alpha}_{\text{ОС}} + \boldsymbol{\beta}_{\text{ОС}} + \boldsymbol{f}_{\text{ОС}}\boldsymbol{\tau}}$$

(7) $$\boldsymbol{p}_{\text{ППОн}} = \frac{\boldsymbol{\alpha}_{\text{ППО}}}{\boldsymbol{\alpha}_{\text{ППО}} + \boldsymbol{\beta}_{\text{ППО}} + \boldsymbol{f}_{\text{ППО}}\boldsymbol{\tau}}$$

(8) $$\boldsymbol{p}_{\text{ППОа}} = \frac{\boldsymbol{\alpha}_{\text{ППО}}}{\boldsymbol{\alpha}_{\text{ППО}} + \boldsymbol{\beta}_{\text{ППО}} + \boldsymbol{n}_{\boldsymbol{test}}}$$

где $f_{\text{ОС}}$ и $f_{\text{ППО}}$ – частота сканирования модулей ОС и ППО, τ – время проведения теста в секундах, n_{test} - количество тестов, выполненных для изменения состояния отключения. Процесс оценки вероятности сбоя ПО представлен на рис. 4.

Хотя оценочную модель вероятности сбоя ПО можно использовать для проверки предположения, что программное обеспечение является достаточно надежным после применения средств контроля

кибербезопасности, но результаты этой проверки не могут учитываться при проведении проверочных испытаний. Даже при проведении инспекций и испытаний они обычно применяются изолированно, без обмена информацией между двумя процессами, что приводит к неэффективности процесса проверки. Следовательно, для каждой системы, важной для безопасности АЭС, должна быть разработана эффективная модель процесса проверки, которая идентифицирует и устанавливает приоритеты элементов управления безопасностью, предрасположенных к сбоям, и проводит проверочные тесты в зависимости от степени предрасположенности к сбоям.

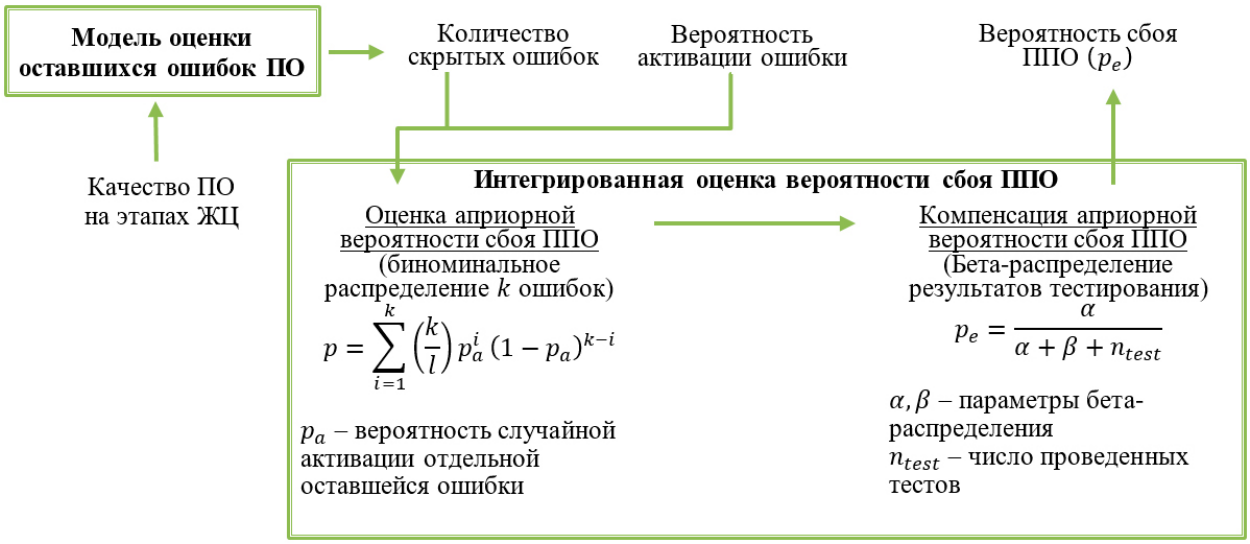

Рис. 4. Процесс оценки вероятности сбоя ПО.

