Экз. №__

УТВЕРЖДАЮ

Генеральный директор

_____

_____ _____

«___»_____2024 г.

Программа и методики оценки соответствия программного обеспечения требованиям по разработке безопасного программного обеспечения в форме самооценки

Москва 2024

Содержание

1. Общие сведения

Настоящий документ (далее – Программа и методики) определяет цель, объект и содержание испытаний программного обеспечения, на соответствие части требований по разработке безопасного программного обеспечения на основе ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Разработчик, изготовитель программного обеспечения: Название и адрес компании разработчика программного обеспечения.

Испытания проводятся в форме самооценки.

Основание для проведения испытаний: Требование Ассоциации «Цифровая энергетика».

2. Объект испытаний

Объект испытаний: Название программного обеспечения.

Версия программного обеспечения - _____.

Краткое описание программного обеспечения _____.

Краткое описание процесса разработки безопасного программного обеспечения, реализованного в интересах разработки исследуемого программного обеспечения _____.

Для проведения испытаний программного обеспечения должен быть представлен один образец программного обеспечения (далее – ПО). Также должны быть представлены: Руководство по безопасной разработке программного обеспечения, свидетельства реализации процесса разработки безопасного программного обеспечения в части определения поверхности атаки и подтверждения наличия процесса выявления и устранения уязвимостей.

3. Цели испытаний

Целями испытаний программного обеспечения является:

– оценка соответствия требованиям пункта 29.3 Приказа ФСТЭК России № 239 от 25 декабря 2017 г. «об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации» в части требований к прикладному программному обеспечению, планируемого к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта и обеспечивающее выполнение его функций по назначению;

– оценка соответствия требованиям документа ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» в части наличия руководства по разработке безопасного программного обеспечения и осуществления процедур статического и динамического анализа;

– оценка соответствия части требований документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) по 6 уровню доверия.

4. Условия проведения испытаний

Испытания программного обеспечения проводятся на материально-технической базе разработчика программного обеспечения, расположенной на территории Российской Федерации.

Испытания проводятся в нормальных климатических условиях эксплуатации СВТ (п. 1.3.2 ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение») в помещениях, удовлетворяющих условиям эксплуатации СВТ, в дневное время, в помещениях, при температуре от +20º С до +25º С. Никаких специальных мер по обеспечению давления и влажности в помещениях, отличных от условий в рабочих помещениях настоящей Программой и методиками не предусматривается.

5. Технические требования

5.1. Требования к тестовой среде

Проведение испытаний ПО должно осуществляться на материально-технической базе разработчика программного обеспечения, расположенной на территории Российской Федерации, используемой разработчиком при разработке ПО на момент проведения испытаний.

5.2. Требования к документации

Документированные материалы программного обеспечения должны соответствовать требованиям документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) по 6 уровню доверия в части касающейся.

Состав документированных материалов программного обеспечения приведен в таблице 5.1.

Таблица 5.1 – Состав документированных материалов программного обеспечения

Наименование	Обозначение	Примечание
Руководство пользователя		
Руководство администратора		
Документ, определяющий поверхность атаки		
Документ, подтверждающий наличие процесса выявления и устранения уязвимостей		
Руководство по разработке безопасного программного обеспечения		

5.3. Требования к персоналу

Для выполнения проверок, предусмотренных методиками испытаний, требуется специалист с опытом эксплуатации и администрирования средств обеспечения разработки безопасного программного обеспечения, знаниями методов проведения статического и динамического анализа, знаниями ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» и Приказа ФСТЭК России № 239 от 25 декабря 2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации».

Все проводимые работы в ходе испытаний выполняются разработчиком программного обеспечения, оценка результатов испытаний осуществляется сотрудниками организации, осуществляющей оценку, имеющими соответствующий уровень квалификации.

6. Программа испытаний

6.1. Общие положения

Испытания программного обеспечения проводятся по настоящей Программе и методике испытаний, утвержденной Ассоциацией «Цифровая энергетика».

При проведении испытаний используются следующие нормативные документы:

– ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

– ГОСТ 28195-89 «Оценка качества программных средств. Общие положения»;

– ГОСТ 28806-90 «Качество программных средств. Термины и определения»;

– ГОСТ Р ИСО/МЭК 9126-93 «Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению»;

– ГОСТ 19.104-78 «Единая система программной документации. Основные надписи»;

– ГОСТ 19.105-78 «Единая система программной документации. Общие требования к программным документам»;

– ГОСТ 19.106-78 «Единая система программной документации. Требования к программным документам, выполненным печатным способом».

– Приказ ФСТЭК России № 239 от 25 декабря 2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации»;

– Приказ ФСТЭК России № 76 от 2 июня 2020 г. «Об утверждении требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»;

– «Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении» (ФСТЭК России, 2020).

Испытания проводятся на материально-технической базе разработчика программного обеспечения, расположенной на территории Российской Федерации.

Условием начала каждой стадии испытаний является готовность оборудования, программного обеспечения и персонала к его проведению.

Все проводимые работы в ходе испытаний выполняются сотрудниками организации, осуществляющей испытания, имеющими соответствующий уровень квалификации.

Меры, обеспечивающие безопасность и безаварийность проведения испытаний, а также техническое оснащение испытательного стенда должны соответствовать

требованиям ГОСТ 21552-84, действующим нормам и правилам обеспечения безопасности работ с вычислительной техникой.

Испытания проводятся в объеме, предусмотренном п. 6.2 настоящей программы по методикам, приведенным в разделе 7.

Допускается проводить проверки по нескольким пунктам Программы и методик одновременно.

Все ситуации, не предусмотренные методиками испытаний, должны фиксироваться в протоколе испытаний с указанием причины возникновения ситуации (недоработка испытываемого образца, принципиальная невозможность достижения требуемого технического решения, ошибка в документации или другие причины).

Испытания считаются выполненными, если успешно реализованы требования и завершены испытания (проверки) по всем пунктам настоящей Программы и методик. Пункты, проверки по которым не проводились или были прекращены по причине ошибок (неготовности) документации или программных средств, считаются невыполненными.

Настоящая Программа и методики может уточняться и изменяться в установленном порядке согласно требованиям Ассоциации «Цифровая энергетика».

Внесение изменений в программное обеспечение в период проведения испытаний (проверок) не допускается.

6.2. Объем и порядок проведения испытаний

Основными технологическими операциями в рамках испытаний программного обеспечения являются:

- идентификация объекта испытаний;
- оценка процесса разработки безопасного программного обеспечения;
- оценка соответствия требованиям по 6 уровню доверия к документации в части касающейся;
- выявление уязвимостей и недекларированных возможностей в части статического и композитного анализа;
- оценка соответствия требованиям к поддержке безопасности ПО;
- анализ и обработка полученных результатов;
- оформление протоколов испытаний и технического заключения.

