Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)

В. В. Селифанов, П. А. Звягинцева

НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ОЦЕНКА СООТВЕТСТВИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Утверждено редакционно-издательским советом университета
в качестве учебного пособия для обучающихся по направлению подготовки
10.03.01 Информационная безопасность (уровень бакалавриата)

Новосибирск
СГУГиТ
2024

УДК 004.056
С291

Рецензенты: кандидат юридических наук, доцент СибГУТИ
Е. А. Овчинникова
Ph. D., кандидат химических наук, доцент СГУГиТ
А. В. Троеглазова

Селифанов, В. В.
С291 Нормативные акты и стандарты по информационной безопасности. Оценка соответствия средств защиты информации : учебное пособие / В. В. Селифанов, П. А. Звягинцева. – Новосибирск : СГУГиТ, 2024. – 46 с. – Текст : непосредственный.
ISBN 978-5-907711-70-9

Учебное пособие подготовлено доцентами В. В. Селифановым, П. А. Звягинцевой на кафедре информационной безопасности СГУГиТ.

Данное учебное пособие представляет собой основной исчерпывающий источник информации о проведении оценки соответствия средств защиты информации. В его содержании представлены тщательно структурированные разделы, которые пошагово вводят читателя в процесс оценки, объясняют основные концепции и принципы, а также предоставляют необходимые инструменты и методики для успешной реализации этой процедуры.

Учебное пособие по дисциплине «Нормативные акты и стандарты по информационной безопасности» предназначено для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).

Рекомендовано к изданию кафедрой информационной безопасности, Ученым советом Института оптики и технологий информационной безопасности СГУГиТ.

Печатается по решению редакционно-издательского совета СГУГиТ

УДК 004.056

ISBN 978-5-907711-70-9

ОГЛАВЛЕНИЕ

Введение 4
1. Существующие требования к оценке соответствия 6
1.1. Понятие оценки соответствия и его формы в законе «О техническом регулировании» 6
1.2. Сертификация средств защиты информации 6
1.3. Система сертификации ФСБ России 8
1.4. Система сертификации ФСТЭК России 8
1.5. Виды, типы и классы средств защиты информации 10
2. Функциональные требования к СЗИ 19
2.1. Функционал средств защиты информации 19
2.2. Требования доверия к СЗИ 24
3. Поиск уязвимостей и недекларированных возможностей 28
3.1. Недекларированные возможности 28
3.2. Общие требования к проведению исследований по выявлению уязвимостей и недекларированных возможностей 30
3.3. Подготовка к проведению исследований по выявлению уязвимостей и недекларированных возможностей 31
3.4. Проведение исследований по выявлению уязвимостей и недекларированных возможностей 33
Заключение 43
Библиографический список 44

ВВЕДЕНИЕ

В данном пособии рассмотрим важные аспекты информационной безопасности – нормативные акты и стандарты, – а также оценку соответствия средств защиты информации.

Нормативные акты и стандарты по информационной безопасности являются основой для разработки и применения мер по защите информации. Они определяют требования к обеспечению безопасности информационных систем, сетей и данных. Такие акты и стандарты разрабатываются и утверждаются соответствующими органами, включая правительственные органы и международные организации.

Одним из ключевых нормативных актов в области информационной безопасности является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». Он определяет основные принципы и положения обеспечения безопасности информации в различных сферах деятельности. Кроме того, существуют и другие законы и постановления, регулирующие вопросы информационной безопасности в определенных областях, таких как финансовый сектор или государственные органы.

Более подробные требования и рекомендации по обеспечению информационной безопасности содержатся в стандартах. Один из наиболее известных и широко применяемых стандартов в этой области – это стандарт ISO/IEC 27001. Он определяет систему управления информационной безопасностью и обеспечивает базовый набор требований, которые должны быть реализованы в организации для обеспечения безопасности информации.

Оценка соответствия средств защиты информации является важной частью процесса обеспечения безопасности информации. Она включает в себя тщательное исследование и проверку средств защиты, таких как программное обеспечение, аппаратные средства и механизмы контроля доступа. При оценке соответствия учитываются требования, установленные

нормативными актами и стандартами, а также особенности конкретной организации.

В завершение следует отметить, что соблюдение нормативных актов и стандартов по информационной безопасности, а также проведение оценки соответствия средств защиты информации являются неотъемлемой частью эффективной и надежной защиты информации. Эти меры позволяют организациям минимизировать риски и предотвращать возможные угрозы, связанные с нарушением безопасности информации. Все это способствует успешной деятельности организаций в современном информационном обществе.

1. СУЩЕСТВУЮЩИЕ ТРЕБОВАНИЯ К ОЦЕНКЕ СООТВЕТСТВИЯ

1.1. Понятие оценки соответствия и его формы в законе «О техническом регулировании»

В соответствии с Федеральным законом «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ (далее – 184-ФЗ) в Российской Федерации понятие оценки соответствия означает прямое или косвенное определение соблюдения требований, предъявляемых к объекту, а также процедуру подтверждения соответствия объекта, то есть документальное удостоверение соответствия продукции, выполнения работ или оказания услуг требованиям технических регламентов, документам по стандартизации или условиям договоров [1].

Формы оценки соответствия в рамках 184-ФЗ могут включать в себя:

– добровольное подтверждение соответствия, которое осуществляется по инициативе заявителя на условиях договора между заявителем и органом по сертификации. Добровольное подтверждение соответствия может осуществляться для установления соответствия документам по стандартизации, системам добровольной сертификации, условиям договоров;

– декларирование соответствия – процедуру, при которой изготовитель или поставщик самостоятельно заявляет о соответствии своей продукции установленным требованиям путем оформления декларации соответствия;

– обязательную сертификацию, которая осуществляется органом по сертификации на основании договора с заявителем. Схемы сертификации, применяемые для сертификации определенных видов продукции, устанавливаются соответствующим техническим регламентом. Круг заявителей устанавливается соответствующим техническим регламентом.

Эти формы оценки соответствия помогают обеспечить надежность и эффективность средств защиты информации, что является важным аспектом в современном цифровом мире, где конфиденциальность и целостность информации играют ключевую роль.

1.2. Сертификация средств защиты информации

Сертификация средств защиты информации – это процедура, целью которой является подтверждение соответствия различных программных

и аппаратных средств установленным требованиям по безопасности информации. В России данный процесс регулируется постановлением Правительства от 29 июля 1995 г. № 608 «О сертификации средств защиты информации», которое устанавливает порядок сертификации средств защиты информации в Российской Федерации (далее – постановление).

Согласно постановлению, все средства защиты информации, используемые на объектах информатизации или при работе с секретной информацией, должны быть сертифицированными. Для этого предусмотрены специальные процедуры и испытания, проводимые аккредитованными организациями.

Сертификация средств защиты информации имеет несколько основных целей. Во-первых, это обеспечение соответствия уровня защиты информации установленным требованиям. Во-вторых, это повышение доверия к средствам защиты информации (СЗИ) со стороны пользователей. Также сертификация позволяет выявить уязвимости и недостатки в работе средств защиты информации и устранить их до возникновения серьезных проблем.

Важно отметить, что сертификация средств защиты информации обязательна для всех средств, используемых в критически важных секторах экономики, таких как финансы, энергетика, телекоммуникации и др. Только сертифицированные средства могут быть использованы в процессе обработки, хранения и передачи конфиденциальной информации (рис. 1).

Рис. 1. Нормативная правовая база по сертификации СЗИ

1.3. Система сертификации ФСБ России

В условиях активного развития цифровых технологий и повсеместного использования компьютеров и мобильных устройств защита конфиденциальности данных становится все более актуальной задачей, поэтому важно обратить внимание на систему сертификации средств защиты информации, которая была определена федеральным органом исполнительной власти, уполномоченным в области безопасности, – Федеральной службой безопасности (ФСБ России).

Приказ ФСБ России от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия» определил процедуру сертификации средств защиты информации. Этот документ определяет порядок прохождения сертификации для всех организаций и предприятий, занимающихся разработкой и использованием средств защиты информации.

Основная цель сертификации заключается в обеспечении конфиденциальности информации и защите ее от несанкционированного доступа. Другими словами, система сертификации направлена на подтверждение целостности данных и исключение возможности их несанкционированного изменения или подмены. Кроме того, сертификация стремится гарантировать, что информация будет доступна только авторизованным пользователям, и исключать возможность блокировки или ограничения доступа.

Основная задача системы сертификации – оценка и подтверждение надежности и эффективности защитных мер, применяемых к информационным ресурсам. Это позволяет обеспечить высокий уровень безопасности и защиты данных.

Система сертификации предусматривает механизмы контроля за выполнением требований безопасности в течение срока действия сертификата. Кроме того, она предусматривает процедуру периодического обновления сертификатов с учетом изменяющейся обстановки и появления новых технологий.

1.4. Система сертификации ФСТЭК России

Система сертификации средств защиты информации, управляемая Федеральной службой по техническому и экспортному контролю (ФСТЭК

России), играет ключевую роль. Введение в действие приказа ФСТЭК России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации» (далее – приказ № 55) стало важным шагом к обеспечению высокого уровня безопасности информационных систем и данных на территории России [2].

В соответствии с приказом № 55 средства защиты информации делятся на различные классы в зависимости от уровня защищенности, а также по типу информационных объектов, для которых они предназначены. Это позволяет обеспечить адекватную защиту в зависимости от конкретных потребностей и угроз.

Важным аспектом приказа № 55 является определение требований к испытательным лабораториям, проводящим сертификационные испытания. ФСТЭК России устанавливает высокие стандарты квалификации и аккредитации таких лабораторий, чтобы обеспечить объективность и надежность результатов сертификации (рис. 2).

Рис. 2. Система нормативно-правовых актов в области сертификации

Кроме того, данный приказ устанавливает порядок выдачи сертификатов на средства защиты информации. Этот процесс включает в себя предоставление заявителем необходимых документов, проведение сертификационных испытаний и анализ результатов, после чего ФСТЭК России выдает сертификат о соответствии установленным требованиям.

1.5. Виды, типы и классы средств защиты информации

В современном информационном обществе, где данные являются одним из самых ценных активов, защита информации становится приоритетом для организаций и частных лиц. Средства защиты информации играют ключевую роль в обеспечении конфиденциальности, целостности и доступности данных, предотвращая угрозы вроде кибератак и утечек информации.

Путем изучения классификаций СЗИ читатели смогут лучше понять, какие инструменты и подходы наиболее эффективно соответствуют их конкретным потребностям и задачам по обеспечению безопасности данных.

Рассмотрим классификацию средств защиты информации. Она является важным инструментом для понимания разнообразия СЗИ, их целей и применения в практических задачах обеспечения безопасности.

Одним из ключевых инструментов обеспечения информационной безопасности является криптография – наука об обеспечении конфиденциальности, целостности и аутентичности данных с помощью математических методов и алгоритмов шифрования [3]. Мы разберем классификацию криптографических средств защиты (КСЗ), которая включает в себя криптографические средства защиты уровня 1 (КС1), криптографические средства защиты уровня 2 (КС2), криптографические средства защиты уровня 3 (КС3), ключевую архитектуру (классы КВ и КА).

