**Описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения**

1. Разработка ПО

## Инструментарий, рабочая среда и инфраструктура

В процессе разработки программного обеспечения (ПО) участниками проекта применяются программные средства, представленные ниже:

Suricata написана на C/C++ – компилируемые и быстрые языки, поскольку исполняемые файлы, написанные на этих языках достаточно быстро позволяют осуществлять обработку трафика, поступающего на сетевой датчик.

В качестве компилятора используются GCC, g++.

GСС – компилятор для языков C, C++.

g++ – [компилятор](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B8%D0%BB%D1%8F%D1%82%D0%BE%D1%80) языка C++. Является частью [GCC](https://ru.wikipedia.org/wiki/GNU_Compiler_Collection).

Web-интерфейс системы написан на языке Python в качестве языка backend и стандартный стэк JavaScript/HTML/CSS.

Python применяется во всех остальных компонентах, так как имеет все необходимые драйвера и системы взаимодействия с необходимы процессами. Также в качестве основного framework используется Django, в свою очередь основанная на Python.

Python – интерпретируемый объектно-ориентированный язык программирования высокого уровня с динамической типизацией, автоматическим управлением памятью и удобными высокоуровневыми структурами данных, который используется в том числе и для разработки веб-приложений Язык поддерживает: структурное, объектно-ориентированное, функциональное и аспектно-ориентированное программирование. Python используется для создания плагинов и скриптов. Python потребляет меньше оперативной памяти и быстрее работает.

Также используются:

IDE – SublimeText с набором плагинов. Плагины включают в себя подсветку и проверку синтаксиса. Синхронизация с системой контроля версия Git.

IDE – система программных средств, используемая программистами для разработки ПО.

Sublime Text – [текстовый редактор](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BA%D1%81%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%80%D0%B5%D0%B4%D0%B0%D0%BA%D1%82%D0%BE%D1%80). Поддерживает [плагины](https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%B3%D0%B8%D0%BD) на языке программирования [Python](https://ru.wikipedia.org/wiki/Python).

GitLab – git репозиторий для исходного кода (система управления [репозиториями](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%BF%D0%BE%D0%B7%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%B9) кода для [Git](https://ru.wikipedia.org/wiki/Git)).

Git – распределенная [система управления версиями](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B2%D0%B5%D1%80%D1%81%D0%B8%D1%8F%D0%BC%D0%B8).

Bandit – статический анализатор кода. Используется для поиска общей угрозы безопасности в коде python.

JIRA / Confluence – [система отслеживания ошибок](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BE%D1%82%D1%81%D0%BB%D0%B5%D0%B6%D0%B8%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F_%D0%BE%D1%88%D0%B8%D0%B1%D0%BE%D0%BA) / [вики](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8)-система для внутреннего использования с целью создания единой базы знаний.

Отсутствие небезопасных синтаксических конструкций в JavaScript коде достигается путем проверки кода статическим анализатором eslint ([https://eslint.org](https://eslint.org/)) с использованием плагина eslint-config-scanjs. (<https://github.com/mozfreddyb/eslint-config-scanjs>).

Процессы конфигурационного управления ведутся с использованием GitLab - сайта и системы управления репозиториями кода для git.

Каждый разработчик клонирует исходный код продукта к себе на рабочую станцию, создает отдельную ветку git, в которой вносит изменения в продукт, после внесения изменения он заливает в свою ветку на git изменения и создает запрос (Merge Request) на влитие изменений в основную ветку, после этого изменения проверяются ведущим разработчикам и вливаются в основную ветку (рис. 1, 2).