Идентификация объекта испытаний проводится в целях подтверждения соответствия представленного на испытания ПО образцу ПО, отобранному при отборе образцов. Исходными данными для проведения идентификации объекта испытаний являются: комплект ПО, представленный на испытания, акт отбора образцов.

В ходе идентификации объекта испытаний должно быть проверено соответствие идентификационных признаков элементов ПО, представленного на испытания, идентификационным признакам, отраженным в акте отбора образцов, по результатам чего должен быть сделан вывод о соответствии ПО, представленного на испытания, программному обеспечению, отраженному в акте отбора образцов.

Перечень проверок, проводимых при проведении испытаний, приведен в таблице 6.1.

Таблица 6.1 – Перечень проверок

№ п/п	Наименование требований		Номер пункта методики испытаний
1	Требования к организации процесса разработки безопасного программного обеспечения	Требования к наличию решения руководства о реализации процесса РБПО	7.1.5.1.1
		Требования к наличию человеческих ресурсов на реализацию процесса РБПО	7.1.5.1.2
		Требования к наличию процесса обучения работников требованиям к процессу РБПО	7.1.5.1.3
		Требования к наличию процесса использования систем хранения исходного кода, дистрибутива и сборки программного обеспечения	7.1.5.1.4
		Требования к наличию процесса обеспечения безопасности сборочной среды программного обеспечения, системы хранения исходного кода и реализован процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю	7.1.5.1.5
		Требования к наличию процесса формирования и предъявления требований безопасности к программному обеспечению	7.1.5.1.6
2	Требования к документации	Требования к эксплуатационной документации и документации в части определения поверхности атаки	7.1.5.2.1
		Требования к наличию документальных свидетельств реализации процесса РБПО	7.1.5.2.2
3	Требования к поддержке безопасности ПО	Требования к процессу управления уязвимостями	7.1.5.3.1
		Требования к процессу поддержки программного обеспечения	7.1.5.3.2
4	Требования к декларированию обязательства через год обеспечить выполнение базового уровня соответствия требованиям по РБПО	Требования к декларации обязательства достичь через год базового уровня соответствия требованиям РБПО	7.1.5.4

5	Требования к проведению испытаний по выявлению уязвимостей и недекларированных возможностей	Требования к испытаниям по выявлению уязвимостей и недекларированных возможностей	7.2

Перечень проверок, проводимых в соответствии с требованиями по выявлению уязвимостей и недекларированных возможностей, приведен в таблице 6.2.

Таблица 6.2 – Перечень проверок по выявлению уязвимостей и недекларированных возможностей

№ п/п	Требование методики выявления уязвимостей и недекларированных возможностей	Номер пункта методики испытаний
1	Подготовка к проведению исследований по выявлению уязвимостей и недекларированных возможностей	7.2.5.1.1
2	Подготовка исследовательского стенда	7.2.5.1.2
3	Анализ состава модулей, конфигураций и интерфейсов	7.2.5.2.1
4	Анализ безопасности объекта оценки на основе открытых источников	7.2.5.2.2
5	Статический анализ исходного кода объекта оценки	7.2.5.3
6	Композитный анализ программного обеспечения	7.2.5.4
7	Проверка процесса разработки на предмет внедрения вредоносного кода через цепочки поставок	7.2.5.5
8	Проверка процесса функционального тестирования	7.2.5.6

7. Методики испытаний

7.1. Методика оценки соответствия документации

7.1.1. Объект испытаний

Объект испытаний – программное обеспечение, указанное в разделе 2 настоящего документа.

7.1.2. Цель испытаний

Цель испытаний – самооценка соответствия программного обеспечения:

– требованиям пункта 29.3 Приказа ФСТЭК России № 239 от 25 декабря 2017 г. «об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации» в части требований к прикладному программному обеспечению, планируемого к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта и обеспечивающее выполнение его функций по назначению;

– части требований документа ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» в части наличия руководства по разработке безопасного программного обеспечения и осуществления процедур статического и динамического анализа;

– части требований документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) по 6 уровню доверия.

По результатам самооценки эксперты Ассоциации «Цифровая энергетика» принимают решение о рекомендации применения ПО, успешно прошедшего самооценку, членами ассоциации.

7.1.3. Метод испытаний

При проведении испытаний используется экспертно-документальный метод.

7.1.4. Этапы испытаний

Испытания включают следующие этапы, определенные в таблицах 6.1, 6.2 Программы испытаний.

7.1.5. Порядок проведения испытаний

7.1.5.1. Оценка соответствия требованиям к организации процесса разработки безопасного программного обеспечения требованиям установленных ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

7.1.5.1.1 Требования к наличию решения руководства о реализации процесса РБПО

Исходные данные:

Документация, подтверждающая вовлеченность руководства в процессы создания и развития процессов разработки безопасного ПО.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, предоставленных руководством разработчика, и убедиться, что предоставленная документация содержит подтверждения вовлеченности руководства разработчика в реализацию и развитие процессов разработки безопасного ПО.

В качестве таких свидетельств может выступать:

- приказ\распоряжение о реализации процесса РБПО;
- приказ\распоряжение об утверждении руководства\регламента процесса РБПО;
- протоколы совещаний, задачи, распоряжения, зафиксированные во внутренних системах документооборота, подтверждающие вовлеченность руководства разработчика в реализацию и развитие процессов разработки безопасного ПО.

Проверка прошла успешно, если эксперт получил документированные свидетельства подтверждающие вовлеченность руководства разработчика в реализацию и развитие процессов разработки безопасного ПО.

7.1.5.1.2 Требования к наличию человеческих ресурсов на реализацию процесса РБПО

Исходные данные:

Документация, подтверждающая наличие человеческих ресурсов на реализацию процесса РБПО.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, предоставленных руководством разработчика, и убедиться, что предоставленная документация содержит подтверждения наличия человеческих ресурсов на реализацию процесса РБПО.

В качестве таких свидетельств может выступать:

- приказ\распоряжение о реализации процесса РБПО с указанием ответственных работников из числа штатных работников;
- должностные инструкции с указанием роли работника в процессах РБПО;

– протоколы совещаний, задачи, распоряжения, зафиксированные во внутренних системах документооборота, подтверждающие участие конкретных работников разработчика в процессов разработки безопасного ПО;

– протоколы совещаний, задачи, распоряжения, зафиксированные во внутренних системах документооборота, подтверждающие планирование потребностей в ресурсах, необходимых для реализации процессов разработки безопасного ПО.