Классификация криптографических средств защиты информации:

– КС1 охватывает основные алгоритмы шифрования, предназначенные для обеспечения конфиденциальности информации. Этот уровень включает в себя такие методы, как симметричное шифрование, асимметричное шифрование и хэширование данных. Применение КС1 позволяет

зашифровывать данные таким образом, чтобы они стали непонятными для посторонних лиц, не обладающих соответствующим ключом;

– КС2 включает алгоритмы цифровой подписи и механизмы обеспечения целостности данных. Этот уровень криптографии позволяет проверять подлинность и целостность данных, а также обеспечивать невозможность их изменения без обнаружения;

– КС3 включает средства аутентификации и контроля доступа к информации. Этот уровень криптографии предназначен для подтверждения легитимности пользователей и управления их доступом к данным;

– КВ включает в себя методы безопасного хранения криптографических ключей, методы обмена ключами между участниками криптографической системы, аудит и мониторинг ключевых операций и управление ключами шифрования. Ключевая архитектура играет важную роль в обеспечении безопасного хранения, передачи и использования криптографических ключей, необходимых для шифрования и дешифрования данных;

– КА также относится к стандартизации и управлению ключами, но в контексте атрибутов ключей. Это включает управление атрибутами ключей, такими как срок действия, права доступа и прочие параметры, которые могут влиять на безопасность криптографических операций.

Помимо криптографии существуют другие методы и средства защиты информации, включая системы разграничения доступа, средства обнаружения вторжений, антивирусные программы, системы управления безопасностью и многое другое. Рассмотрим их подробнее.

Системы разграничения доступа (СРД) представляют собой инструменты управления доступом к информационным ресурсам на основе уровня авторизации пользователей. Они обеспечивают возможность определения, контроля и ограничения доступа к конфиденциальным данным и ресурсам в соответствии с установленными политиками безопасности. СРД позволяют установить гранулярные права доступа для различных пользователей и групп пользователей, минимизируя риск несанкционированного доступа к информации [4]. Они играют важную роль в обеспечении конфиденциальности, целостности и доступности данных, а также в соблюдении требований безопасности и регулирований (рис. 3).

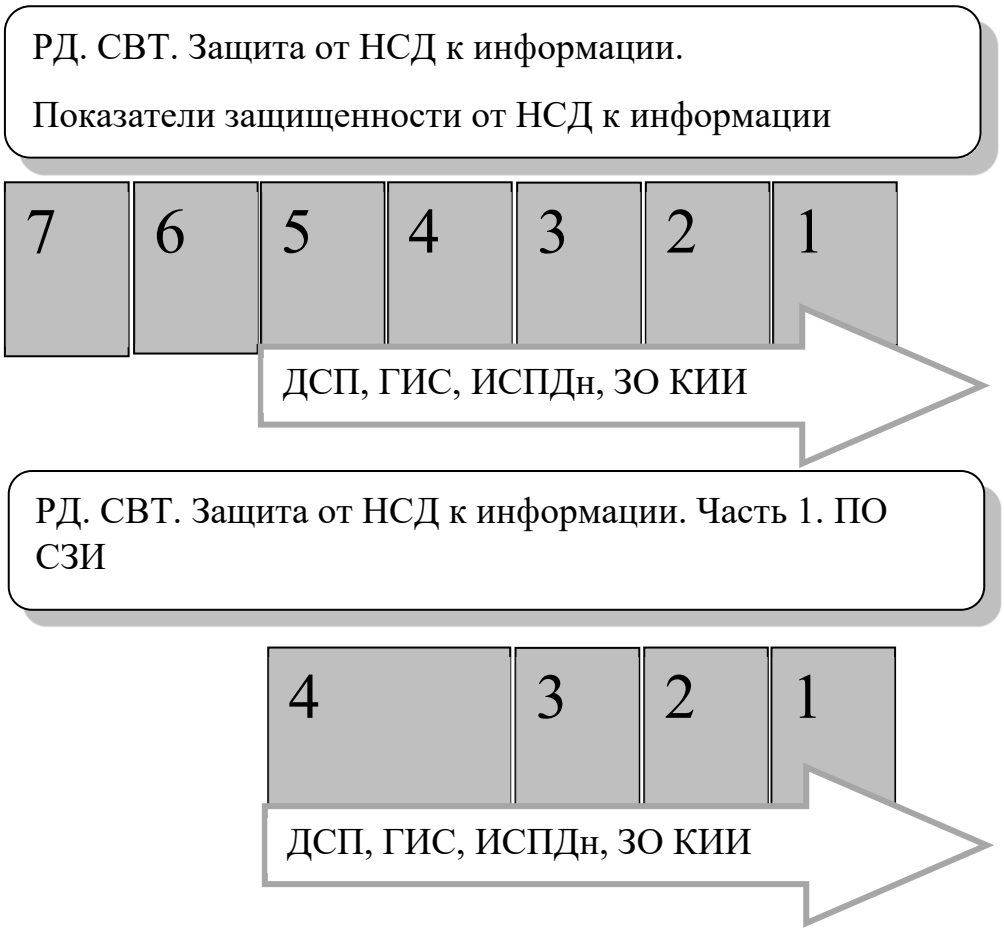

Рис. 3. Классы СВТ

Системы обнаружения вторжений (СОВ) предназначены для мониторинга сетевой активности и выявления аномальных или подозрительных событий, которые могут указывать на попытки несанкционированного доступа или вторжения в информационные системы. СОВ осуществляют анализ трафика, аудит событий и обнаружение аномалий с целью предотвращения угроз безопасности [5]. Они позволяют оперативно реагировать на инциденты безопасности, минимизируя риск утечки данных или нарушения конфиденциальности (рис. 4).

Средства антивирусной защиты предназначены для обнаружения, блокирования и удаления вредоносных программ, таких как вирусы, троянские кони, шпионские программы и другие угрозы для информационной безопасности. Они сканируют файлы и сетевой трафик на наличие подозрительных и вредоносных активностей, обеспечивая защиту от возможных

атак и инцидентов безопасности. Средства антивирусной защиты являются неотъемлемой частью защиты от угроз в современном цифровом мире.

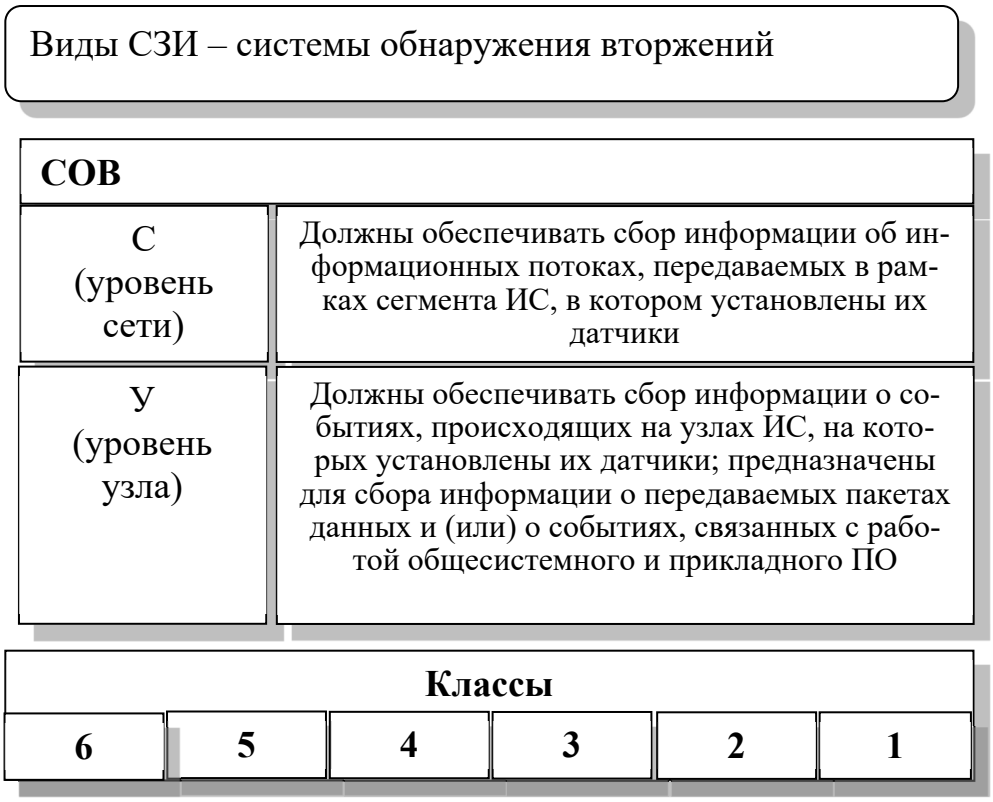

Рис. 4. Классификация СОВ

Средства доверенной загрузки (СДЗ) обеспечивают безопасный и надежный процесс загрузки операционной системы и приложений, предотвращая возможные атаки во время этапа загрузки. Они используют технологии аутентификации и цифровых подписей для проверки целостности и подлинности загружаемого программного обеспечения, а также для предотвращения загрузки неавторизованных или вредоносных компонентов [6]. Средства доверенной загрузки помогают гарантировать безопасность операционной среды и защищать от возможных уязвимостей в процессе загрузки системы (рис. 5).

Средства контроля съемных машинных носителей информации (СКН) предназначены для контроля и управления доступом к внешним устройствам хранения данных, таким как USB-накопители, внешние жесткие диски и карты памяти. Они обеспечивают возможность ограничения доступа к съемным носителям и предотвращения утечки конфиденциальной информации или внедрения

вредоносных программ через такие устройства [7]. Средства контроля съемных машинных носителей играют важную роль в обеспечении безопасности информационных систем и защите от потенциальных угроз безопасности (рис. 6).

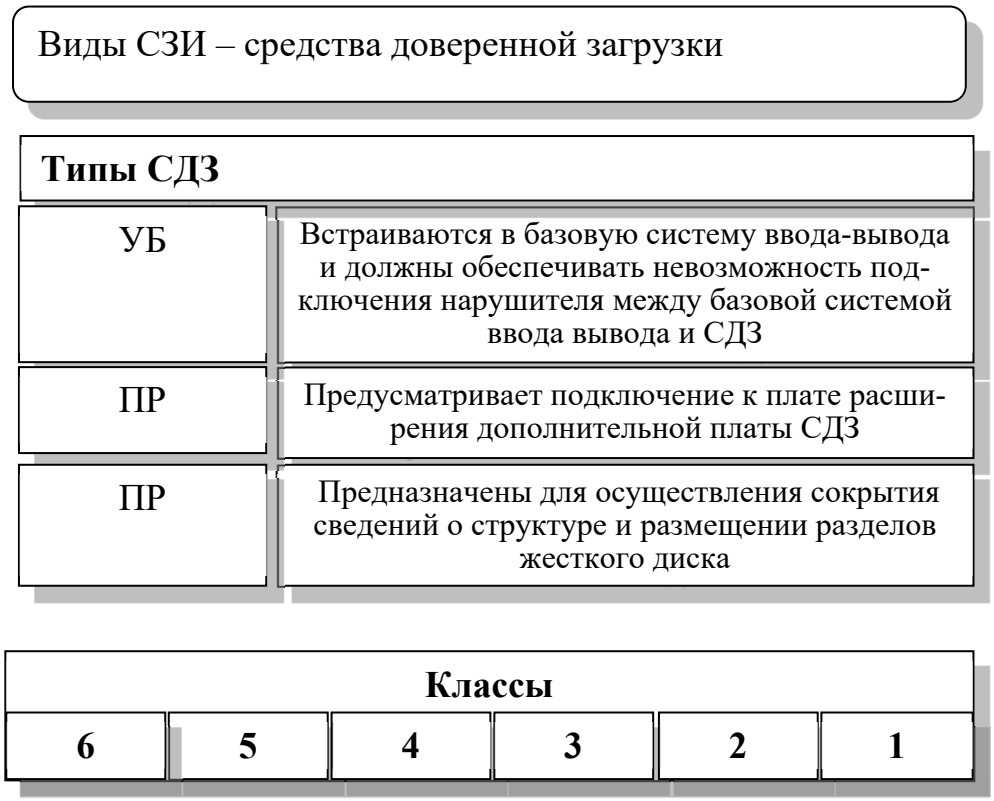

Рис. 5. Классификация СДЗ

Рис. 6. Классификация СКН

Межсетевые экраны (МЭ) (firewalls) играют важную роль в обеспечении безопасности сетевой инфраструктуры. Они контролируют и фильтруют трафик между внутренними и внешними сетями, блокируя нежелательный или подозрительный трафик и обеспечивая соответствие установленным политикам безопасности. Межсетевые экраны способны обнаруживать и предотвращать атаки на прикладном уровне, а также обеспечивать защиту от угроз в реальном времени (рис. 7) [8].