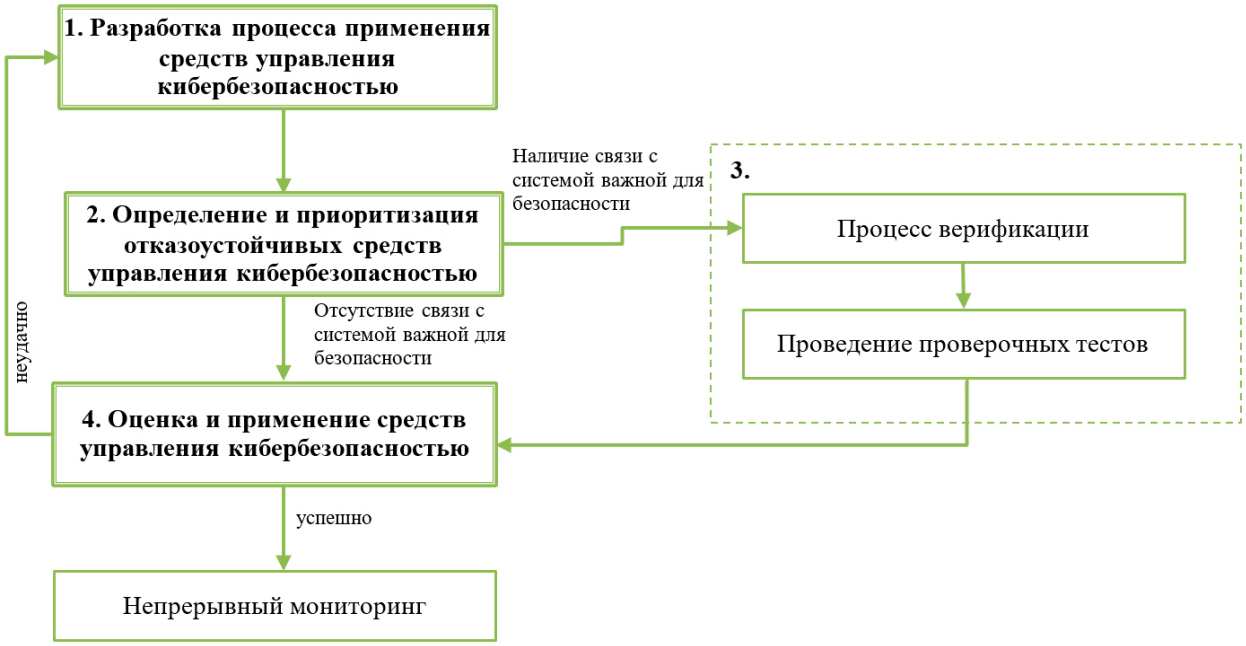

Рис. 5. Качественная модель ВиВ управления кибербезопасностью.

3 Качественная модель ВиВ управления кибербезопасностью

На рис. 5 приведена качественная модель процесса верификации и валидации управления кибербезопасностью. Первым этапом является разработка процесса применения средств управления кибербезопасностью на основе соответствующих цифровых устройств и функций безопасности [21], 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.

Заключение

Верификация и валидация программного обеспечения систем важных для безопасности АЭС являются процессами важными для обеспечения качества ПО на протяжении всего жизненного цикла. В работе предложено использовать процессы обеспечения качества программного обеспечения для средств управления кибербезопасностью, на основе концепции адаптивного тестирования, а также представлена качетвенная модель процесса верификации и валидации управления кибербезопасностью.

