УДК 004.056.5
DOI: 10.53403/9785951505460_519

ОСОБЕННОСТИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ В РАМКАХ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Метелева Юлия Леонидовна (niiis@niiis.nnov.ru), Павлин Артем Юрьевич, Лепёхин Игорь Юрьевич, Харченко Сергей Петрович

Филиал РФЯЦ-ВНИИЭФ «НИИИС им. Ю. Е. Седакова», г. Нижний Новгород

Работа посвящена описанию особенностей разработки программного обеспечения (ПО) автоматизированных систем управления технологическими процессами (АСУ ТП) в рамках системы менеджмента информационной безопасности (СМИБ). Основной особенностью процесса разработки ПО, удовлетворяющего требованиям информационной безопасности, является структурирование на этапы процесса разработки ПО с конкретизацией требований к каждому этапу.

Ключевые слова: ИБ, ПО; СМИБ; АСУ ТП.

FEATURES OF THE DEVELOPMENT OF SOFTWARE FOR AUTOMATED PROCESS CONTROL SYSTEMS IN THE FRAMEWORK OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

Meteleva Iuliia Leonidovna (e-mail: j.meteleva@yandex.ru), Pavlin Artem Yuryevich, Lepekhin Igor Yuryevich, Kharchenko Sergey Petrovich

Branch RFNC-VNIIEF «NIIIS named after Yu. Ye. Sedakov», Nizhny Novgorod

The work presents description of the software development (software) features for automated process control systems (APCS) within the information security management system (ISMS). The main feature of the software development process that meets the information security requirements is structuring the process of the software development into stages, specifying the requirements for each stage.

Keywords: IS, software, ISMS, APCS.

Введение

В настоящее время филиал – один из крупнейших разработчиков, производителей и поставщиков оборудования АСУ ТП и систем автоматизации для АЭС. Филиал осуществляет проектирование, разработку, изготовление и испытания оборудования АСУ ТП и систем автоматизации для объектов атомной энергетики.

Для выполнения работ по международным проектам в филиале ФГУП «РФЯЦ-ВНИИЭФ» «НИИИС им. Ю.Е. Седакова» (филиал) в 2019 году была внедрена система менеджмента информационной безопасности, соответствующая требованиям международного стандарта ISO/IEC 27001:2013 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Основной особенностью процесса разработки ПО, удовлетворяющего требованиям информационной безопасности, является структурирование на этапы процесса разработки ПО с конкретизацией требований к каждому этапу [1, 2]:

− этап I «Формирование требований к ПО» (выделение отдельных требований по информационной безопасности);

− этап II «Разработка проекта архитектуры ПО» (описание реализации требований по информационной безопасности, проведение предварительного анализа уязвимостей предполагаемых к использованию программных компонентов);

− этап III «Разработка исходного кода, документации» (разработка кода осуществляется только идентифицированными средствами разработки);

− этап IV «Тестирование ПО» (применение статического анализа кода, применение динамического тестирования и фаззинг-тестирования);

– этап V «Валидация ПО»;

– этап VI «Интеграция программы и поддержка приемки ПО»;

– этап VII «Поддержка и модификация ПО на протяжении гарантийного обслуживания» (проведение периодического анализа вновь появляющихся уязвимостей и оценка их влияния на ПО).

В результате проведенного анализа была составлена диаграмма процесса разработки ПО. Условные обозначения диаграммы процесса приведены на рис. 1.

Диаграмма процесса разработки ПО приведена на рис. 2.

В филиале в составе научно-исследовательского отделения по разработке АСУ ТП объектами АЭ была создана группа, занимающаяся вопросами информационной безопасности (далее – группа по ИБ). Группа по ИБ определяет предъявляемые к разрабатываемому ПО требования по информационной безопасности [3, 4].