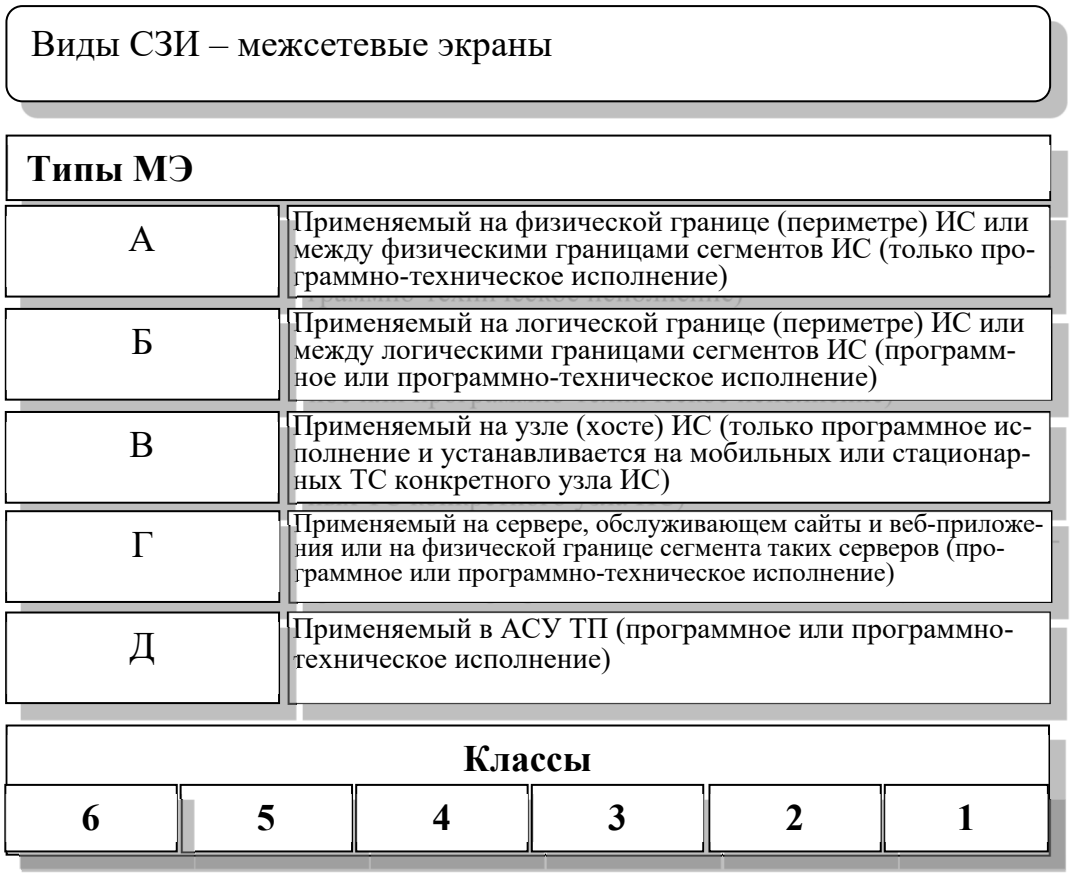

Рис. 7. Классификация МЭ

Операционные системы (ОС) являются основой функционирования компьютера и обеспечивают его работоспособность. ОС выполняют ключевую роль в обеспечении защиты от угроз и вредоносных атак [9]. Операционные системы регулярно обновляются производителями для исправления уязвимостей и обеспечения безопасности (рис. 8).

Средства удаленного доступа предоставляют возможность удаленно подключаться к компьютерным системам или сетям из любого места,

используя сетевые протоколы и методы аутентификации. Они позволяют пользователям работать с данными и приложениями, находящимися в удаленной среде, что обеспечивает гибкость работы и повышает производительность. Однако для обеспечения безопасности удаленного доступа необходимо использовать криптографические протоколы, двухфакторную аутентификацию и другие меры защиты [10].

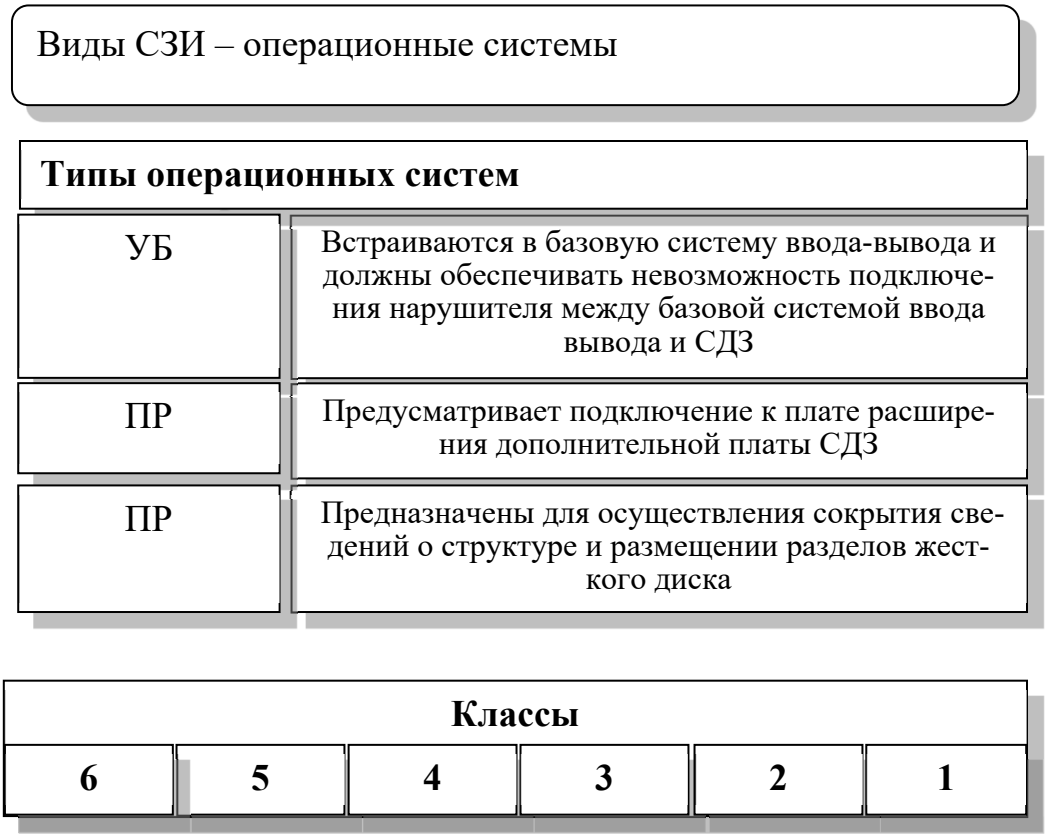

Рис. 8. Классификация ОС

Средства защиты виртуализации предназначены для обеспечения безопасности виртуальных сред, включая виртуальные машины, хранилища данных и средства управления виртуализацией. Они помогают предотвратить атаки на уровне виртуализации, обеспечивают изоляцию виртуальных сред и контролируют доступ к ресурсам. Кроме того, эти средства обеспечивают защиту данных, хранящихся в виртуальных средах, и обеспечивают соответствие стандартам безопасности (рис. 9) [11].

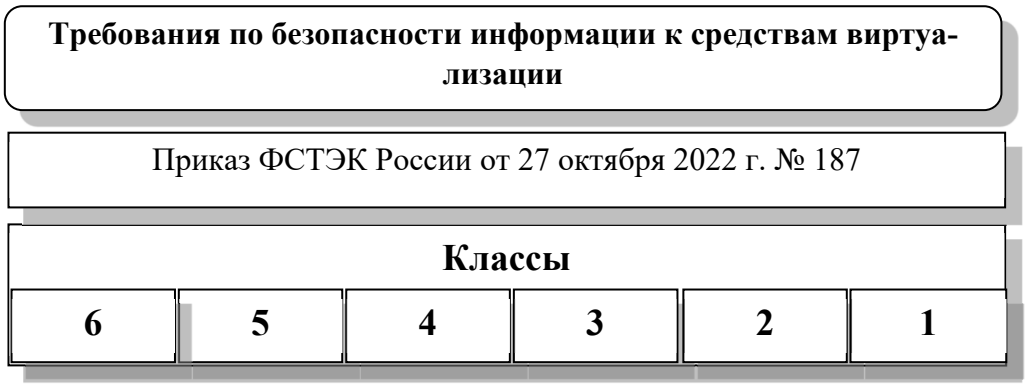

Рис. 9. Требования к средствам защиты среды виртуализации

Средства защиты контейнеризации предназначены для обеспечения безопасности контейнерных сред, таких как Docker, Kubernetes и др. Они обеспечивают изоляцию контейнеров, контролируют доступ к ресурсам и сетевому трафику, а также обнаруживают и предотвращают угрозы на уровне контейнеров. Эти средства также предоставляют механизмы аутентификации и авторизации для контроля доступа к контейнеризованным приложениям и данным (рис. 10).

Рис. 10. Требования к средствам защиты контейнеризации

Системы управления базами данных (СУБД) представляют собой программное обеспечение для создания и управления базами данных. Они обеспечивают хранение, обработку и доступ к данным, а также обеспечивают конфиденциальность, целостность и доступность информации. Для обеспечения безопасности данных и защиты от угроз СУБД предоставляют

средства аутентификации пользователей, управления доступом, шифрования данных и мониторинга активности пользователей.

Многофункциональные межсетевые экраны (UTM – Unified Threat Management) представляют собой интегрированные устройства, которые объединяют в себе несколько функций безопасности сети. Они включают в себя функции файрвола, антивирусной защиты, антиспама, фильтрации веб-трафика, VPN и др. Многофункциональные межсетевые экраны обеспечивают комплексную защиту сети от различных угроз и атак, упрощая управление и снижая стоимость обеспечения безопасности.

2. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К СЗИ

2.1. Функционал средств защиты информации

Система обнаружения вторжений – программный или программно-аппаратный продукт, предназначенный для выявления несанкционированной и/или вредоносной активности в компьютерной сети или на отдельном хосте. Задача – обнаружить проникновение киберпреступников в инфраструктуру и сформировать оповещение безопасности (функций реагирования, например, блокировки нежелательной активности, в таких системах нет), которое будет передано в аналитическую систему для анализа [5].

Средства антивирусной защиты предназначены для сканирования системы и файловых хранилищ на наличие вредоносов; защиты ПК в реальном времени; оповещения пользователя, если обнаружены подозрительные элементы; работы с подозрительными файлами (антивирус может удалить, вылечить или поместить его в карантин).

Средства доверенной загрузки представляют собой инструменты и методы, которые обеспечивают безопасную загрузку и запуск программного обеспечения на компьютере или устройстве. Данные средства позволяют пользователю управлять процессом загрузки и обеспечивают контроль за целостностью и аутентичностью загружаемого программного обеспечения.