Проверка прошла успешно, если эксперт получил документированные свидетельства подтверждающие наличия человеческих ресурсов на реализацию процесса РБПО.

7.1.5.1.3 Требования к наличию процесса обучения работников требованиям к процессу РБПО

Исходные данные:

Документация, подтверждающая наличие процесса обучения работников требованиям к процессу РБПО.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, предоставленных руководством разработчика, и убедиться, что предоставленная документация содержит подтверждения наличия процесса обучения работников требованиям к процессу РБПО.

В качестве таких свидетельств может выступать:

– дипломы, свидетельства работников из числа штатных о прохождении обучения по РБПО;

– наличие рассылок, информации на внутренних ресурсов разработчика по вопросам разработки безопасного программного обеспечения;

– должностные инструкции с указанием роли работника в процессах РБПО;

– протоколы совещаний, задачи, распоряжения, зафиксированные во внутренних системах документооборота, подтверждающие организацию\планирование обучения, включая самообучение;

– иные свидетельства, подтверждающие, что у разработчика организовано обучение или самообучение работников, участвующих в процессах РБПО.

Проверка прошла успешно, если эксперт получил документированные свидетельства подтверждающие наличие процесса обучения работников требованиям к процессу РБПО.

7.1.5.1.4 Требования к наличию процесса использования систем хранения исходного кода, дистрибутива и сборки программного обеспечения

Исходные данные:

Документация, подтверждающая наличие процесса использования систем хранения исходного кода, дистрибутива и сборки программного обеспечения.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, актов приема передачи, лицензионных договоров, актов внедрения, результатов функционирования указанных систем, проектной и эксплуатационной документации на указанные системы и т.д., предоставленных руководством разработчика. Убедиться, что предоставленная документация содержит подтверждения наличия процесса использования систем хранения исходного кода, дистрибутива и сборки программного обеспечения.

В качестве таких свидетельств может выступать:

- приказ\распоряжение о создании систем хранения исходного кода, дистрибутива и сборки программного обеспечения;
- проектная и эксплуатационная документация на системы хранения исходного кода, дистрибутива и сборки программного обеспечения;
- организационно распорядительная документация по использованию системы хранения исходного кода, дистрибутива и сборки программного обеспечения;
- скриншоты использования систем хранения исходного кода, дистрибутива и сборки программного обеспечения;
- скриншоты событий журналов аудита систем хранения исходного кода, дистрибутива и сборки программного обеспечения;
- иные свидетельства, подтверждающие, что разработчик использует собственные системы хранения исходного кода, дистрибутива и сборки программного обеспечения.

Проверка прошла успешно, если эксперт получил документированные свидетельства подтверждающие наличие систем хранения исходного кода, дистрибутива и сборки программного обеспечения.

7.1.5.1.5 Требования к наличию процесса обеспечения безопасности сборочной среды программного обеспечения, системы хранения исходного кода и реализован процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю

Исходные данные:

Документация, подтверждающая наличие процесса обеспечения безопасности сборочной среды программного обеспечения, системы хранения исходного кода и

реализован процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, нормативных актов, организационно распорядительных документов, протоколов совещаний, предоставленных руководством разработчика. Убедиться, что предоставленная документация содержит подтверждения наличия процесса обеспечения безопасности сборочной среды программного обеспечения, системы хранения исходного кода и реализован процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю.

В качестве таких свидетельств может выступать:

– приказ\распоряжение\указание о создании процесса обеспечения безопасности сборочной среды программного обеспечения, системы хранения исходного кода и реализован процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю;

– проектная и эксплуатационная документация на системы обеспечения безопасности сборочной среды программного обеспечения, системы хранения исходного кода и реализован процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю;

– организационно распорядительная документация по обеспечение безопасности сборочной среды программного обеспечения, системы хранения исходного кода и реализован процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю;

– скриншоты использования систем хранения исходного кода, дистрибутива и сборки программного обеспечения;

– скриншоты, подтверждающие реализацию процесса обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю;

– скриншоты событий журналов аудита систем хранения исходного кода, дистрибутива и сборки программного обеспечения, подтверждающие реализацию требований по обеспечению информационной безопасности и реализацию процессов обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю;

– свидетельства реализации хранение результатов сборки ПО в выделенном хранилище кода ПО;

– свидетельства повторяемости сборки ПО (если применимо);

– свидетельства реализации защита внешних каналов связи для обеспечения конфиденциальности информации, обрабатываемой в сборочной среде (если применимо);

– иные свидетельства, подтверждающие, что разработчик реализовал процесс обеспечение безопасности сборочной среды программного обеспечения, системы хранения исходного кода и реализовал процесс обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю;

– свидетельства об обеспечении возможности получения обновления ПО способами, обеспечивающими его целостность.

Проверка прошла успешно, если эксперт получил документированные свидетельства подтверждающие наличие процессов обеспечения безопасности сборочной среды программного обеспечения, системы хранения исходного кода и обеспечения целостности кода при разработке программного обеспечения и передаче дистрибутива пользователю.

7.1.5.1.6 Требования к наличию процесса формирования и предъявления требований безопасности к программному обеспечению

Исходные данные:

Документация, подтверждающая наличие процесса формирования и предъявления требований безопасности к программному обеспечению.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, предоставленных руководством разработчика, и убедиться, что предоставленная документация содержит подтверждения наличия процесса формирования и предъявления требований безопасности к программному обеспечению.

В качестве таких свидетельств может выступать:

– приказ\распоряжение\указание о разработке программного обеспечения со свидетельствами, подтверждающими требования по безопасности;

– техническое задание\технические требования на программное обеспечение со свидетельствами, подтверждающими требования по безопасности;

– проектная и эксплуатационная документация на программного обеспечения со свидетельствами, подтверждающими требования по безопасности;

– протоколы совещаний, задачи, распоряжения, зафиксированные во внутренних системах документооборота, подтверждающие наличие процесса формирования и предъявления требований безопасности к программному обеспечению, а также их периодическому пересмотру.

Проверка прошла успешно, если эксперт получил документированные свидетельства подтверждающие наличие процесса формирования и предъявления требований безопасности к программному обеспечению.

7.1.5.2. Оценка соответствия требованиям к документации

7.1.5.2.1 Оценка соответствия программного обеспечения в части требований к эксплуатационной документации и документации в части определения поверхности атаки

Исходные данные:

Эксплуатационная документация и документация, содержащая информацию, определяющую поверхность атаки программного обеспечения.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку документации программного обеспечения, предоставленной разработчиком, и убедиться, что документация отвечает требованиям документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) в части определения поверхности атаки.