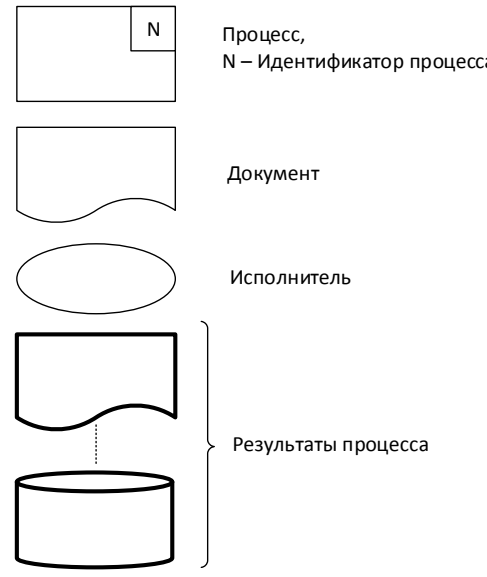

Рис. 1. Условные обозначения диаграммы процесса

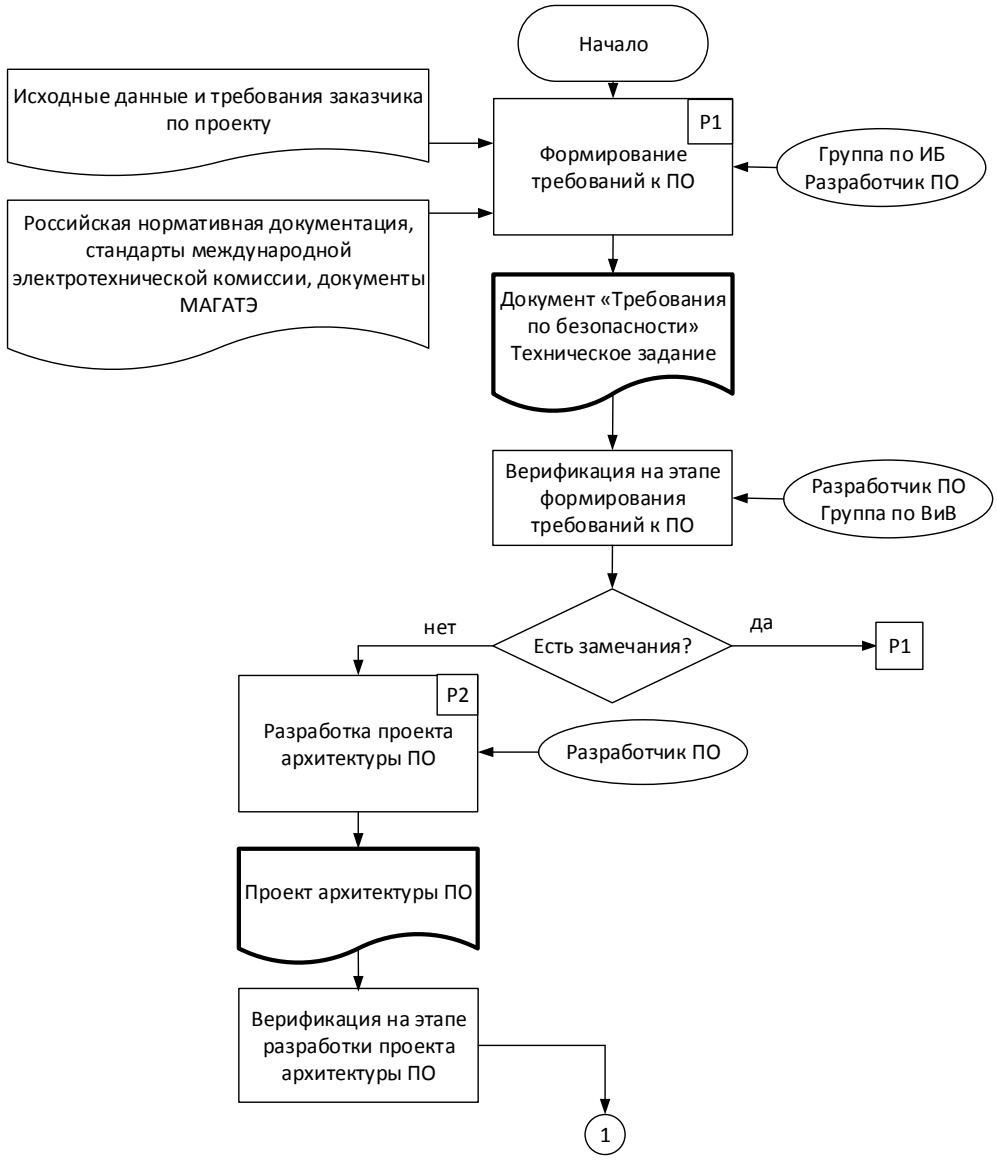

Рис. 2. Диаграмма процесса разработки ПО

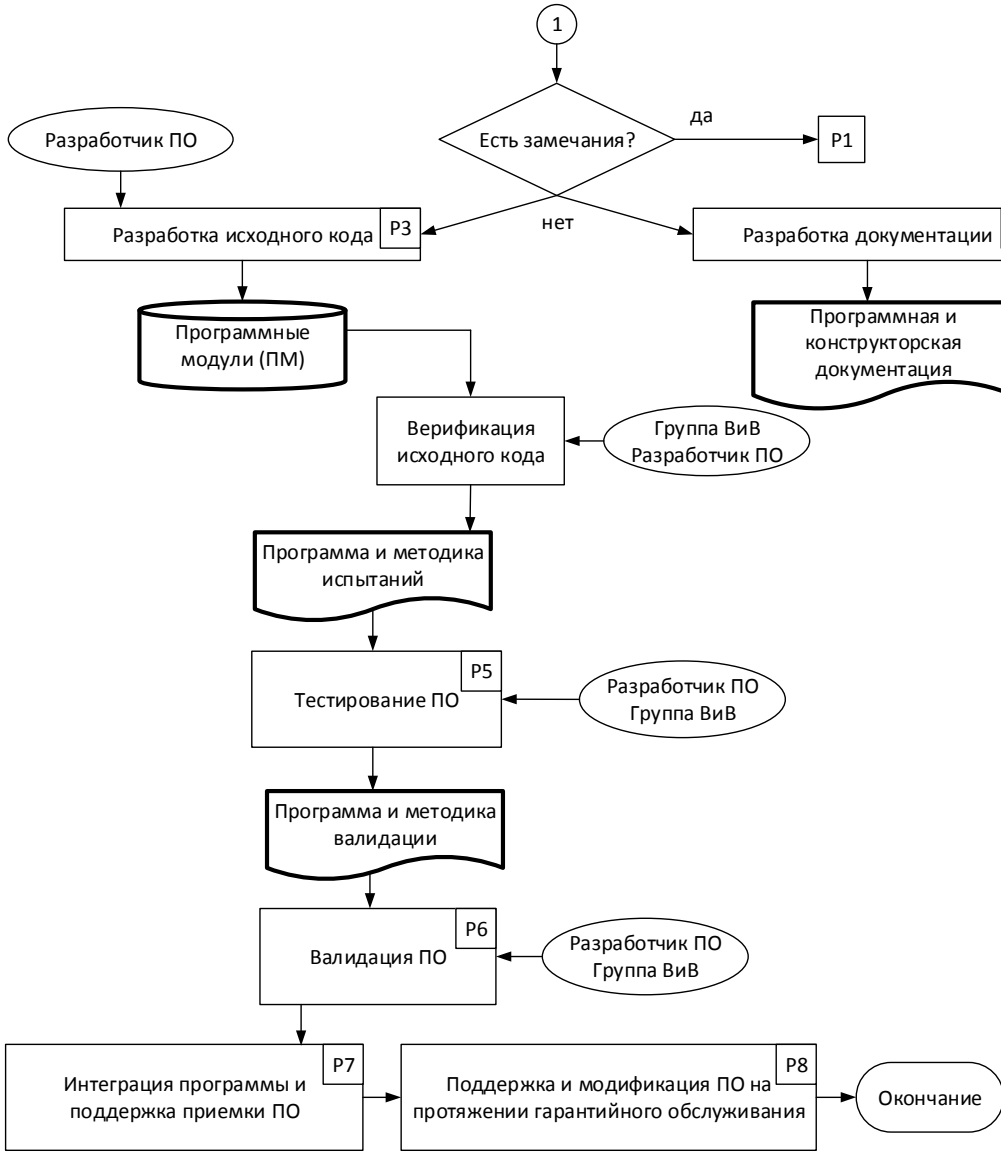

Рис. 2. Диаграмма процесса разработки ПО (Продолжение)

I этап «Формирование требований к ПО»

Группой по ИБ проводится анализ исходных данных и требований заказчика к разрабатываемому ПО, определяются отдельные требования по ИБ, предъявляемые к ПО на каждом этапе жизненного цикла. Разрабатывается документ, который представляет из себя перечень требований по предотвращению угроз информационной безопасности и исключению уязвимостей с указанием соответствующего этапа жизненного цикла ПО [5, 6].

В качестве источников для формирования требований группа по ИБ использует требования российской нормативной документации (Приказ ФСТЭК № 31 от 14 марта 2014 г., ФЗ № 187 от 26 июля 2017 г., Приказ ФСТЭК № 235 от 21.12.2017 г., Приказ ФСТЭК № 239 от 25.12.2017 г.), стандартов международной электротехнической комиссии (IEC 61513:2011, IEC 60880:2006, IEC 62645:2019, IEC 62859:2016, IEC 