Литература

1. *Baylon C., Brunt R., Livingstone D.* Cyber security at civil nuclear facilities: understanding the risks. – Chatham House, 2016. – 56p.
2. Regulatory Guide 5.71 (Ed.), 2010. Cyber Security Programs for Nuclear Facilities. U.S. Nuclear Regulatory Commission.
3. IEEE Std 7-4.3.2-2016. IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations. 2016.
4. Компьютерная безопасность на ядерных установках // Серия изданий МАГАТЭ по физической ядерной безопасности. № 17. 2012.
5. *Song J.G, Lee J.W., Park G.Y, Kwon K.C., Lee D.Y., Lee C.K.* An analysis of technical security control requirements for digital I&C systems in nuclear power plants // Nuclear Engineering and Technology. Vol. 45. 2013, issue 5. – P.637–652.
6. *Полетыкин А.Г., Жарко Е.Ф., Менгазетдинов Н.Э., Промыслов В.Г.* Новое поколение систем верхнего уровня и концепция Industry 4.0 // Материалы 10-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2017, Москва). – М.: ИПУ РАН, 2017, Т. 1. – С.101-107.
7. *Бывайков М.Е., Жарко Е.Ф., Менгазетдинов Н.Э., Полетыкин А.Г., Прангишвили И.В., Промыслов В.Г.* Опыт проектирования и внедрения системы верхнего блочного уровня АСУ ТП АЭС // Автоматика и телемеханика. 2006. № 5. – С.65-79.
8. *Gandhi S., Kang J.* Nuclear safety and nuclear security synergy // Annals of Nuclear Energy. Vol. 60, 2013. – P.357–361.
9. *Kaur R.K., Pandey B., Singh L.K.* Dependability analysis of safety critical systems: issues and challenges // Annals of Nuclear Energy. Vol. 120. 2018. – P.127–154.
10. *Chou I.H.* Secure software configuration management processes for nuclear safety software development environment // Annals of Nuclear Energy. Vol. 38. 2011. – P.2174–2179.
11. *Lee S.J., Jung W.Y., Joon E.* PSA model with consideration of the effect of fault-tolerant techniques in digital I&C systems // Annals of Nuclear Energy. Vol. 87. 2016. – P.375–384.
12. *Li W., Peng M., Wang Q.* Fault detectability analysis in PCA method during condition monitoring of sensors in a nuclear power plant // Annals of Nuclear Energy. Vol. 119. 2018. – P.342–351.
13. *Промыслов В.Г., Тимофеев М.Ю., Полетыкин А.Г., Бабаев Д.И.* Управление архитектурой кибербезопасности АСУ ТП АЭС // Проблемы управления. 2018. № 3. – С.47–55.
14. *Kang H.G., Lee S.H., Lee S.J., Chu T.L., Varuttamaseni A., Yue M., Yang S., Eom H.S., Cho J., Li M.* Development of a bayesian belief network model for software reliability quantification of digital protection systems in nuclear power plants // Annals of Nuclear Energy. Vol. 120. 2018. – P.62–73.
15. *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. Vol. 51. 2013. – P.38–49.
16. *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.

17. *Жарко Е.Ф.* Программное обеспечение для систем с повышенным риском эксплуатации // Труды 8-ой Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2015, Москва). – М.: ИПУ РАН, 2015. Т. 2. – С.114-118.
18. *MacCormack A., Sturtevant D.J.* Technical debt and system architecture: the impact of coupling on defect-related activity // Journal of Systems and Software. Vol. 120. 2016. – P.170–182.
19. *Myers G.J., Sandler C., Badgett T.* The Art of Software Testing. – John Wiley & Sons. 2011. – 254p.
20. *Elberzhager F., Kremer S., Munch J., Assmann D.* Focusing testing by using inspection and product metrics // International Journal of Software Engineering and Knowledge Engineering. Vol. 23. 2013, № 04. – P.433-462.
21. *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, Москва). – М.: ИПУ РАН, 2019. – С.844-847.