Одним из основных средств доверенной загрузки является Trusted Platform Module (TPM). TPM – это чип на материнской плате компьютера, который обеспечивает защиту от вредоносного кода и контролирует цепочку доверия при загрузке системы. Он гарантирует, что загружаемое программное обеспечение не было изменено или подменено третьей стороной.

Еще одним важным средством доверенной загрузки является Secure Boot. Secure Boot используется в операционных системах и позволяет проверять цифровые подписи загружаемых программ и драйверов. Это позволяет обнаруживать и предотвращать загрузку неавторизованного и потенциально вредоносного кода.

Дополнительные средства доверенной загрузки включают в себя механизмы аппаратного уровня, такие как BIOS (Basic Input/Output System) и UEFI (Unified Extensible Firmware Interface), которые обеспечивают безопасность загрузки на более низком уровне аппаратуры компьютера. Они также поддерживают функции, такие как проверка цифровых подписей и аппаратная защита от изменения загрузочного кода.

Средства доверенной загрузки играют важную роль в защите компьютерных систем от вредоносного ПО и несанкционированного доступа. Они обеспечивают пользователю гарантированную безопасность и надежность при загрузке программного обеспечения. Благодаря им компьютерный парк становится более защищенным и контролируемым, а риск утечки данных и кибератак снижается.

Помимо этого, многие СДЗ умеют выполнять роль средства идентификации и аутентификации [6].

Средство контроля съемных машинных носителей информации состоит из двух сертифицированных ФСТЭК России модулей:

– модуль СКН уровня подключения съемных носителей позволяет разграничивать доступ пользователей информационной системы к сменным накопителям и осуществляет контроль подключения накопителей;

– модуль СКН уровня отчуждения (переноса) информации предотвращает утечки информации через сменные накопители и защищает информацию в том числе от внутренних нарушителей [7].

Межсетевой экран предназначен для защиты корпоративной сети, участка сети, сайта или устройства от нежелательного сетевого доступа извне. Основной функционал – фильтрация входящего и исходящего трафика.

Межсетевой экран предотвращает утечку данных, DDoS-атаки и проникновение в сеть вредоносного ПО. Он может иметь программно-аппаратную или программную реализацию. Аппаратный – готовое устройство, которое умеет фильтровать трафик. Программный – ПО, которое нужно установить на сервер, компьютер, устройство [8].

Операционные системы являются основой функционирования компьютера и обеспечивают его работоспособность. В контексте информационной безопасности ОС играют важную роль в обеспечении защиты от угроз

и вредоносных атак. Они предоставляют средства для аутентификации пользователей, контроля доступа, управления ресурсами и обнаружения угроз. Кроме того, операционные системы регулярно обновляются производителями для исправления уязвимостей и обеспечения безопасности [9].

Удаленный доступ работает следующим образом: пользователь устанавливает программу на компьютер, которым он хочет управлять, и на устройство, с которого он будет управлять. После этого он вводит логин и пароль и получает доступ к удаленному компьютеру. При управлении удаленным компьютером все действия, которые пользователь совершает на своем устройстве, передаются на удаленный компьютер, и наоборот [10].

Функции средств защиты виртуализации представлены на рис. 11.

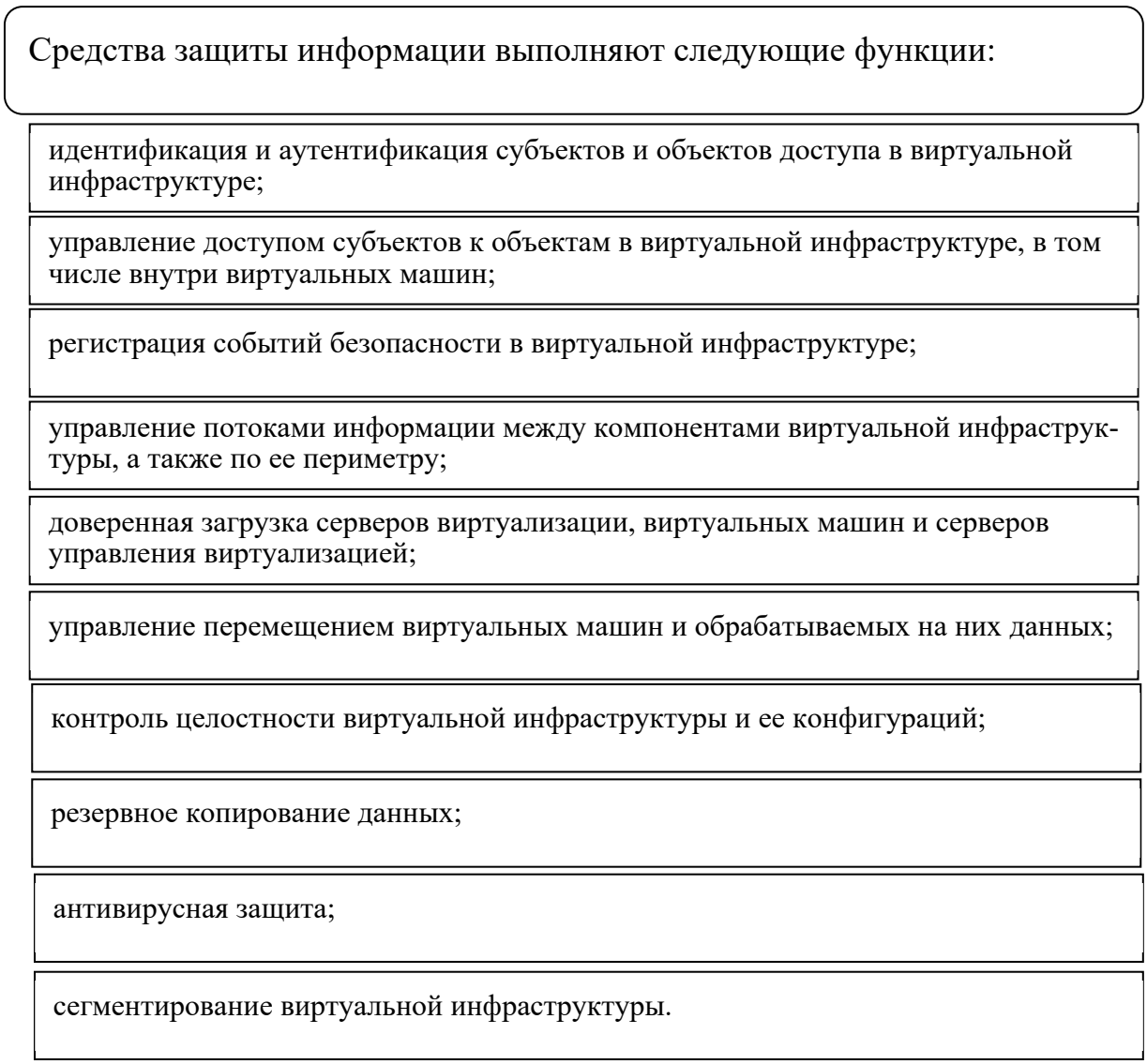

Рис. 11. Функции средств защиты виртуализации

Системы управления базами данных – это программное обеспечение, специально разработанное для эффективного управления большими объемами данных. Они представляют собой мощные инструменты, позволяющие организовать хранение, обработку и доступ к информации в базах данных.

СУБД обеспечивают структурированное хранение данных, что позволяет упростить и ускорить процессы их поиска и обработки. Они предоставляют удобный инструментарий для создания, изменения и удаления данных, а также для выполнения сложных запросов к базе данных. С использованием СУБД можно автоматизировать рутинные операции по обработке информации, что значительно повышает производительность и эффективность работы.

Благодаря СУБД можно реализовать многоуровневую систему безопасности данных. Они позволяют управлять доступом пользователей к информации, устанавливать права на чтение, запись и изменение данных. Кроме того, СУБД автоматически обеспечивают целостность базы данных и защиту от сбоев, что гарантирует сохранность информации и ее доступность в случае сбоев в системе или непредвиденных ситуаций.

Многофункциональные межсетевые экраны (UTM – Unified Threat Management) представляют собой уникальные сетевые устройства, которые предназначены для эффективного управления и обеспечения безопасности компьютерных сетей. UTM объединяет в себе несколько важных функций, таких как защита от вредоносных программ, контроль доступа, противодействие атакам в режиме реального времени, а также обнаружение и предотвращение утечки данных.

Одним из главных преимуществ многофункциональных межсетевых экранов является их способность предоставлять комплексные решения для обеспечения безопасности сети в одном устройстве. Это значительно упрощает процесс управления и экономит ресурсы, так как нет необходимости приобретать и настраивать несколько различных устройств для обеспечения различных аспектов безопасности.

Важным компонентом UTM является их способность обнаруживать и блокировать различные виды угроз, такие как вредоносные программы, спам, фишинг, а также атаки на сетевые ресурсы. Многофункциональные

межсетевые экраны используют несколько слоев защиты, включая межсетевой экран, систему обнаружения вторжений (IPS), систему предотвращения вторжений (IDS), антивирусную защиту, антиспам-фильтры и многое другое. Это позволяет им обнаруживать и обезвреживать различные виды угроз сетевой безопасности, обеспечивая полноценную защиту для организации.

В целом, многофункциональные межсетевые экраны (UTM) представляют собой незаменимый инструмент для обеспечения безопасности компьютерных сетей (рис. 12).

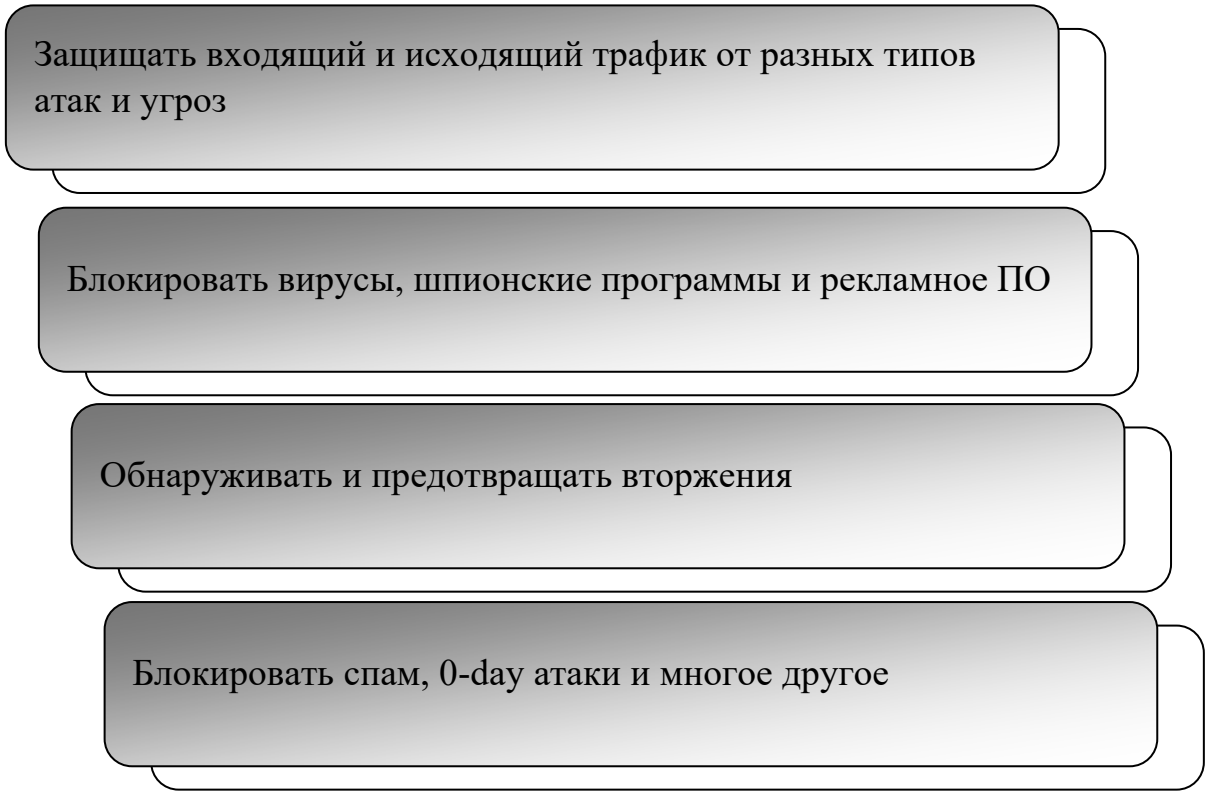

Рис. 12. Функционал UTM

NGFW (Next-Generation Firewall) – межсетевой экран нового поколения, имеющий функции межсетевого экрана, систем защиты каналов и обнаружения вторжений, глубокого анализа, фильтрации веб-трафика и электронной почты, а также разграничения прав доступа пользователей.