63096), документов международного агентства по атомной энергии (NSS 17, NST036, NST037, NST038, NST045, NST047), локальные нормативные правовые акты филиала, отраслевые стандарты ГК «Росатом», требования заказчика.

Требования по информационной безопасности, предъявляемые к разрабатываемому ПО, а также конкретные способы их реализации в разрабатываемом ПО, должны быть отражены в Техническом задании (ТЗ), либо в техническом проекте к данному ПО.

После согласования и утверждения требований по информационной безопасности к ПО и ТЗ проводится процедура верификации с учетом следующих критериев:

– исходные функциональные требования полностью отражены в ТЗ на разработку ПО;

– требования по информационной безопасности полностью отражены в ТЗ на разработку ПО;

– сформулированные требования к ПО не противоречат исходным требованиям и требованиям по информационной безопасности.

Верификация проводится группой по верификации, созданной по указанию главного конструктора филиала по АСУ ТП – начальника конструкторского бюро в соответствии с планом верификации, разработку которого организует начальник группы по верификации, с привлечением разработчиков смежных отделов.

Результатом процесса верификации ТЗ является отчет по верификации, согласованный с группой по ИБ на этапе формирования требований к ПО [7].

II этап «Разработка проекта архитектуры ПО»

Проект архитектуры ПО является основой для разработки ПО в виде программного кода. Проект архитектуры должен удовлетворять критериям полноты, точности и непротиворечивости отражения требований, сформированных в ТЗ и оформлен в соответствии с нормативными документами и стандартами атомной отрасли.

Проект архитектуры ПО должен содержать детализированное описание архитектуры ПО, его структуры и состава. В проекте архитектуры ПО должны быть подробно описаны режимы работы ПО, указаны разрешения и ограничения при выполнении конкретных операций пользователями с разными учетными записями.

В проекте архитектуры ПО должны быть перечислены используемые при разработке системное ПО, базы данных, сторонние утилиты, языки программирования и инструментальные средства. Проект архитектуры ПО должен содержать идентифицированные инструментальные средства и системное ПО.