Представленная документация должна содержать:

- руководство пользователя содержащее:
  - описание режимов работы средства;
  - описание принципов безопасной работы средства;
  - описание функций и интерфейсов функций средства, доступных каждой роли пользователей;
  - описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений;
  - описание типов событий безопасности, связанных с доступными пользователю функциями средства;
  - описание действий после сбоев и ошибок эксплуатации средства;
- руководство администратора содержащее:
  - описание действий по приемке поставленного средства;
  - описание действий по безопасной установке и настройке средства;
  - описание действий по реализации функций безопасности среды функционирования средства;

– описание назначения и способов использования каждого интерфейса функций безопасности (при наличии функций безопасности) и иных функций ПО;

– описание параметров, связанных с каждым интерфейсом функций безопасности (при наличии функций безопасности) и иных функций ПО;

– перечень интерфейсов, не влияющих на функции безопасности ПО (при наличии функций безопасности и наличии таких интерфейсов);

– описание действий с каждым интерфейсом функций безопасности, не влияющим на выполнение требований, предъявляемых к ПО;

– описание сообщений обо всех ошибках, которые могут возникнуть при вызове каждого интерфейса функций безопасности;

– описание защиты функций безопасности ПО от несанкционированного доступа к ним;

– обоснование безопасности процесса инициализации ПО;

– определение всех модулей, реализующих функции безопасности;

– определение всех модулей, реализующих взаимодействие с интерфейсами ПО;

– определение способов взаимодействия модулей, осуществляющих выполнение функций безопасности, с иными модулями, обеспечивающими невозможность влияния на выполнение функций безопасности ПО.

– сопоставление функций ПО и интерфейсов;

– описание взаимодействия подсистем ПО между собой;

– описание структуры ПО на уровне модулей;

– описание всех модулей ПО (для модулей средства, реализующих функции безопасности, - описание интерфейсов, возвращаемых ими в ответ на запросы значений, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей; для модулей средства, не влияющих на выполнение функций безопасности, - описание назначения и взаимодействия с другими модулями);

– исходные тексты программного обеспечения, входящего в состав ПО, с указанием значений контрольных сумм файлов с исходными текстами программного обеспечения

– средств, применяемых для разработки ПО;

– определение модулей входящих в поверхность атаки.

Проверка прошла успешно, если эксплуатационная документация и документация содержащая информацию, определяющую поверхность атаки программного обеспечения, имеются в наличии и соответствует предъявленным требованиям.

7.1.5.2.2 Оценка соответствия программного обеспечения в части требований к наличию документальных свидетельств реализации процесса РБПО

Исходные данные оценки:

Руководство\регламент\порядок (любой в наличии документ) по разработке безопасного ПО.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку документации по разработке безопасного программного обеспечения, предоставленной разработчиком, и убедиться, что документация отвечает требованиям документа ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Представленный документ по разработке безопасного ПО должно включать:

– описание области действия руководства (идентификационные признаки ПО, для которого реализуют меры по разработке безопасного ПО);

– цели организации в области создания безопасного ПО;

– перечень и описание мер по разработке безопасного ПО, подлежащих реализации в среде разработки ПО;

– распределение ролей и обязанностей, связанных с реализацией мер по разработке безопасного ПО, между работниками;

– перечень документации разработчика ПО, связанной с реализацией мер по разработке безопасного ПО;

– правила и требования, относящиеся к планированию и проведению внутренних проверок реализации мер по разработке безопасного ПО, сообщений о результатах;

– описание действий, направленных на улучшение процессов, связанных с разработкой безопасного ПО.

При реализации компенсирующих мер по разработке безопасного ПО в руководстве по разработке безопасного ПО должно быть приведено обоснование применения компенсирующих мер, включающее:

– изложение причин исключения меры (мер) по разработке безопасного ПО, определенных ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного ПО. Общие требования»;

– описание содержания компенсирующих мер по разработке безопасного ПО;

– сравнительный анализ компенсирующих мер по разработке безопасного ПО с мерами, исключаемыми из состава базового набора мер по разработке безопасного ПО;

– аргументацию подтверждающую, что предлагаемые компенсирующие меры разработки безопасного ПО обеспечивают достижение целей, соответствующих исключаемым мерам по разработке безопасного ПО.

Проверка прошла успешно, если Руководство по разработке безопасного программного обеспечения соответствует предъявленным требованиям.

7.1.5.3. Оценка соответствия требованиям к поддержке безопасности ПО

7.1.5.3.1 Оценка соответствия программного обеспечения в части требований к процессу управления уязвимостями

Исходные данные:

Эксплуатационная документация на программное обеспечение и организационно распорядительная документация.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, по созданию процесса управления рисками, а также результатов функционирования данного процесса, предоставленных руководством разработчика. Убедиться, что предоставленная документация, сведения содержат подтверждения наличия процесса управления рисками. Убедиться, что процесс реально функционирует, есть ресурсы для приема обращений об уязвимостях, назначены ответственные за обработку поступающих уязвимостей, за поиск уязвимостей, а также устранение обнаруженных уязвимостей. По возможности самостоятельно разместить заявку об уязвимости и проследить путь и результат ее исполнения.

Представленная документация и свидетельства должны содержать:

– документ, регламентирующий процесс управления уязвимостями;

– приказ\распоряжение о реализации процесса управления уязвимостями;

– приказ\распоряжение о назначении ответственных за процесс управления уязвимостями;

– протоколы совещаний, задачи, распоряжения, зафиксированные во внутренних системах документооборота, подтверждающие наличие процесса управления уязвимостями;

– наличие ресурсов, предназначенных для приема обращений об уязвимостях;

– свидетельства (при наличии) результатов приема и обработки поступающих запросов от пользователей с последующим анализом ошибок функционирования на предмет наличия уязвимостей;

– свидетельства (при наличии) результатов поиска уязвимостей в ПО на протяжении всего срока действия технической поддержки на него.

– свидетельства (при наличии) результатов устранения выявленных уязвимостей;

– информацию о процессе поиска информации о недостатках программного обеспечения в открытых источниках;

– сведения о процессе получение сведений о недостатках программного обеспечения от потребителя;

– сведения о проведении испытаний по выявлению уязвимостей и недекларированных возможностей программного обеспечения;

– сведения о порядке разработки ограничений по применению программного обеспечения, снижающих возможности эксплуатации уязвимостей;

– сведения о порядке доведения информации об уязвимостях, а также об ограничениях по применению программного обеспечения до потребителей;

– сведения об информировании потребителей программного обеспечения о выпуске обновлений.