NGFW является результатом развития системы UTM (Unified Threat Management), которая также имела различные функции защиты (рис. 13).

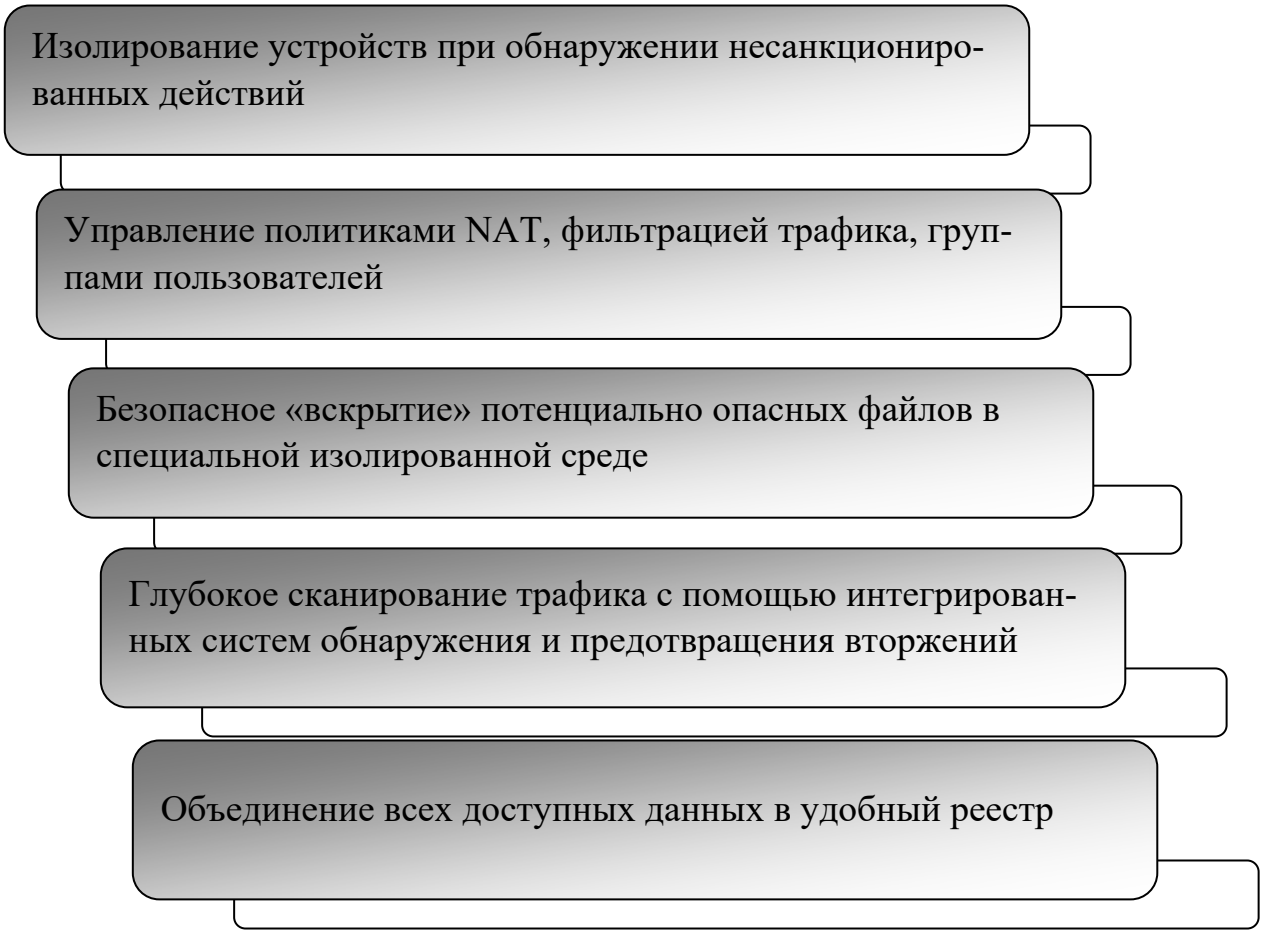

Рис. 13. Функционал NGFW

NGFW предоставляется производителями в качестве программно-аппаратных решений и готовых образов виртуальных машин, которые легко масштабируются под нужды клиентов.

Помимо программно-аппаратного NGFW также можно использовать виртуальный NGFW. Решение является гибко настраиваемым средством организации и защиты межсетевого взаимодействия и может быть частью комплексного решения совместно с другими сервисами кибербезопасности.

2.2. Требования доверия к СЗИ

Требования являются обязательными в области технического регулирования к продукции (работам, услугам), используемой в целях защиты сведений, составляющих государственную тайну или относимых

к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа.

Требования доверия к системам защиты информации являются одним из ключевых аспектов обеспечения надежной защиты информационных ресурсов. Эти требования были утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76 (далее – требования доверия) [12].

Доверие к СЗИ также предполагает их соответствие установленным нормам и стандартам безопасности. Важно, чтобы системы защиты информации были адаптированы к российским требованиям и имели соответствующие сертификаты и документацию.

Кроме того, требования доверия к СЗИ включают в себя проверку производителя и поставщика системы. Они должны быть аккредитованы и иметь репутацию надежных и ответственных организаций.

Важным аспектом требований доверия к СЗИ является высокий уровень защиты от внутренних и внешних угроз. Системы должны быть защищены от вирусов, хакерских атак и других видов мошенничества. Это достигается за счет использования современных алгоритмов шифрования, межсетевых экранов и других средств защиты.

Следует отметить, что соблюдение требований к СЗИ обеспечивает высокий уровень безопасности и надежности систем защиты информации, что является ключевым фактором для успешной деятельности организаций и государства.

Выполнение настоящих требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности информационных технологий, организуемых ФСТЭК России в пределах своих полномочий в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации» [2].

Для дифференциации требований по безопасности информации к средствам устанавливается 6 уровней доверия (рис. 14).

Разработчик, создавая средство защиты информации, должен выполнить следующие процедуры и мероприятия (рис. 15).

ТРЕБОВАНИЯ ПРИМЕНЯЮТСЯ:

- в значимых объектах критической информационной инфраструктуры;
- в государственных информационных системах;
- в автоматизированных системах управления производственными и технологическими процессами;
- в информационных системах персональных данных.

Рис. 14. Виды информационных систем, для которых применяются требования доверия к СЗИ

При разработке средства разработчиком должны быть выполнены процедуры, предусматривающие:

- разработку модели безопасности средства;
- проектирование архитектуры безопасности средства;
- разработку функциональной спецификации средства;
- проектирование средства;
- разработку проектной (программной) документации;
- выбор средств разработки, применяемых для создания средства;
- управление конфигурацией средства;
- разработку документации по безопасной разработке средства;
- разработку эксплуатационной документации.

Рис. 15. Обязательные процедуры для разработчиков СЗИ

Разрабатываемое средство защиты информации должно подвергнуться испытаниям (рис. 16).

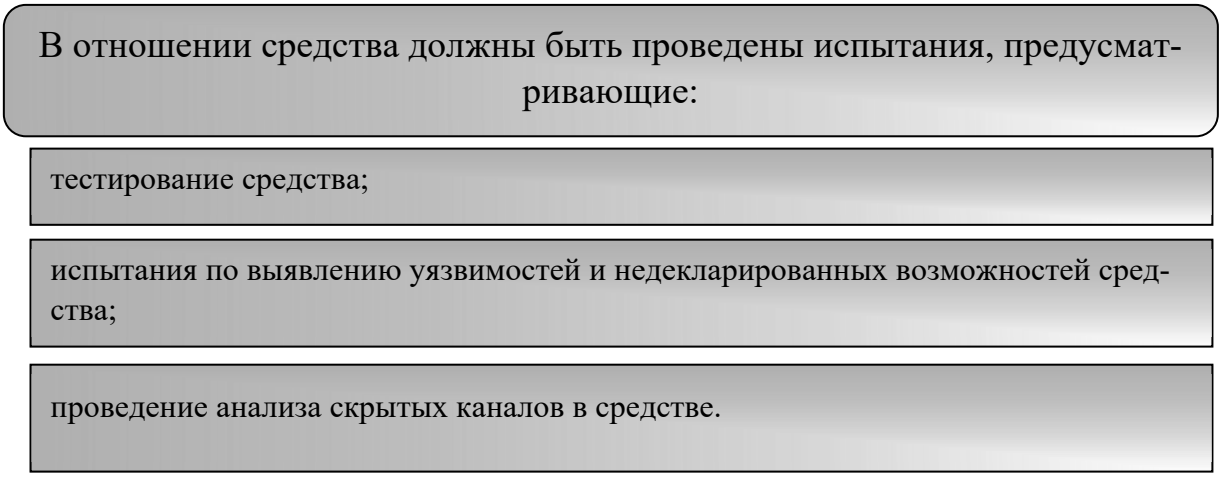

Рис. 16. Испытания для СЗИ

Разрабатываемое средство защиты информации должно обеспечиваться поддержкой безопасности средства, при котором должны учитываться следующие факторы (рис. 17).