При выполнении проектирования архитектуры ПО разработчик (группа разработчиков) реализовывает следующие мероприятия:

− проводит моделирование угроз безопасности информации или определяет применимые механизмы обеспечения ИБ в соответствии с отраслевыми стандартами атомной энергетики;

− разрабатывает сформулированные в ТЗ политику, план и конкретные процедуры реализации требований по информационной безопасности;

− уточняет проект архитектуры ПО с учетом разработанных процедур реализации требований по информационной безопасности.

Исходными данными для моделирования угроз информационной безопасности являются информация Проекта архитектуры ПО о логической структуре ПО и информация из открытых источников (например, из банка данных угроз безопасности информации ФСТЭК России), связанная с типовыми сценариями компьютерных атак и угрозами безопасности информации. Выявленные в результате моделирования вероятные угрозы информационной безопасности должны стать исходными данными при проведении тестирования ПО.

После согласования и утверждения проекта архитектуры ПО проводится его верификация.

Результатом процесса верификации проекта архитектуры ПО является отчет по верификации, согласованный с группой по ИБ на этапе проектирования архитектуры ПО.

III этап «Разработка исходного кода, документации»

Программный код разрабатывается на основе требований, изложенных в ТЗ и Проекте архитектуры ПО. Программный код должен соответствовать требованиям ТЗ и Проекта архитектуры ПО.

Программный код должен быть организован в соответствии с правилами, изложенными в документе «Методические указания по оформлению исходного кода» и обеспечивать:

− надлежащую последовательность событий;

− согласованные интерфейсы;

− корректные данные и поток команд управления;

− определение ошибок, их локализацию и восстановление.

При разработке ПО разработчик должен:

− использовать идентифицированные инструментальные средства;

− учитывать требования по разработке ПО.

Под идентифицированными инструментальными средствами понимается задокументированный перечень ПО, содержащий:

− наименование ПО и версию;

− наименование разработчика;

− опции (настройки).

Перечень инструментальных средств, используемых при разработке ПО, согласовывается с начальником группы по ИБ, менеджером по ИБ и утверждается заместителем начальника научно-исследовательского отделения по разработке ПТС, ПТК и СКУ объектами АЭ.

Изделие программное (программные модули – ПМ) выполняется в виде компакт-диска, а также в электронном виде в архиве сетевого файлового ресурса филиала. Для каждого ПМ вычисляется контрольная сумма (КС) с использованием стандартного алгоритма (инструкция и приложение для подсчета КС записывается на носитель с ПМ).

Каждый ПМ сопровождается ведомостью магнитного носителя с записью (МНЗ). Ведомость МНЗ содержит наименование программы, КС, состав и объем информации в байтах на носителе.

Документация на программу разрабатывается в соответствии со стандартами Единой системы программной документации (ГОСТ 19 ЕСПД).

Разработка ПО и программной документации (ПД) ведется с применением репозитория в системе контроля версий. Каждая новая версия ПО и ПД сохраняется в папке программы в хранилище в соответствии с инструкцией по работе с хранилищем.

Каждый ПД, ПМ и исходный код ПМ должен быть верифицирован относительно полноты и согласованности с требованиями ТЗ на ПО и проекта ПО.

Исходные коды ПМ должны быть верифицированы с учетом следующих критериев:

− исходный код является следствием ТЗ на ПО и проекта ПО, а также соответствует установленным требованиям и стандартам, относящимся к кодированию;

− исходный код осуществляет надлежащую последовательность событий, согласованные интерфейсы, корректные данные и поток команд управления, а также определение ошибок, локализацию и восстановление;

− исходный код корректно реализует требования по информационной безопасности, защищенности и другим критическим свойствам;

− исходный код не содержит потенциально уязвимых конструкций, которые могут привести к наличию уязвимости в ПО.

Результатом процесса верификации ПО является отчет о верификации ПД, ПМ и исходных кодов ПМ, согласованный с группой по ИБ.

IV этап «Тестирование ПО»

Целью тестовых испытаний (предварительные испытания) является подтверждение соответствия разработанного ПО требованиям ТЗ.