Проверка прошла успешно, если представленная документация и свидетельства наличия процесса управления рисками соответствует предъявленным требованиям.

7.1.5.3.2 Оценка соответствия программного обеспечения в части требований к процессу поддержки программного обеспечения

Исходные данные:

Эксплуатационная документация на программное обеспечение и организационно распорядительная документация.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, по созданию процесса поддержки программного обеспечения а также результатов функционирования данного процесса, предоставленных руководством разработчика. Проверить наличия в договоре на поставку сведений о технической поддержке и условий ее оказания. Убедиться, что предоставленная документация, сведения содержат подтверждения наличия процесса поддержки программного обеспечения. Убедиться, что процесс реально функционирует, есть ресурсы для приема обращений пользователей в рамках технической поддержки, назначены ответственные за обработку поступающих обращений. По возможности самостоятельно разместить заявку на техническую поддержку и проследить путь и результат ее исполнения.

В ходе проведения самооценки должно быть проверено, что разработчик программного обеспечения документировал процесс оказания технической поддержки,

обеспечил его необходимыми ресурсами и осуществляет контроль за его функционированием. Представленная документация должны содержать:

– свидетельства наличия в договорах с пользователями раздела о технической поддержке;

– свидетельства документирования процесса оказания технической поддержки (включая условия оказания);

– свидетельства наличия и работы служба технической поддержки;

– свидетельства реализации оповещения пользователей о выпуске обновлений;

– свидетельства реализации процедур информирования пользователей ПО о выявленных уязвимостях\дефектах и способах реализации мер по их нейтрализации до разработки обновлений безопасности, устраняющих уязвимость;

– свидетельства размещения запроса не техническую поддержку и факта его отработки в соответствии с условиями оказания технической поддержки.

Проверка прошла успешно, если ПО обеспечивается технической поддержкой, которая определена в договорах и соответствует предъявленным требованиям.

7.1.6. **Анализ и оценка результатов**

Обработка результатов испытаний сводится к оценке соответствия программного обеспечения установленным требованиям в части касающейся, результаты оценки соответствия заносятся в таблицу 7.1.

Таблица 7.1 – Результаты анализа и оценки результатов

Наименование требований к ПО	**Оценка соответствия**
1	**2**

В таблице 7.1 в графе 1 перечисляются требования данной методики, графе 2 отмечается соответствие или несоответствие оцениваемых показателей.

7.1.7. **Отчетность**

По результатам проведенных по настоящей методике испытаний составляется протокол, в котором указываются результаты оценки соответствия документации.

7.2. Методика выявления уязвимостей и недекларированных возможностей ПО

7.2.1. **Объект испытаний**

Объект испытаний – программное обеспечение, указанное в разделе 2 настоящего документа.

7.2.2. **Цель испытаний**

Объект испытаний – выявление уязвимостей и недекларированных возможностей в программном обеспечении по результатам анализа уязвимостей, статического анализа, композитного анализа, функционального тестирования и проверки процесса разработки на предмет внедрения вредоносного кода через цепочки поставок.

7.2.3. **Методы испытаний**

При проведении испытаний используется следующие методы:

– экспертно-документальный;

– инструментально-экспертный.

7.2.4. **Этапы испытаний**

Выявление уязвимостей и недекларированных возможностей программного обеспечения выполняется в соответствии с методическим документом «Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении» (ФСТЭК России, 2020) – в части касающейся и включает следующие этапы:

– подготовка к проведению исследований по выявлению уязвимостей и недекларированных возможностей;

– анализ уязвимостей;

– статический анализ исходного кода программного обеспечения;

– композитный анализ программного обеспечения;

– проверка процесса разработки на предмет внедрения вредоносного кода через цепочки поставок;

– функциональное тестирование.

7.2.5. **Порядок проведения испытаний**

7.2.5.1. Подготовка к проведению исследований по выявлению уязвимостей и недекларированных возможностей

7.2.5.1.1 Подготовка к проведению исследований по выявлению уязвимостей и недекларированных возможностей

Действия, проводимые в ходе испытаний:

должен быть проведен анализ документации и иных исходных данных, по результатам которого экспертом организации, осуществляющей самооценку, определяется представление о ПО, его интерфейсах, поверхности атаки на ПО.

Исходные данные: документация на ПО и иные сведения, предоставленные разработчиком.

В результате анализа должны быть получены следующие сведения:

– структура ПО на уровне программ (файлов), модулей и интерфейсов;

– условиях и режимах функционирования ПО, параметрах и способах запуска;

– функциональных возможностях ПО, в том числе реализованных функциях безопасности.

Должен быть проведен анализ поверхности атаки ПО, предусматривающий определение и включение в состав поверхности атаки внешних интерфейсов ПО, непосредственно доступных для атаки потенциальным нарушителям. Должен быть составлен перечень программных модулей, реализующих эти интерфейсы. Полученная информация сравнена с выводами, сделанными разработчиком по поверхности атаки.

Должен быть составлен перечень модулей ПО, реализующих функции безопасности, и показана их связь с интерфейсами функций безопасности ПО. Указанные сведения должны содержаться в представленной разработчиком документации.

Проверка прошла успешно, если получено представление о структуре ПО на уровне программ (файлов), модулей и интерфейсов, условиях и режимах функционирования программного обеспечения, параметрах и способах запуска программного обеспечения, функциональных возможностях программного обеспечения, проведен анализ поверхности атаки программного обеспечения.

7.2.5.1.2 Подготовка исследовательского стенда

Требования к исследованиям: в ходе подготовки к проведению исследований должен быть создан исследовательский стенд, обеспечивающий всестороннее и качественное проведение испытаний в соответствии с разработанной методикой испытаний и представлением об ПО. Исследовательский стенд создается на материально-технической базе разработчика программного обеспечения, расположенной на территории Российской Федерации, используемой разработчиком при разработке ПО на момент проведения испытаний.

Исходные данные: сведения, полученные по результатам анализа документации ПО и других исходных данных, содержащих сведения об ПО, дистрибутив программного обеспечения.

Действия, проводимые в ходе испытаний:

В ходе подготовки исследовательского стенда должны быть выполнены:

– контрольная сборка программного обеспечения;

– настройка сред функционирования ПО;

– идентификация ПО путем расчета контрольных сумм дистрибутива и исполняемых файлов программного обеспечения;

– установка и настройка программного обеспечения;

– антивирусный контроль программного обеспечения и среды его функционирования.