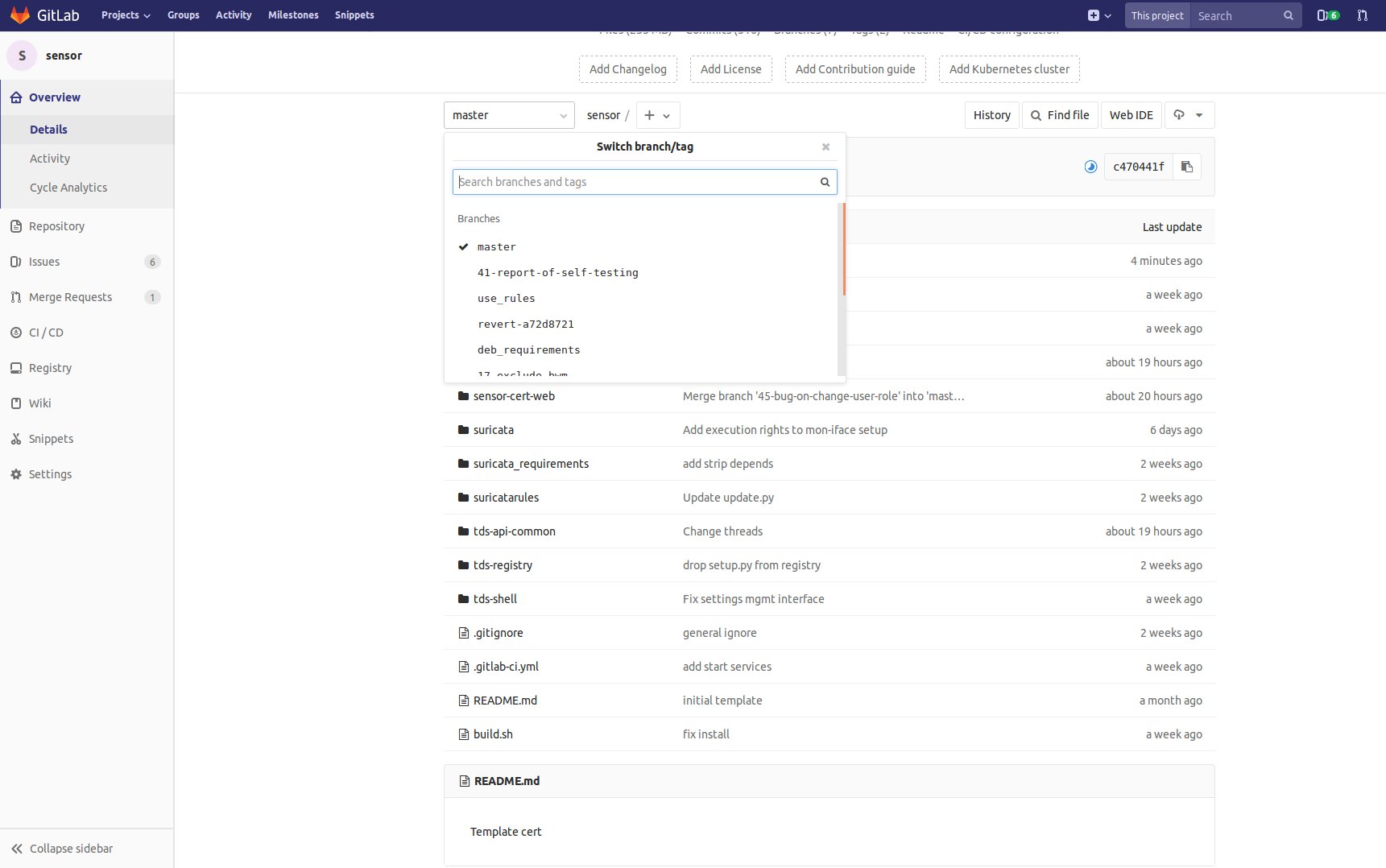


Рис. 1

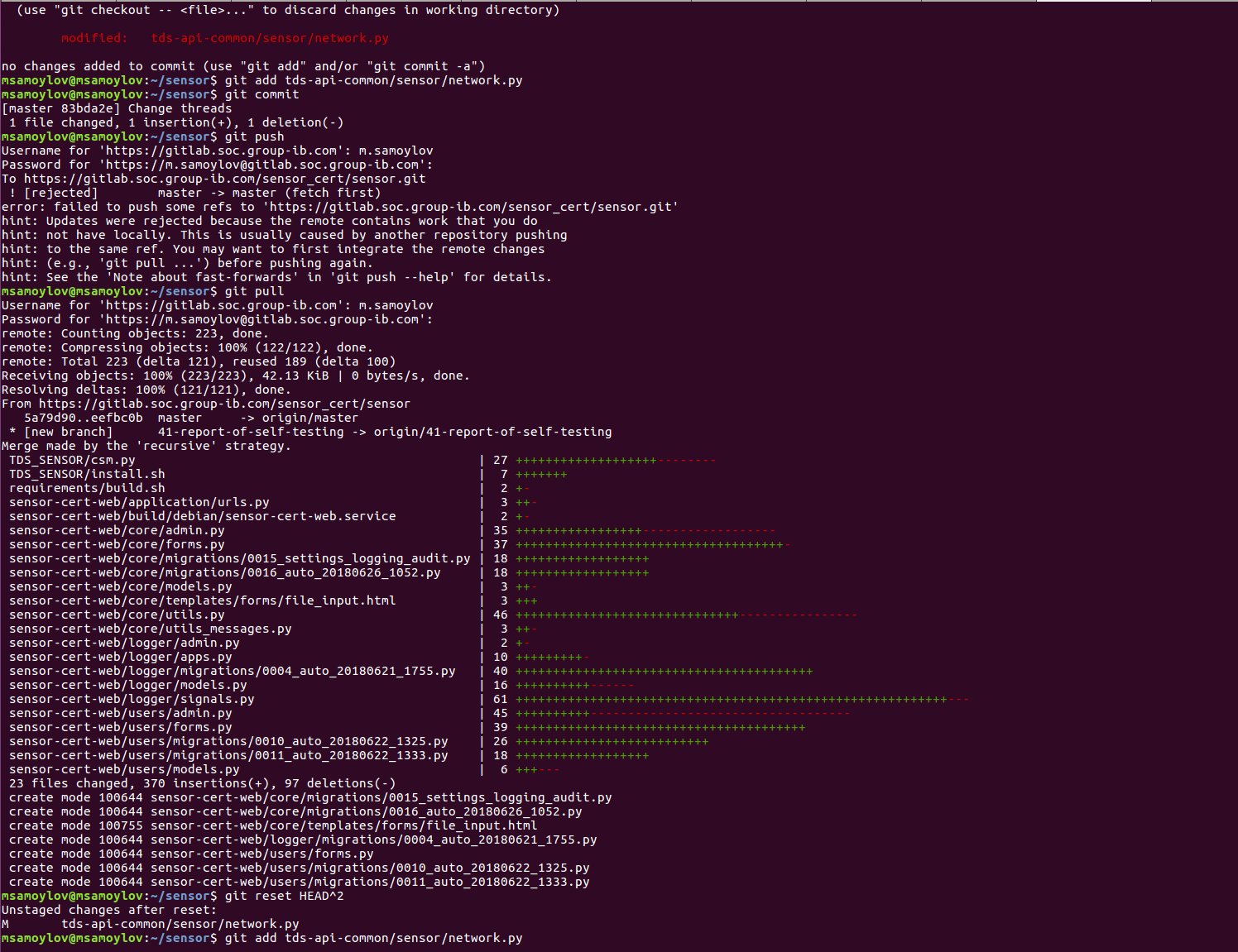


Рис. 2

Для исправления дефектов используется встроенная в GitLab система управления дефектами.

Эталонные исходные тексты и дистрибутив хранятся в электронном архиве на компьютере (сервере), а также на эталонном внешнем диске в закрытом сейфе архива.

Эталонные версии документов хранятся в электронном архиве компании на файловом сервере. Доступ к документам имеет только специалист по документации и менеджер проекта.

## Организация, распределение ответственности и взаимодействия

Состав проектной группы и распределение ответственности приведены в таблице 1.

Таблица 1 – Состав проектной группы

|  |  |
| --- | --- |
| Роль | Область ответственности |
| Менеджер проекта | Планирование деятельности команды проекта; управление проектом и организация внедрения; распределение работ и задач среди участников проекта и контроль их исполнения |
| Ведущий инженер программист | Контроль за соблюдением установленных правил управления конфигурацией и изменениями, обеспечение качественного выполнения работ в установленные сроки |
| Инженер-программист | Разработка, отладка и модификация программного продукта, интеграция результатов выполнения заданий, создание базовых версий |
| Специалист по тестированию | Тестирование программного продукта в соответствии с планом и процедурой тестирования, фиксирование найденных дефектов; ведение тестовой документации |
| Специалист по документации | Разработка документации на текущий проект |

## Контроль изменений

### Отработка запросов на изменение ПО

Запросы на исправления принимаются службой поддержки. После анализа и обработки запроса, выполняется передача описания проблемы разработчикам кода или предоставляются клиенту письменные инструкции по исправлению проблемы. Далее запросы передаются в отдел разработки. Обычно запросы клиентов связаны с невнимательным чтением руководств по эксплуатации изделия. Исправления кода учитываются в рамках следующих версий продукта.