Тестирование осуществляется разработчиками ПО при участии рабочей группы с привлечением группы по ИБ и в соответствии с программой и методикой испытаний. Ответственный за тестирование работник вычисляет КС, сравнивает ее с КС в утверждённом листинге и проводит тестирование в случае их совпадения. Если КС не совпали, заместителю начальника научно-исследовательского отделения по разработке ПТС, ПТК и СКУ объектами АЭ направляется соответствующая служебная записка.

При выполнении внутреннего тестирования ПО начальник группы по ИБ должен обеспечить проведение следующих мероприятий:

− функциональное тестирование ПО – проверка, выполняются ли требования информационной безопасности, идентифицированные в процессе анализа требований к ПО;

− тестирование устойчивости ПО на некорректные входные данные – установление влияния на функционирование ПО ввода (получения) некорректных (непредвиденных) входных данных, с целью выявления уязвимостей и иных дефектов ПО.

Результаты тестирования ПО должны быть занесены в протокол тестирования, доведены до сведения начальника группы по ИБ и заместителя начальника научно-исследовательского отделения по разработке ПТС, ПТК и СКУ объектами АЭ.

Протокол тестирования должен содержать:

− план тестирования, описание выполняемых тестов и инструментальных средств, используемых для данного вида тестирования;

− фактические результаты тестирования;

− отчеты, содержащие список выявленных несоответствий требованиям информационной безопасности и уязвимостей ПО, описание действий, направленных на их устранение, либо обоснование невозможности или отсутствия необходимости в устранении несоответствия требованиям информационной безопасности или уязвимости ПО;

− контрольную сумму дистрибутива ПО.

При обнаружении уязвимостей ПО или несоответствий ПО исходным требованиям начальник рабочей группы должен инициировать доработку ПО с последующим прохождением всех этапов коррекции и проверки.

Критериями верификации на этапе тестирования ПО являются:

− соответствие программы и методики испытаний требованиям нормативной документации;

− полнота (оценка) тестового покрытия;

− соответствие результатов испытаний требованиям ТЗ и Проекта ПО;

− корректность функционирования ПО при наличии искажающих воздействий;

− наличие встроенных тестов, проверенных при испытаниях, результаты которых свидетельствуют о ненадежности работы или непредусмотренном поведении ПО;

− корректность оформления протоколов испытаний.

Результатом процесса верификации является отчет по верификации на этапе тестирования ПО. В случае наличия замечаний по результатам верификации начальник группы ВиВ должен инициировать процедуру устранения этих замечаний. В этом случае вновь выполняются необходимые процедуры предыдущих процессов, после чего верификация этапа тестирования проводится повторно.

Этап V «Валидация ПО»

Протестированная версия ПО должна пройти процедуру валидации с целью подтверждения соответствия функционала разработанного ПО.

В соответствии с программой и методикой валидации валидация ПО должна проводиться членами группы ВиВ, в состав которой входят члены группы по ИБ.

Основными критериями валидации являются:

− ясность и корректность инструкций по инсталляции;

− соответствие ожидаемым результатам испытаний (получена информация, подтверждающая правильность выполнения операций и соответствие контролируемых параметров установленным критериям);

− готовность документации;

− возможность эксплуатации и сопровождения.

В случае наличия замечаний по результатам валидации ПО начальник группы по ВиВ должен инициировать процедуру устранения замечаний и повторную валидацию.

В случае отсутствия замечаний по результатам валидации ПО необходимые документы и носители данных передаются нормоконтролеру для проверки и последующей постановки на учет в архив.

В архиве филиала хранятся только актуальные версии документов, ПМ и ПО.

Этап VI «Интеграция программы и поддержка приемки ПО»

При выполнении интеграции ПО и поддержки приемки начальник группы по ИБ должен реализовать следующие мероприятия:

− обеспечение защиты ПО от угроз безопасности информации, связанных с нарушением целостности, в процессе его интеграции с оборудованием и передачи заказчику;

− поставка заказчику эксплуатационных документов.