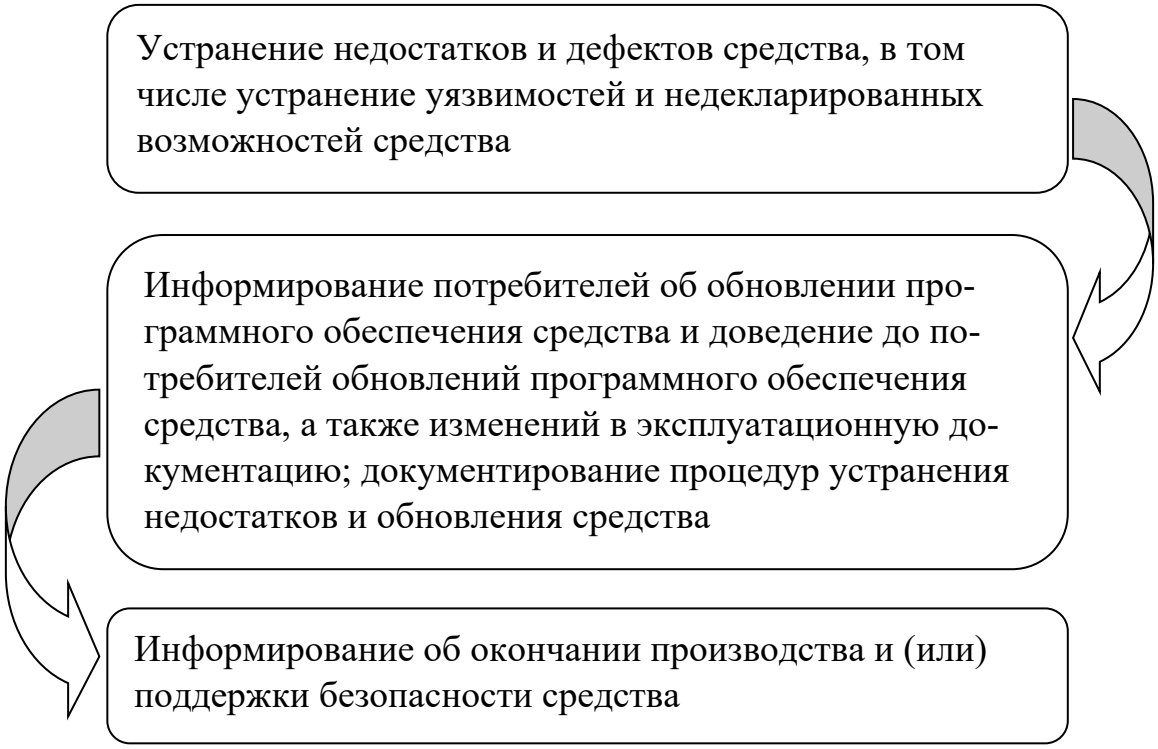

Рис. 17. Поддержка безопасности

3. ПОИСК УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

3.1. Недекларированные возможности

Недекларированные возможности – это функциональные возможности, которые не были описаны или не соответствуют описанию в документации. Их использование может привести к нарушению конфиденциальности, доступности или целостности обрабатываемой информации. Такие возможности являются скрытыми и не подразумеваются в процессе обычного использования программного обеспечения. Они могут быть преднамеренно внедрены разработчиками для специальных целей или по ошибке оставлены без внимания. Недекларированные возможности могут стать уязвимостями, которые злоумышленники могут использовать для несанкционированного доступа к системе или получения чувствительной информации. Поэтому при разработке программного обеспечения важно уделить должное внимание обнаружению и устранению таких возможностей, чтобы обеспечить безопасность и защиту данных, обрабатываемых системой.

Данная работа осуществляется в соответствии с Методикой выявления уязвимостей и недекларированных возможностей в программном обеспечении (далее – Методика), разработана в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 [13].

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении – это структурированный и систематический подход, при помощи которого выполняется анализ программного обеспечения с целью обнаружения и идентификации потенциальных проблемных мест. Эта методика позволяет выявить уязвимости, которые могут стать точкой входа для злоумышленников, а также обнаружить скрытые возможности, которые могут быть использованы для улучшения функциональности программы.

Основной этап методики заключается в проведении тщательного анализа и тестирования программного обеспечения с использованием различных техник и инструментов. В процессе анализа проводится проверка наличия уязвимостей и недекларированных возможностей, а также оценивается их серьезность и потенциальные последствия для системы.

Для выявления уязвимостей и недекларированных возможностей могут применяться различные методы, включая статический и динамический анализ программного кода, инструменты поиска синтаксических и логических ошибок, анализ возможных векторов атак и моделирование угроз.

Одним из важных аспектов такой методики является составление и выполнение специально разработанных тестовых сценариев, которые помогут выявить скрытые уязвимости и недокументированные возможности. Также могут использоваться автоматизированные инструменты для обнаружения и анализа уязвимостей, что позволяет оптимизировать процесс и сэкономить время.

Методика определяет состав и содержание исследований по выявлению уязвимостей и недекларированных возможностей в общесистемном и прикладном программном обеспечении, в программном обеспечении средств защиты информации (далее – объект оценки, ОО), а также применяемые при этом методы исследований и инструментальные средства анализа и контроля.

Методика применяется при проведении контроля отсутствия уязвимостей и недекларированных возможностей в ОО, проводимого в соответствии с Требованиями доверия.

Методика ориентирована на проведение исследований, проводимых испытательными лабораториями и разработчиками в рамках сертификационных испытаний программных, программно-аппаратных средств защиты информации и защищенных программных, программно-технических средств, а также при внесении изменений в ранее сертифицированные средства. Разработчикам ОО рекомендуется использовать положения Методики для организации внутренних процессов жизненного цикла программного обеспечения в соответствии с ГОСТ Р 56939-2016 «Защита

информации. Разработка безопасного программного обеспечения. Общие требования».

3.2. Общие требования к проведению исследований по выявлению уязвимостей и недекларированных возможностей

Исследования ОО по выявлению уязвимостей и недекларированных возможностей (НДВ) проводятся с целью выявления условий и факторов, создающих возможность нарушения целостности ОО, а также нарушения конфиденциальности, целостности и доступности обрабатываемых (защищаемых) данных (далее – нарушение безопасности ОО) (рис. 18).

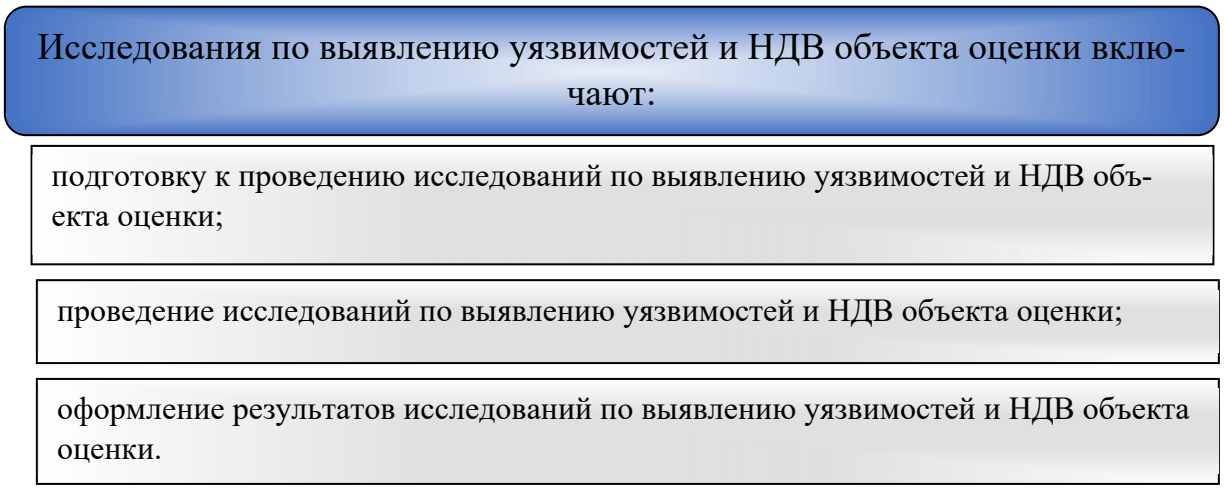

Рис. 18. Исследования ОО

Для дифференциации требований к исследованиям ОО по выявлению уязвимостей и НДВ устанавливается 6 уровней контроля. Самый низкий уровень – шестой, самый высокий – первый.

Разработчиком предоставляются следующие исходные данные для выявления уязвимостей (рис. 19).

От разработчика ОО испытательная лаборатория получает все, что указано на рис. 19. Методика содержит требования к проведению исследований.

Исходными данными, предоставляемыми разработчиком для выявления уязвимостей и НДВ объекта оценки, являются:

- документация на ОО;
- исходный текст (исходный код) объекта оценки, за исключением 6-го уровня доверия;
- сборочная среда объекта оценки;
- дистрибутив объекта оценки;
- функциональные тесты;
- результаты, полученные в ходе реализации процессов безопасной разработки ОО в соответствии с принятыми у разработчика процедурами по безопасной разработке программного обеспечения.

Рис. 19. Исходные данные

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

В ходе подготовки к проведению исследований по выявлению уязвимостей и НДВ объекта оценки должны выполняться:

а) анализ документации и иных исходных данных;

б) подготовка исследовательского стенда.

При анализе документации и иных исходных данных должен быть проведен анализ документации на ОО и иных исходных данных, по результатам которого испытательной лабораторией определяется представление об ОО, его интерфейсах, поверхности атаки на ОО, а также разрабатывается методика проведения испытаний.

Исходными данными при проведении исследований являются: документация на ОО и документы согласно Требованиям к доверию.

Дополнительно для проведения исследований разработчик предоставляет тестовую документацию, демонстрирующую полное, неизбыточное

покрытие функциональными тестами заявленных функций безопасности. Предоставляемая разработчиком тестовая документация должна содержать описание целей тестирования, тестовых процедур и ожидаемых результатов, а также фактические результаты тестирования (журналы регистрации событий, скриншоты и т. п.).

Должен быть проведен анализ поверхности атаки ОО, предусматривающий определение и включение в состав поверхности атаки внешних интерфейсов ОО, непосредственно доступных для атаки потенциальным нарушителям. Должен быть составлен перечень программных модулей, реализующих эти интерфейсы.

К внешним интерфейсам ОО, непосредственно доступным для атаки потенциальным нарушителям, относятся все интерфейсы, для которых одновременно выполняются следующие условия:

а) интерфейс доступен потенциальному нарушителю в ходе штатного функционирования ОО (файлы, сетевые порты, консольный интерфейс и интерфейсы подключения съемных носителей информации к техническим средствам, на которых эксплуатируется ОО);

б) наличие потенциальных уязвимостей в модулях, реализующих данный интерфейс, может привести к нарушению безопасного функционирования ОО.

Интерфейсы, защищенные посредством применения шифрования в соответствии с требованиями ФСБ России, не относятся к интерфейсам ОО, доступным для атаки потенциальным нарушителям. Данное исключение не относится к иным интерфейсам ОО, которые становятся доступными, после прохождения интерфейсов, защищенных шифрованием.

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 ОО.

При проведении исследований исходными данными являются: сведения, полученные по результатам анализа документации ОО и других исходных данных, содержащих сведения об ОО и сборочной среде, а также дистрибутив объекта оценки.

В ходе подготовки исследовательского стенда должны быть выполнены:

а) настройка сред функционирования ОО;

б) контрольная сборка ОО с расчетом контрольных сумм для исходного кода, исполняемых файлов и дистрибутива ОО (для соответствующих уровней контроля);

в) установка и настройка ОО;

г) антивирусный контроль ОО и среды его функционирования.

3.4. Проведение исследований по выявлению уязвимостей и недекларированных возможностей

В ходе проведения исследований по выявлению уязвимостей и НДВ объекта оценки должны выполняться:

а) анализ архитектуры ОО;

б) статический анализ ОО;

в) динамический анализ ОО;

г) экспертиза кода ОО.

Анализ архитектуры ОО включает:

а) анализ состава модулей, конфигураций и интерфейсов ОО;

б) анализ безопасности ОО на основе открытых источников.

Должен быть проведен анализ архитектуры ОО с целью выявления в нем потенциально опасных функциональных возможностей, архитектурных уязвимостей и уязвимостей конфигурации.

Исходными данными при проведении исследований являются:

– исходный текст;

– документация на оцениваемый объект;

– исполняемый код;

– представление об объекте оценки, включая сведения о сторонних компонентах программного обеспечения.

Когда проводится анализ безопасности объекта оценки на основе открытых источников, то предъявляются требования к исследованиям: должна быть проведена идентификация уязвимостей ОО по открытым источникам информации, предусматривающая выявление актуальных

известных уязвимостей в ОО, а также потенциальных уязвимостей ОО с последующим тестированием их на проникновение.