### Отработка запросов на изменение документации

Рабочая документация может уточняться в процессе эксплуатации изделия. Запросы на изменении документации рассматриваются через службу поддержки и передаются руководителю проекта. Менеджер проекта рассматривает существенность замечания и принимает решение о необходимости внесения уточнения в рабочую документацию. При изменении документа производится его доработка специалистом по документации и исправленная версия документации в электронном виде передается заказчику. Уточненная документация может быть передана на носителе информации, по электронной почте или через официальный сайт производителя.

Изменение состава дистрибутива производится согласно «Регламенту разработки продукта» с указанием жизненного цикла развития продукта и назначенных ответственных за каждый этап жизненного цикла развития программного продукта.

### Контроль версий ПО и документации

На GitLab сохраняются актуальные и логически завершенные версии исходных текстов. Таким образом, ветка разработки проекта всегда актуальна и может быть использована для сборки и для последующих правок.

Документация на изделие хранится в электронном архиве компании. До утверждения документация находится в рабочем архиве с указанием номера версии документа, после утверждения документация переносится ответственным лицом в главный архив компании.

### Резервирование данных

Ежедневно создается резервная копия хранилищ и материалов проекта.

## Процедуры устранения недостатков

Основной процедурой устранения недостатков является сбор сведений о работе продуктов производства ООО «Группа АйБи ТДС» (в том числе программного комплекса Bot-Trek TDS) и устранение недостатков, выявленных уже в процессе эксплуатации. Компания имеет специализированное структурное подразделение – Технический Центр, который обеспечивает послепродажное обслуживание. В случае появления каких-либо проблем Заказчик обращается в Технический Центр по телефону или по электронной почте и оставляет заявку, заполненную по определенной форме. Каждая заявка проходит обязательную регистрацию в Техническом Центре.

Инженер Технического Центра, получивший заявку на устранение недостатков, производит ее первичное рассмотрение. На этом этапе перед ним ставится задача выяснить, решается ли проблема с помощью изменения настроек той версии программного обеспечения, которая стоит у Заказчика, или же она связана с наличием ошибки в самом программном обеспечении. В первом случае инженер подготавливает рекомендации по изменениям в конфигурации и направляет их Заказчику. В наиболее сложных случаях осуществляется выезд на место. Если проблему решить удалось, то диспетчер Технического Центра присваивает заявке статус завершенной. Для наиболее типичных случаев подготавливается краткое заключение с изложением способа решения и размещается в корпоративной базе знаний.

В случае невозможности решить проблему инженер подготавливает документ «Извещение об ошибке», и заявка в комплекте с этим документом направляется разработчику изделия. В «Извещении об ошибке» должны быть отражены: версия изделия, установленная у Заказчика, условия эксплуатации, при которых возникла ошибка, частота повторяемости ошибки, степень критичности для функционирования ПО, данные о среде функционирования (информационном окружении) изделия. Извещение направляется в Группу тестирования программного обеспечения. Инженер Технического Центра делает в базе заявок отметку о направлении Извещения и посылает Заказчику уведомление, что его проблема может быть решена только в новой версии.

Группа тестирования ведет свою собственную базу данных, где регистрируются поступающие извещения и, одновременно, свой раздел в корпоративной базе знаний. Получив извещение, группа тестирования анализирует ситуацию и производит сбор информации о таких же или похожих ситуациях. Как правило, инженер Технического Центра приглашается для консультаций. Все собранные сведения заносятся в специальную форму в базе данных группы тестирования. Если в результате анализа не удалось найти решение сразу, то принимается решение о моделировании ситуации на стенде.

В процессе моделирования главной является задача воспроизводства аварийной ситуации, т.е. поиск ответа на вопрос – для каких условий характерно возникновение аварии? Когда такие условия определены, то приглашается один или несколько разработчиков и им передается доступ к стенду и вся собранная информация. Обязанностью разработчика в данном случае будет устранить неисправность в программном обеспечении и представить группе тестирования новую версию.