При контрольной сборке программного обеспечения необходимо зафиксировать контрольные суммы исходных текстов и полученного дистрибутива.

При подготовке исследовательского стенда должны быть развернуты и настроены требуемые среды функционирования, в которых будет эксплуатироваться программное обеспечение, а также необходимые для проведения исследований инструментальные средства.

Перед установкой программного обеспечения необходимо выполнить расчет контрольных сумм дистрибутивного носителя программного обеспечения и проверить, что значение совпадает со значениями ранее проведенной сборки. После установки необходимо выполнить расчет контрольных сумм неизменяемых файлов программного обеспечения и проверить, что их значения совпадают со значениями, приведенными в документации программного обеспечения.

Установка, настройка и конфигурирование программного обеспечения должны осуществляться в соответствии с эксплуатационной документацией на ПО. В ходе установки дистрибутива программного обеспечения должны регистрироваться все события, связанные с его взаимодействием с внешними сетевыми ресурсами, и устанавливаться цели такого взаимодействия. Регистрация событий осуществляется средством мониторинга сетевого трафика ПО Wireshark. В исследовательском стенде должны быть реализованы меры защиты, направленные на обеспечение целостности ПО и среды функционирования, а также исключение возможности несанкционированного доступа к результатам проведения исследований.

После установки, настройки, конфигурирования ПО должен быть проведен антивирусный контроль программного обеспечения, предусматривающий анализ дистрибутивного носителя и развернутого ПО с использованием специализированного программного обеспечения с актуальными на момент проведения контроля базами данных признаков вредоносных компьютерных программ.

В отношении каждой выявленной в ходе подготовки исследовательского стенда потенциально опасной функциональной возможности ПО должен быть проведен анализ возможности возникновения угроз безопасности. В случае если в результате такого анализа выявлена потенциальная возможность нарушения безопасности ПО, потенциально опасная возможность должна быть исключена разработчиком или приняты другие меры, исключающие возможность ее использования для реализации угроз безопасности.

Проверка прошла успешно, если

– программное обеспечение успешно идентифицировано;

– подготовлен и настроен исследовательский стенд;

– по результатам антивирусного контроля и контроля сетевых взаимодействий в ходе установки и настройки ПО подтверждено отсутствие вредоносного программного обеспечения в составе программного обеспечения и отсутствие недекларированного сетевого взаимодействия.

7.2.5.2. Анализ уязвимостей

7.2.5.2.1 Анализ состава модулей, конфигураций и интерфейсов ПО

Требования к исследованиям: должен быть проведен анализ документации ПО с целью выявления в нем потенциально опасных функциональных возможностей, архитектурных уязвимостей и уязвимостей конфигурации.

Исходные данные: дистрибутив программного обеспечения, документация на программного обеспечения, иные сведения о программного обеспечения, в том числе, полученные из открытых источников информации.

Действия, проводимые в ходе испытаний:

В ходе испытаний:

– должен быть проведен анализ исходного кода ПО в части комментариев разработчика к исходному коду, направленный на выявление потенциально опасных функциональных возможностей;

– должен быть проведен анализ исходного кода ПО, направленный на выявление в исходных кодах открыто присутствующей чувствительной информации и «секретов»;

– должен быть проведен анализ документация на программного обеспечения с целью выявления: потенциально опасных функциональных возможностей, архитектурных уязвимостей ПО.

Для анализа исходного кода ПО в части комментариев разработчика к исходному коду и чувствительной информации необходимо использовать специализированное ПО. Специализированное ПО производит обход исходного кода, сохраняя комментарии разработчика в специально созданный файл. Если в ходе работы скрипта будет найдена чувствительная информация, скрипт сохранит фрагмент кода в специально созданном файле. После завершения работы скрипта экспертным методом изучить полученные файлы с комментариями к исходным текстам и числительной информации на предмет наличия потенциально опасных функциональных возможностей.

Необходимо выполнить автоматизированный анализ сетевых интерфейсов с использованием средства анализа защищенности с целью выявления известных типовых уязвимостей и ошибок конфигурирования ПО, а также компонентов в составе ПО, имеющих известные уязвимости.

Должен быть выполнен анализ настроек ПО, направленный на выявление уязвимостей конфигурации ПО.

Выявленные в ходе исследований подтвержденные актуальные уязвимости предоставляются разработчику ПО для устранения. Меры по устранению уязвимостей, разработанные разработчиком, подлежат исследованию на предмет корректности исправления уязвимостей, а также с целью контроля отсутствия новых уязвимостей.

Проверка считается успешно пройденной, если по результатам исследований и разработки мер подтвержденные актуальные уязвимости ПО в средах его функционирования отсутствуют.

7.2.5.2.2 Анализ безопасности программного обеспечения на основе открытых источников

Требования к исследованиям: должна быть проведена идентификация уязвимостей ПО по открытым источникам информации, предусматривающая выявление актуальных известных уязвимостей в ПО, а также потенциальных уязвимостей ПО с последующим тестированием их на проникновение. Должен быть выполнен анализ сборочной среды с целью выявления компонентов и их конфигурационных параметров, оказывающих негативное влияние на безопасность ПО вследствие наличия известных уязвимостей и НДВ в компонентах сборочной среды.

Исходные данные: дистрибутив программного обеспечения, документация на программного обеспечения, сведения об уязвимостях программного обеспечения, его компонентов и сред функционирования, сред сборки, полученные от разработчика и из открытых источников информации.

Действия, проводимые в ходе испытаний:

Для выявления не устраненных известных уязвимостей в объекте оценки необходимо осуществить поиск сведений об уязвимостях программного обеспечения и среды его функционирования в общедоступных источниках по названию ПО, его компонентов, сред функционирования и сред сборки:

- Банк данных угроз безопасности информации (https://bdu.fstec.ru/ubi/vul);
- The Open Source Vulnerabilities Database (OSVDB) (https://www.osvdb.org/);
- Common Vulnerabilities and Exposures (CVE) (https://cve.mitre.org/);
- National Vulnerability Database (https://nvd.nist.gov/);
- Secunia (https://secunia.com/advisories/);
- SecurityFocus (https://www.securityfocus.com/bid/);
- SecurityTracker (https://www.securitytracker.com/);
- CVE Details (https://www.cvedetails.com/);

– сайт разработчика;

– результаты автоматизированного сканирования.