При статическом анализе объекта оценки предъявляются требования к исследованиям. Должен быть выполнен статический анализ исходного кода ОО, направленный на выявление потенциальных уязвимостей кода и НДВ в исходном коде ОО.

К результатам применения разработчиком статического анализа относятся предупреждения о потенциальных уязвимостях кода, полученные от статического анализатора, разметка полученных предупреждений, принятые меры по исправлению уязвимостей.

Испытательной лабораторией оцениваются предоставленные разработчиком результаты применения статического анализа исходного кода, проводимого при разработке безопасного ПО:

а) оценивается соответствие технологического уровня применяемого разработчиком статического анализатора требованиям к уровню исследований, определенным Методикой;

б) оценивается корректность настройки статического анализатора (должен выполняться поиск всех поддерживаемых типов ошибок, относящихся к критическому уровню и высокому уровню опасности);

в) оценивается полнота применения статического анализа (анализ исходного кода должен проводиться в отношении всего набора модулей ОО, согласно требованиям уровня контроля);

г) оценивается регулярность применения статического анализатора, полнота исправления ошибок, относящихся к критическому уровню и высокому уровню опасности (регулярным считается применение статического анализатора не реже чем 1 раз в неделю при условии обновления исходного кода или конфигурации статического анализатора).

Если по совокупности выполнения пунктов «а» – «г» установлено соответствие положениям Методики (дана положительная оценка), испытательная лаборатория должна самостоятельно провести статический анализ исходного кода.

О полученных предупреждениях об ошибках, относящихся к критическому уровню и высокому уровню опасности и классифицированных

разработчиком как ложные срабатывания, испытательной лабораторией оценивается корректность такой классификации.

Если по совокупности выполнения пунктов «а» – «г» установлено несоответствие положениям Методики (дана отрицательная оценка), статический анализ проводится испытательной лабораторией самостоятельно.

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

Испытательной лабораторией проводится разметка (истинные и ложные срабатывания) всех предупреждений об ошибках, относящихся к критическому уровню и высокому уровню опасности.

При проведении динамического анализа объекта оценки динамический анализ ОО включает:

а) тестирование модулей;

б) фаззинг-тестирование;

в) системное тестирование.

В зависимости от уровня контроля исследования ОО динамический анализ должен проводиться на специальной сборке ОО со встроенными датчиками срабатывания ошибок, подготовленной на предыдущем этапе. Комплект используемых датчиков (санитайзеры и отладочные аллокаторы) фиксируется в протоколе испытаний.

Если используемый компилятор для выбранной среды (сред) функционирования не позволяет штатным образом встраивать такие датчики срабатывания ошибок, исследование проводится на обычной сборке с применением средств динамического двоичного инструментирования и отладочных аллокаторов, подключаемых на этапе компоновки, при условии наличия таких средств инструментирования и отладки.

Если при проведении какого-либо вида динамического анализа ОО были выявлены механизмы, встроенные в исходный или исполняемый код ОО и препятствующие проведению исследований, то такие механизмы и защищенные программные модули (участки кода) должны быть проанализированы при проведении экспертизы кода. Если суммарный объем исходного кода данных механизмов и защищенных модулей (участков кода)

превосходит 10 000 строк, делается вывод о невозможности проведения дальнейших испытаний.

При тестировании модулей объекта оценки требования к исследованиям: в ходе проведения исследований должно быть проведено выполнение модульных и регрессионных тестов модулей ОО со сбором покрытия по каждому модулю.

Тестирование модулей ОО обеспечивается применением соответствующего метода, описание которого приведено в прил. 2 Методики (рис. 20).

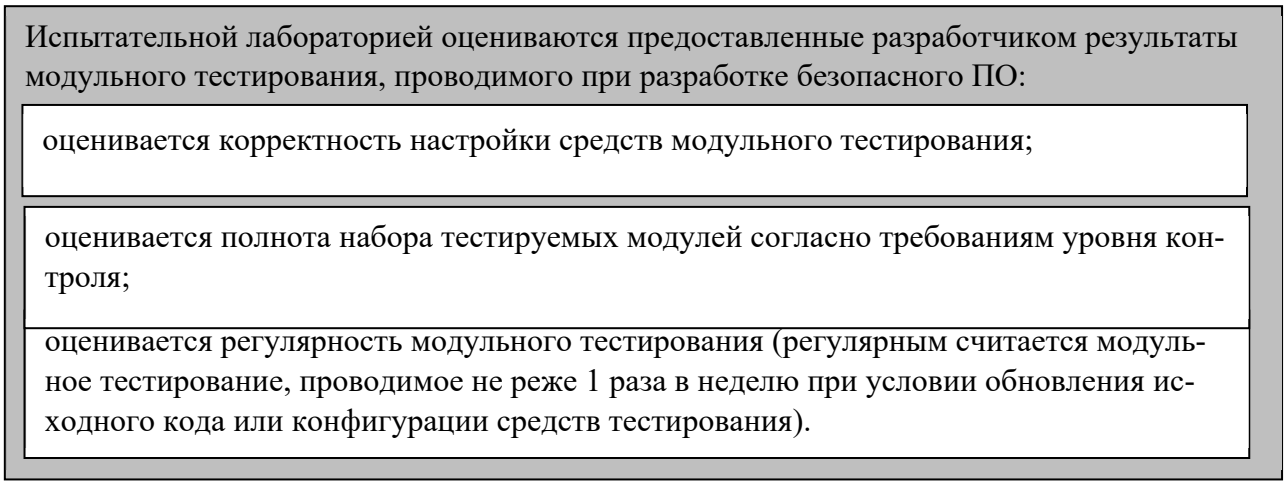

Рис. 20. Схема оценки результатов модульного тестирования

Если по совокупности выполнения пунктов «а» – «в» дана положительная оценка, исследования ограничиваются верификацией результатов модульного тестирования, предоставленных разработчиком. При этом все зафиксированные сбои (аварийные завершения, «зависания», нарушение спецификаций и др. должны быть исправлены.

Если по совокупности выполнения пунктов «а» – «в» дана отрицательная оценка, испытательная лаборатория должна самостоятельно провести тестирование модулей.

При проведении фаззинг-тестирования объекта оценки требованиями к исследованиям являются: должно быть проведено фаззинг-тестирование ОО, направленное на выявление архитектурных уязвимостей и уязвимостей кода в ОО.

Исходные данные устанавливаются Методикой в соответствии с требуемым уровнем контроля.

К результатам фаззинг-тестирования относятся конфигурационные параметры фаззинг-тестирования, наборы входных данных (в том числе словари и модели), результаты фаззинг-тестирования (журналы работы, выявленные уязвимости), принятые меры по исправлению подтвержденных уязвимостей (рис. 21).

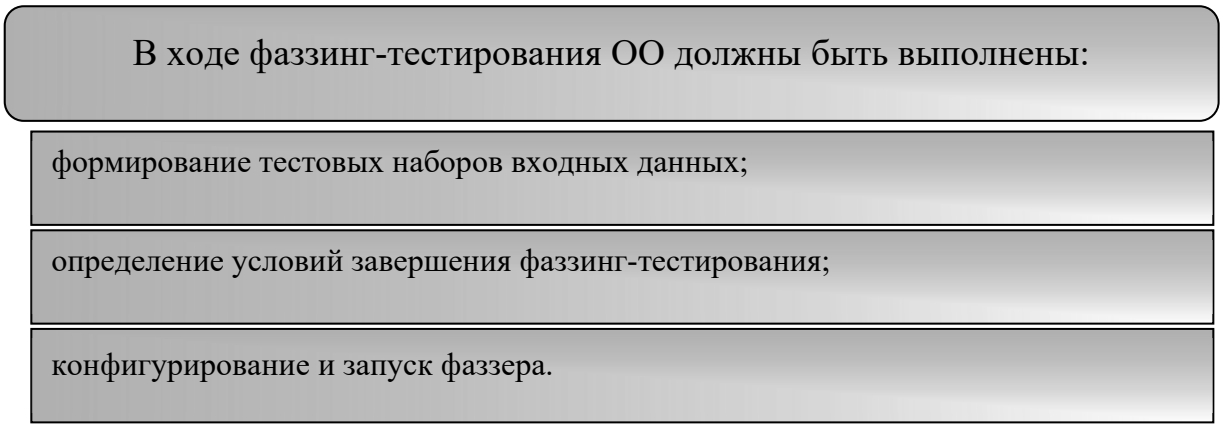

Рис. 21. Процедуры, проводимые в ходе фаззинг-тестирования

Фаззинг-тестирование ОО выполняется методом мутационного фаззинг-тестирования, описание метода приведено в прил. 2 Методики.

Испытательной лабораторией оцениваются предоставленные разработчиком результаты фаззинг-тестирования, проводимого при разработке безопасного ПО (рис. 22).

При проведении системного тестирования объекта оценки требованиями к исследованиям выступают: должен быть проведен анализ трасс выполнения ОО, зафиксированных в ходе выполнения системных тестов, с целью выявления уязвимостей кода и НДВ, связанных с утечками данных и несанкционированным удаленным управлением ОО.

Для проведения исследования разработчик ОО предоставляет испытательной лаборатории высокоуровневое описание всех интерфейсов (типов данных), посредством которых ОО отправляет какие-либо данные во внешнюю сеть (записывает данные из памяти на носитель информации), с указанием типов информации. Описание интерфейсов и типов данных может

быть предоставлено без конкретизации форматов и значений полей и необходимо для выявления несанкционированного обращения объекта оценки к различным ресурсам. К результатам системного тестирования относятся результаты выполнения функциональных системных тестов, собранные журналы (трассы) сетевой активности и системных вызовов, принятые меры по устранению выявленных уязвимостей и НДВ.

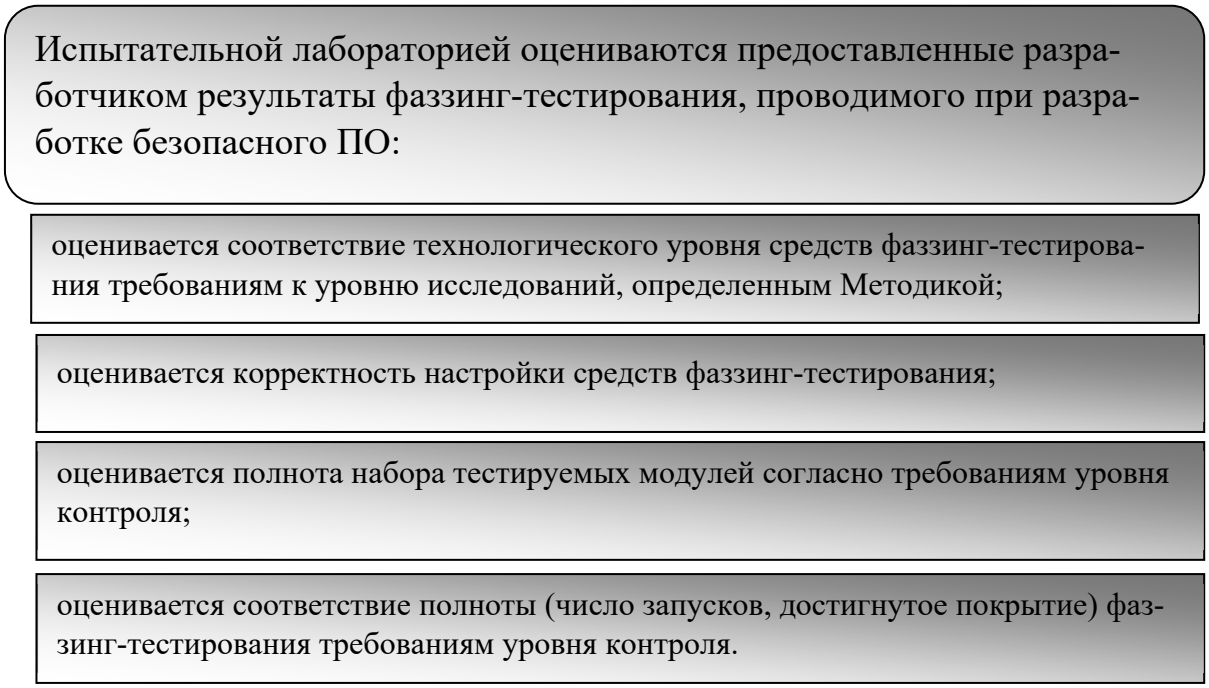

Рис. 22. Схема оценки результатов фаззинг-тестирования

Используемые в исследовании системные тесты должны быть воспроизводимыми.