Когда исправленная версия готова, группа тестирования осуществляет комплексные стендовые испытания. В ходе испытаний проверяется: во-первых, отсутствие аварийной ситуации после установки на стенд этой версии, а во-вторых, наличие у нее всех функциональных возможностей. Таким образом, принимается решение о том, что исправленная версия свободна от неисправности и процесс ее устранения не затронул остальную часть кода. После появления исправленной версии может быть принято решение о внесении необходимых изменений в документацию.

По завершении всех работ производится сохранение исправленных исходных кодов в системе управления конфигурацией и формируется индексация новой версии. Формируется новый дистрибутивный носитель и передается инженеру Технического Центра. Заказчику направляется уведомление, что обновления готовы, и с ним согласуется способ их отправки и установки.

Установка обновлений производится под контролем инженера Технического Центра, в особо сложных случаях инженер лично устанавливает обновление с выездом на место. После получения от Заказчика подтверждения о ликвидации проблемы, инженер Технического Центра присваивает заявке статус завершенной.

## Руководство по устранению недостатков

*Действия при получении сообщения о недостатке*

При получении сообщения о предполагаемом недостатке безопасности выполняются следующие действия:

1. Занесение проблемы в систему управления недостатками, с подробным описанием.
2. Назначается исполнитель по данной проблеме.
3. Исполнитель проводит анализ воспроизводимости проблемы, анализ исходного кода для выявления модуля и/или функции реализующей функцию безопасности, содержащую предполагаемый недостаток.
4. Проводится моделирование действий для воспроизведения предполагаемого недостатка безопасности.
5. В случае если проблема воспроизводится, проводится отладка для выявления места в исходном коде предполагаемого недостатка безопасности.
6. Вносится исправление в исходный код для исправления выявленного недостатка безопасности.
7. Осуществляется проверка разработчиком устранения недостатка безопасности.
8. Выполняется компиляция и сборка изделия для передачи на тестирование.
9. Изделие проходит тестирование.
10. В случае обнаружения дефектов исполнитель продолжает работу по устранению дефектов (пункты 3-8).
11. В случае успешного прохождения тестов исправление фиксируется в системе контроля версий в репозитории исполнителя, и отправляется запрос руководителю проекта на внесение изменений в главный репозиторий и сборку релизной версии.

*Способы, используемые для предоставления пользователям изделия необходимой информации о каждом недостатке безопасности*

Пользователи изделия информируются по электронной почте о выпуске обновлений изделия и устраненных в новых версиях недостатках. Сроки устранения недостатков определяются в каждом конкретном случае индивидуально, но не могут превышать 6 месяцев с момента занесения проблемы в систему управления недостатками.

*Способ связи пользователей изделия с разработчиком*

Связь пользователей с разработчиками осуществляется посредством электронной почты технической поддержки изделия: tds@group-ib.ru или через сайт компании.

2. Производство ПО

*Технический контроль*

Особо важные операции производства программных изделий подлежат техническому контролю.

К особо важным операциям производства программных изделий относятся:

1. Изготовление электронного носителя изделия с образа эталонной копии;
2. Проверка контрольной суммы;
3. Маркировка электронного носителя;
4. Изготовление комплекта эксплуатационной документации на электронном носителе;
5. Изготовление документов на бумажном носителе.

*Стендовые испытания*

Каждая новая версия изделия проверяется на стендовых испытаниях. Порядок и методика проведения стендовых испытаний определяется документом «Программа и методика испытаний».

Завершение испытаний каждой новой версии изделия оформляется протоколом. Новая версия принимается в эксплуатацию только в случае успешного проведения всех испытаний.

3. Поставка ПО

*Методы идентификации ПО*

В настоящем разделе описываются методы уникальной маркировки изделия и связанных с ним компонентов для обеспечения пользователей возможностью идентифицировать изделие и убедиться в том, что они используют сертифицированное изделие и сопутствующую документацию.

*Идентификация программного обеспечения*

Носитель, на котором поставляется изделие, маркируется следующей информацией:

1. Наименование (логотип) производителя.
2. Наименование изделия.
3. Обозначение изделия.
4. Серийный номер.
5. Контрольная сумма (приводится в формуляре на изделие).
6. Дата изготовления (приводится в формуляре на изделие).