Для идентификации потенциальных уязвимостей необходимо выполнить следующие действия:

– осуществить поиск уязвимостей программного обеспечения с использованием средства анализа защищенности:

– при обнаружении в отчетах сведений о возможных уязвимостях программного обеспечения, включить их в перечень потенциальных уязвимостей;

– осуществить поиск известных (подтвержденных) уязвимостей в общедоступных источниках для версий ПО, отличных от исследуемых, и для ПО, однотипных с исследуемым;

– при обнаружении уязвимостей, включить их в перечень потенциальных уязвимостей;

– проанализировать перечень потенциальных уязвимостей ПО, составленный при выполнении действий по предыдущим пунктам;

– исключить из рассмотрения (из сформированного перечня потенциальных уязвимостей) потенциальные уязвимости, которые не могут быть использованы при выполнении мер защиты информации, используемых в среде функционирования ПО, с приведением обоснования;

– в случае отсутствия в документации на программного обеспечения указаний по установке обновлений для среды, заявителю направляется сообщение о проблеме, если заявитель не устраняет данную проблему, то может быть выдано отрицательное заключение;

– после формирования перечня потенциальных уязвимостей выполнить теоретический расчет потенциала нападения, требуемого для эксплуатации каждой потенциальной уязвимости.

Результат идентификации потенциальных уязвимостей – перечень потенциальных уязвимостей, которые являются предметом тестирования на проникновение и применимы к объекту оценки.

Для каждой идентифицированной потенциальной уязвимости должны быть определены

– источник сведений об уязвимости;

– возможность использования потенциальной уязвимости в конкретной среде или средах функционирования;

– функции безопасности, которые могут быть нарушены в результаты использования потенциальной уязвимости;

– шаблон или вектор атаки (нескольких атак), которые могут быть реализованы в отношении объекта оцени с использований потенциальной уязвимости;

– количество времени, уровень компетенции, уровень знания объекта оценки, уровень доступа к объекту оценки, оборудование, необходимое для использования идентифицированных уязвимостей.

В отношении идентифицированных потенциальных уязвимостей должно быть проведено тестирование на проникновение. Для проведения данного исследования необходимо выполнить следующие действия:

– разработать тесты проникновения относительно всех идентифицированных потенциальных уязвимостей;

– для каждой идентифицированной потенциальной уязвимости разработать способы тестирования, учитывающие интерфейсы программного обеспечения, используемые для выполнения функций безопасности, исходные данные и условия, которые необходимы для тестирования, средства тестирования, необходимые для инициирования интерфейсов; описание теста для каждой потенциальной уязвимости из перечня должно включать:

- идентификацию тестируемой потенциальной уязвимости;
- инструкции по подключению и настройке тестового оборудования, которая требуется для проведения конкретного теста проникновения;
- инструкции по установке всех предварительных начальных условий выполнения теста проникновения;
- описание ожидаемых результатов;
- инструкции по завершению теста и установке необходимого пост-тестового состояния программного обеспечения;

– провести тестирование на проникновение с использованием разработанных тестов;

– проанализировать результаты тестирования проникновения;

– после устранения заявителем (разработчиком) проблемы (уязвимости) проверить меры, принятые заявителем по устранению уязвимостей (при необходимости провести повторное тестирование);

– если меры, принятые заявителем (включая организационно-технические меры), устраняют уязвимости, то делается вывод об отсутствии актуальных уязвимостей

программного обеспечения, которые может использовать нарушитель с базовым потенциалом нападения;

– в случае отсутствия применения мер заявителем по устранению идентифицированных уязвимостей, то может быть выдано отрицательное заключение.

Проверка считается успешно выполненной, если

– по результатам анализа не найдены сведения об известных, но не устраненных уязвимостях программного обеспечения, его компонентов, сред функционирования;

– сформирован перечень потенциальных уязвимостей для ПО и его компонентов, ПО в средах функционирования;

– по результатам тестирования на проникновение подтверждено отсутствие возможности эксплуатации (использования) идентифицированных потенциальных уязвимостей в программном обеспечении нарушителем, обладающим базовым потенциалом нападения.

7.2.5.3. Статический анализ исходного кода

Требования к исследованиям: Должен быть выполнен статический анализ исходного кода ПО, направленный на выявление потенциальных уязвимостей кода и НДВ в исходном коде ПО. Проведено исследование процесса статического анализа.

Проводится в отношении модулей ПО, входящих в поверхность атаки.

Исходные данные: Исходные тексты программного обеспечения, сборочная среда.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен провести синтаксический анализ исходного кода объекта оценки, предусматривающий автоматическое сопоставление линейной последовательности лексем, в которую преобразуется исходный код с неким формальным набором правил (сигнатур). Для выполнения данной процедуры необходимо использовать специализированные анализаторы исходных текстов. Статический анализ проводится в отношении модулей, составляющих поверхность атаки, реализующих функции безопасности, реализующих среду выполнения интерпретируемого кода или кода, компилируемого в промежуточное представление.

В отношении полученных по результатам синтаксического анализа программных ошибок объекта оценки должна быть проведена ручная разметка результатов анализа для всех выявленных программных ошибок с целью исключения ложных предупреждений.

Каждая квалифицированная как истинная ошибка должна быть передана разработчику для исправления. После устранения ошибки должны быть проведены

исследования, подтверждающие корректность её исправления и отсутствие новых ошибок, которые могли быть внесены в объект оценки в результате устранения.

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, по созданию процесса статического анализа программного обеспечения а также результатов функционирования данного процесса, предоставленных руководством разработчика. Убедиться, что процесс реально функционирует, есть ресурсы для его реализации. Представленная документация должны содержать:

– документальные свидетельства реализации процесса статического анализа исходного кода ПО (порядок, регламент, инструкцию);

– перечень инструментов статического анализа для каждого используемого в ПО языка программирования;

– конфигурации и параметры настройки инструментов статического анализа;

– подтверждения что статический анализ проводится в соответствии с установленными требованиями, все срабатывания инструментов статического анализа регистрируются, для установленных типов и уровней критичности ошибок выполняется разметка;

Проверка прошла успешно, если на момент проведения испытаний уязвимостей в коде не обнаружено и процесс статического анализа реализован.

7.2.5.4. Композитный анализ программного обеспечения

Требования к исследованиям: Должен быть выполнен композитный анализ исходного кода ПО, направленный на выявление потенциальных уязвимостей кода и НДВ в исходном коде ПО используемых зависимостей и компонент. Проведено исследование процесса композитного анализа.

Проводится в отношении зависимостей и компонент необходимых для сборки и работы ПО.