Испытательной лабораторией оцениваются предоставленные разработчиком результаты системного тестирования, проводимого при разработке безопасного ПО в соответствии с Методикой, для требуемого уровня контроля.

Если по совокупности выполнения пунктов «а» – «г» дана положительная оценка, исследования ограничиваются верификацией результатов системного тестирования, предоставленных разработчиком. Все зафиксированные сбои (аварийные завершения, «зависания», нарушение спецификаций и др.) и идентифицированные НДВ должны быть исправлены.

Если по совокупности выполнения пунктов «а» – «г» дана отрицательная оценка, системное тестирование проводится испытательной лабораторией самостоятельно.

Выявленные в ходе системного тестирования уязвимости кода и НДВ предоставляются разработчику ОО для устранения.

При проведении экспертизы кода объекта оценки проводится экспертиза кода ОО, которая представляет собой ручной анализ (экспертизу) участков исходного/восстановленного кода ОО с целью выявления уязвимостей и НДВ.

Требования к исследованиям: должен быть выполнен ручной направленный анализ с целью выявления архитектурных уязвимостей, уязвимостей кода, потенциально опасных функциональных возможностей, НДВ в ОО.

Экспертиза участков исходного/восстановленного кода предусматривает ручной направленный анализ кода, незадействованного в ходе динамического анализа из-за встроенных в код механизмов, препятствующих динамическому анализу, участков исходного кода, написанного с использованием языков программирования, не поддерживаемых используемым статическим анализатором, а также программных модулей, исполняемый код которых был подвергнут преобразованиям (инструментированию, модификациям произвольного вида) в процессе сборки.

В отношении программных модулей, исполняемый код которых после компиляции был подвергнут преобразованиям (инструментированию, модификациям произвольного вида), проводится экспертиза исполняемого кода.

В отношении участков исходного кода, написанного с использованием языков программирования, не поддерживаемых используемым статическим анализатором, проводится экспертиза исходного кода.

В отношении кода, незадействованного в ходе динамического анализа, проводится экспертиза исходного и исполняемого кода.

Рекомендуется проводить работы по выявлению фактов:

– использования потенциально опасных программных интерфейсов;

– наличия в ОО заведомо некачественного программного кода (заведомо некорректное оформление исходного текста, невыполнимые или тождественные условия, не удаленные отладочные сообщения и т. п.);

– небезопасной загрузки библиотек;

– некорректной обработки ошибок;

– недостаточного ограничения прав доступа посторонних субъектов к временным файлам;

– недостаточно полной проверки недопустимости присутствия во входных данных фрагментов программ на интерпретируемых языках (SQL-инъекции, XSS-атаки и т. п.);

– некорректной обработки длин буферов с данными;

– некорректной обработки ситуаций, когда вместо обычного файла 00 предоставляется именованный канал, символическая ссылка или иной файловый объект специального вида;

– ненадлежащего обеспечения корректности совместного доступа к глобальным данным в параллельных вычислениях;

– ненадлежащего хранения аутентификационных данных в оперативной или внешней памяти;

– переполнения буферов;

– предоставления пользователям избыточной функциональности до аутентификации;

– предоставления пользователям избыточных полномочий;

– утечки чувствительных данных в журнальные файлы;

– утечки оперативной памяти, файловых дескрипторов, графических ресурсов и т. п.;

– целочисленных переполнений;

– наличия неиспользуемых программных компонентов: функций, процедур, переменных, классов и др.

Если при проведении динамического анализа были выявлены механизмы, препятствующие проведению исследований, то программы (программные модули), участки кода, содержащие такие механизмы защиты, должны быть проанализированы совместно с разработчиком ОО. В случае отказа разработчика от анализа специалистами испытательной лаборатории могут быть самостоятельно разработаны решения по снятию механизмов защиты от исследований. Если разработчик ОО отказался снимать механизмы защиты, препятствующие проведению исследований, или

предлагаемые разработчиком или специалистами испытательной лаборатории решения по снятию механизма защиты не позволяют провести исследования в полном объеме, то делается вывод о невозможности дальнейших исследований.

Определение программных ошибок должно осуществляться на основании сведений, содержащихся в соответствующих базах данных (например, таких как Common Weakness Enumeration или Fortify Taxonomy: Software Security Errors), а также руководствах и стандартах, отражающих лучшие практики разработки безопасных программ (например, таких как SEICERTC++ Coding Standard или The CERT Oracle Secure Coding Standard for Java).

В ходе экспертизы кода помимо наличия программных ошибок должен проводиться контроль отсутствия фактов использования сторонних программ (программных модулей), не входящих в состав ОО при реализации ОО функций безопасности.

В ходе экспертизы участков исходного/восстановленного кода должен быть зафиксирован перечень проверяемых программных ошибок и критерии их выявления.

Экспертиза исходного кода должна проводиться с использованием инструментов, обеспечивающих навигацию на уровнях модулей (файлов) и структурных элементов языка программирования анализируемой программы. Если код написан на языке программирования, для которого отсутствуют инструменты с такими возможностями, допускается проводить исследование с помощью штатных утилит работы с текстами и файлами, такими как Is, find, grep, cat, sort и др.

Инструментальные средства для исследования физической структуры. При проведении экспертизы восстановленного исполняемого кода применяемый дизассемблер должен выполнять итеративное дизассемблирование, обеспечивающее лучшее покрытие дизассемблируемого кода в сравнении с линейным (жадным, от англ. greedy) дизассемблированием. Рекомендуется применять программные инструменты, обеспечивающие восстановление и визуализацию потоков управления и данных на уровне исполняемого кода, либо декомпиляторы в язык высокого уровня.

Проведение экспертизы кода обеспечивается применением метода экспертизы кода, описание которого приведено в прил. 2 к Методике.

Выявленные недостатки предоставляются заявителю для устранения. Меры по устранению уязвимостей и НДВ, разработанные заявителем, подлежат исследованию в соответствии с Методикой.

В отношении включенных в состав анализируемого ОО сред выполнения интерпретируемых языков данное исследование не проводится.

ЗАКЛЮЧЕНИЕ

Данное учебное пособие представляет собой основной исчерпывающий источник информации о проведении оценки соответствия средств защиты информации. В его содержании представлены тщательно структурированные разделы, которые пошагово вводят читателя в процесс оценки, объясняют основные концепции и принципы, а также предоставляют необходимые инструменты и методики для успешной реализации данной процедуры.

Основной целью учебного пособия является обеспечение читателей необходимыми знаниями и навыками, которые помогут им профессионально и качественно выполнить оценку соответствия средств защиты информации в их организации. Для достижения этой цели каждый раздел пособия подробно описывает основные этапы проведения оценки, начиная с планирования и определения целевых показателей и заканчивая анализом и оценкой полученных результатов.

Кроме того, учебное пособие акцентирует внимание на важности правильного подхода к выбору и использованию средств защиты информации. Оно предоставляет рекомендации и руководства по определению подходящих средств защиты, их конфигурированию и эффективному использованию в соответствии с уникальными потребностями каждой организации.

Продуманный и логически структурированный подход данного учебного пособия делает его одним из наиболее ценных ресурсов для всех, кто заинтересован в эффективной оценке соответствия средств защиты информации. Благодаря обширным примерам, иллюстрациям и практическим рекомендациям читатели получают всестороннее и практически применимое знание для успешного выполнения данной задачи. Будь то опытный специалист по информационной безопасности или новичок, данное учебное пособие даст им все необходимое для достижения высоких результатов в области оценки соответствия средств защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О техническом регулировании [Электронный ресурс] : федер. закон от 27.12.2002 № 184-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».

2. Об утверждении положения о системе сертификации средств защиты информации [Электронный ресурс] : приказ ФСТЭК России от 03.04.2018 № 55. – Доступ из справ.-правовой системы «КонсультантПлюс».

3. Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия [Электронный ресурс] : приказ ФСБ России от 13.10.1999 № 564. – Доступ из справ.-правовой системы «КонсультантПлюс».

4. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [Электронный ресурс] : утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992. – Доступ из справ.-правовой системы «КонсультантПлюс».

5. Требования к системам обнаружения вторжений [Электронный ресурс] : приказ ФСТЭК России от 6.12.2011 № 638. – Доступ из справ.-правовой системы «КонсультантПлюс».

6. Требования к средствам доверенной загрузки [Электронный ресурс] : утверждены приказом ФСТЭК России от 27.09.2013 № 119. – Доступ из справ.-правовой системы «КонсультантПлюс».

7. Требования к средствам контроля съемных машинных носителей информации [Электронный ресурс] : приказ ФСТЭК России от 28.07.2014 № 87. – Доступ из справ.-правовой системы «КонсультантПлюс».

8. Требования к межсетевым экранам [Электронный ресурс] : приказ ФСТЭК России от 9.02.2016 № 9. – Доступ из справ.-правовой системы «КонсультантПлюс».

9. Требования безопасности информации к операционным системам [Электронный ресурс] : приказ ФСТЭК России от 19.08.2016 № 119. – Доступ из справ.-правовой системы «КонсультантПлюс».

10. Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах [Электронный ресурс] : приказ ФСТЭК России от 16.02.2021 № 32. – Доступ из справ.-правовой системы «КонсультантПлюс».

11. Требования безопасности информации к средствам виртуализации [Электронный ресурс] : приказ ФСТЭК России от 27.10.2022 № 187. – Доступ из справ.-правовой системы «КонсультантПлюс».

12. Требования по безопасности информации [Электронный ресурс] : приказ ФСТЭК России от 02.06.2020 № 76. – Доступ из справ.-правовой системы «КонсультантПлюс».

13. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении, новая редакция [Электронный ресурс] : утверждена ФСТЭК России 25.10.2020. – Доступ из справ.-правовой системы «КонсультантПлюс».

Учебное издание

Селифанов Валентин Валерьевич

Звягинцева Полина Александровна

НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ОЦЕНКА СООТВЕТСТВИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Редактор *О. В. Георгиевская*

Компьютерная верстка *Ю. С. Мерзликиной*

Изд. лиц. ЛР № 020461 от 04.03.1997.
Подписано в печать 12.09.2024. Формат 60 × 84 1/16.
Усл. печ. л. 2,67. Тираж 115 экз. Заказ 107.
Гигиеническое заключение
№ 54.НК.05.953.П.000147.12.02. от 10.12.2002.

Редакционно-издательский отдел СГУГиТ
630108, Новосибирск, ул. Плахотного, 10.

Отпечатано в картопечатной лаборатории СГУГиТ
630108, Новосибирск, ул. Плахотного, 8.