При передаче заказчику рекомендуется опломбировать упаковку с поставляемым дистрибутивом ПО и документацией разрываемой при первом вскрытии упаковки наклейкой.

В состав поставляемого ПО должны быть включены эксплуатационные документы в объеме, достаточном для правильной настройки и безопасного применения ПО. При этом в эксплуатационные документы рекомендуется включить перечень и эталонные значения конфигурационных параметров ПО для выявления уязвимостей ПО, появившихся в результате определения конфигурации (параметров настройки) ПО.

Этап VII «Поддержка и модификация ПО на протяжении гарантийного обслуживания»

Разработчик ПО выполняет систематический поиск уязвимостей разрабатываемого ПО с целью выявления уязвимостей ПО и ее компонентов, в том числе компонентов ПО, заимствованных у сторонних производителей. Дополнительно в целях управления уязвимостями системного ПО на момент утверждения ТЗ на разработку ПО разработчик идентифицирует последнюю стабильную версию используемого системного ПО (или наборы соответствующих обновлений безопасности) и обеспечивает их использование на последующих этапах разработки ПО, если это не противоречит требованиям ТЗ.

Период изучения информации о возможных уязвимостях составляет не более полугода.

Основными источниками информации о возможных уязвимостях являются:

− сайты и новостные рассылки производителей ПО;

− корпоративные рассылки по ИБ;

− новостные сайты и рассылки третьих сторон;

− специализированные базы данных уязвимостей;

− другие уведомления об уязвимостях, обновлениях или угрозах;

− данные регулярного наблюдения за функционированием ПО.

Разработчик должен проанализировать поступившие от заказчика сообщения об ошибках или обнаруженных уязвимостях ПО. По результатам обработки сообщений от заказчика при необходимости должна проводиться доработка ПО. Должны быть проанализированы причины ошибок и уязвимостей ПО и приняты меры по предотвращению подобных ошибок и уязвимостей ПО в будущем.

Разработчик должен проанализировать отчет о поиске уязвимостей и сделать выводы о возможных уязвимостях разработанного ПО.

Разработчик выпускает отчет, содержащий перечень выявленных ошибок и уязвимостей ПО и описание действий, направленных на их устранение, либо обоснование невозможности или отсутствия необходимости в их устранении.

Любые модификации и модернизации ПО на этапе эксплуатации и обслуживания рассматриваются как мероприятия по разработке ПО и должны пройти все предусмотренные процедуры верификации и валидации.

Заключение

Процесс разработки ПО разбит на этапы, к которым предъявляются четко сформулированные требования, отраженные в документе «Положение о безопасной разработке ПО». После каждого этапа проводится верификация с результатами предыдущего этапа, что позволяет отслеживать разработку ПО, выявлять и устранять ошибки в ПО на ранних этапах.

Таким образом процесс разработки ПО приведен в соответствие требованиям системы менеджмента информационной безопасности филиала, на которую выдан сертификат BSI, подтверждаемый ежегодно.

Список литературы

1. ГОСТ Р ИСО/МЭК 12207-2010 Процессы жизненного цикла программных средств. ГОСТ Р 56939 2016 Разработка безопасного программного обеспечения. Общие требования.

2. Система менеджмента информационной безопасности. Положение о безопасной разработке программного обеспечениях» 195-95-90-9610-04/171 от 09.08.2019.

3. Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Современные методы обеспечения безопасности в атомной энергетике. Монография под редакцией Астайкина А. И. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2014.

4. ГОСТ Р ИСО/МЭК 15408. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

5. ГОСТ Р 58412 2019 Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения.

6. РД-03-34-2000 Требования к составу и содержанию отчета о верификации и обосновании программных средств, применяемых для обоснования безопасности объектов использования атомной энергии.

7. Стандарт ISO/IEC 27001:2013 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.