Исходные данные: Все компоненты и зависимости, необходимые для обеспечения сборки и функционирования ПО, сборочная среда.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен провести композитный анализ исходного кода объекта оценки, предусматривающий автоматический анализ всех зависимых компонент на предмет выявления в них уязвимостей. Для выполнения данной процедуры необходимо использовать специализированные анализаторы исходных текстов.

В отношении полученных по результатам анализа уязвимостей оценки должна быть проведена оценка применимости и реализуемости уязвимости. По результатам анализа необходимо провести устранение актуальных уязвимостей. После устранения уязвимостей должны быть проведены исследования, подтверждающие корректность её исправления и отсутствие новых уязвимостей, которые могли быть внесены в объект оценки в результате устранения.

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, по созданию процесса композитного анализа программного обеспечения а также результатов функционирования данного процесса, предоставленных руководством разработчика. Убедиться, что процесс реально функционирует, есть ресурсы для его реализации. Представленная документация должны содержать сведения:

– документальные свидетельства реализации процесса композитного анализа исходного кода ПО (порядок, регламент, инструкцию);

– перечень инструментов композитного анализа;

– конфигурации и параметры настройки инструментов композитного анализа;

– перечень зависимостей ПО;

– подтверждающие актуальности перечня зависимостей ПО;

– подтверждающие наличия процесса анализ заимствованных компонентов на предмет наличия известных уязвимостей при сборке (непосредственно перед сборкой) ПО (компонентов, модулей ПО);

– подтверждающие наличия процесса разработки корректирующих воздействий по результатам анализа уязвимостей в зависимостях ПО.

Проверка считается успешно выполненной, если по результатам на момент проведения испытаний уязвимостей в заимствованном коде не обнаружено и процесс композитного анализа реализован.

7.2.5.5. Проверка процесса разработки на предмет внедрения вредоносного кода через цепочки поставок

Требования к исследованиям: Должен быть выполнен анализ процесса разработки на предмет внедрения вредоносного кода через цепочки поставок, направленный на выявление потенциальных воздействий на ПО или механизмы его доставки до получения ПО конечными пользователями и недопущение компрометации данных (информации) или информационной системы, использующей такое ПО.

Проводится в отношении всех зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков; компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков).

Исходные данные: Процесс разработки, документация на инфраструктуру обеспечения разработки ПО.

Действия, проводимые в ходе испытаний:

7.2.5.6. Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, по организации процесса выявления фактов внедрения вредоносного кода через цепочки поставок, а также результатов функционирования данного процесса, предоставленных руководством разработчика. Убедиться, что процесс реально функционирует, есть ресурсы для его реализации. Представленная документация должны содержать сведения:

– документальные свидетельства реализации процесса выявления фактов внедрения вредоносного кода через цепочки поставок (порядок, регламент, инструкцию);

– о реализации контроля зависящих от сторонних поставщиков элементов разработки (при наличии);

– о реализации контроля контроль договорных обязательств со сторонними поставщиками (при наличии);

– о выявление элементов инфраструктуры разработчика, воздействие на которые может повлиять на возникновение недекларированных возможностей в ПО.

Проверка считается успешно выполненной, если по результатам испытаний уязвимостей процесс внедрения вредоносного кода через цепочки поставок реализован.

7.2.5.7. Проверка процесса функционального тестирования

Требования к исследованиям: Должно быть выполнено функциональное тестирование ПО. Проведено исследование процесса функционального тестирования. Проводится на стенде, где проводился анализ уязвимостей, после успешного прохождения анализа уязвимостей.

Исходные данные: дистрибутив программного обеспечения, документация на программного обеспечения, испытательный стенд.

Действия, проводимые в ходе испытаний:

Эксперт организации, осуществляющей самооценку, должен провести функциональное тестирование программного обеспечения, предусмотренное программой методикой приемочных испытаний.

Эксперт организации, осуществляющей самооценку, должен выполнить проверку приказов, распоряжений и указаний, по организации процесса приемочных испытаний программного обеспечения а также результатов функционирования данного процесса, предоставленных руководством разработчика. Убедиться, что процесс реально функционирует, есть ресурсы для его реализации. В процессе приемочных испытаний проводится функциональное тестирование. Представленная документация должны содержать:

– документальные свидетельства реализации процесса функционального тестирования ПО (порядок, регламент, инструкцию);

– программу и методику приемочных испытаний (функционального тестирования);

– свидетельства проведения функционального тестирования;

– отчеты по результатам функционального тестирования, позволяющие идентифицировать выполненные функциональные тесты ПО на уровне модулей, компонентов, подсистем, всего ПО в целом;

– журналы регистрации хода проведения функционального тестирования;

– результаты исправления выявленных в ходе тестирования ошибок.

Проверка прошла успешно, если на момент проведения испытаний функциональные тесты прошли успешно и процесс функционального тестирования реализован.

7.2.6. **Анализ и оценка результатов**

Обработка результатов испытаний сводится к оценке идентифицированных уязвимостей для программного обеспечения.

Оценка идентифицированных уязвимостей для программного обеспечения сводится в таблицу 7.2.

Таблица 7.2 – Результаты анализа и оценки результатов (анализ уязвимостей)

Требование методики выявления уязвимостей и недекларированных возможностей	**Оценка соответствия**
1	**2**

В таблице 7.2 в графе 1 перечисляются требования данной методики, в графе 2 отмечается результат оценки соответствующего компонента (по показателям: «соответствует – испытания проведены, актуальные уязвимости и недекларированные возможности отсутствуют», «не соответствует – испытания не проведены в полном объеме и (или) присутствуют актуальные уязвимости критического уровня и (или) недекларированные возможности, не устраненные разработчиком»).

Составляется предварительное заключение о продолжении или о прекращении испытаний в зависимости от степени критичности полученных результатов испытаний.

7.2.7. **Отчетность**

По результатам проведенных по настоящей методике самооценке предоставляются отчеты по анализу уязвимостей и составляется протокол, в котором указываются результаты анализа уязвимостей, перечень проанализированных источников информации, перечень идентифицированных потенциальных уязвимостей, описание тестов и методик тестирования проникновения, результатов тестирования.

8. Отчетность

8.1. Отчёт о проведенных испытаниях оформляется в виде Протоколов испытаний и Технического заключения по результатам испытаний.

8.2. Ответственным за оформление протоколов испытаний и технического заключения является назначенный руководителем организации, осуществляющей самооценку, эксперт.

8.3. Протоколы испытаний и Техническое заключение направляются организацией, осуществляющей самооценку, в Ассоциацию «Цифровая энергетика».

8.4. Порядок, место и сроки хранения первичных материалов испытаний определяются соответствующими нормативными документами, действующими в организации, осуществляющей самооценку.