*Идентификация документации*

Документация маркируется с использованием наименования документа и его обозначения в соответствии с требованиями ГОСТов серии ЕСПД (ГОСТ 19.101,   
ГОСТ 19.103).

Используемые методы маркировки документации позволяют однозначно идентифицировать документ. Пример маркировки документации приведен на рис. 3.

|  |
| --- |
| http://www.group-ib.ru/templates/group-ib/images/logo.gif  Программный комплекс Bot-Trek TDS  Формуляр  ГТДС.00001-01 30 01 |

Рис. 3 – Маркировка формуляра

*Процедура для поддержки безопасности при распространении версий изделия к местам использования*

Распространение версий изделия должно осуществляться на компакт-дисках или USB-накопителях, промаркированных в соответствии с «Техническими условиями».

Установку и обновление изделия должен выполнять уполномоченный администратор, ознакомившийся с эксплуатационной документацией.

Запись на электронные носители осуществляется строго по «Регламенту разработки» в компании – в соответствии с которым выпускающий редактор предоставляет уполномоченному администратору образ для записи на электронный носитель с контрольными суммами для сверки записываемого дистрибутива.

*Процедура обнаружения расхождения между оригиналом и полученной версией*

Проверка внешнего вида

Порядок проверки внешнего вида приведен ниже.

1. Убедиться, что изделие поставлено на компакт-диске.
2. Убедиться, что маркировка футляра компакт-диска выполнена печатным способом и содержит наименование, обозначение, серийный номер изделия, контрольную сумму и дату изготовления.
3. Убедиться, что маркировка компакт-диска выполнена печатным способом и содержит наименование, обозначение, серийный номер изделия, контрольную сумму и дату изготовления.

Проверка комплектности

Убедиться, что изделие содержит:

* компакт-диск с записанным на нем дистрибутивом;
* копию сертификата на бумажном носителе;
* формуляр на бумажном носителе;
* комплект эксплуатационной документации на электронном носителе.

*Проверка соответствия, полученного потребителем изделия, сертифицированному*

Проверка изделия проводится сверкой контрольной суммы дистрибутива изделия со значением, указанным в соответствующем разделе формуляра и на этикетке компакт-диска.

Методика проверки контрольной суммы приведена в Формуляре и Технических условиях на изделие.

*Процедура обновления ПО*

Обновление ПО должно осуществляться уполномоченным администратором после получения официального уведомления об обновлении ПО.

Процедура обновления описана в Руководстве администратора.

*Действия при обнаружении несоответствий*

В случае обнаружения несоответствий при проведении проверки изделия необходимо обратиться к производителю.

4. Обновление БРП

*Фиксация появления нового типа вторжения*

Обновление БРП является одним из важных аспектов эффективного функционирования системы обнаружения вторжения.

Поставщики БРП осуществляют постоянный мониторинг появления новых сетевых атак. Обнаруженные атаки локализуются, и на их основе формируется ежемесячное обновление. Разработчик ежедневно осуществляет загрузку, проверку и анализ обновлений от Поставщиков БРП.

Кроме того, Разработчик независимо от Поставщиков БРП осуществляет постоянный мониторинг появления новых сетевых угроз. На основании проведенного мониторинга Разработчик может пополнить обновленную БРП собственными правилами, а также модифицировать полученные от Поставщика БРП правила.

Существует два механизма, которые используются для обнаружения новых типов вторжений:

* исследовательские работы, выполняемые сотрудниками предприятия- производителя (ООО «Группа АйБи ТДС) сертифицированного Программного комплекса Bot-Trek TDS (далее по тексту – изделие);
* акты рекламации, поступающие от пользователей сертифицированного изделия.

Исследовательские работы предусматривают анализ открытых источников, данных сети «Интернет», содержащих сведения об уязвимостях программного обеспечения.

При получении акта рекламации выполняется анализ вторжения, описание которого не присутствует в текущей БРП. Выполняются тестовые атаки и исследования на стенде предприятия-разработчика для изучения атаки и формирования ее признаков.

По результатам изучения нового типа вторжения устанавливается его актуальность и признаки, которые могут быть использованы для его обнаружения.

*Процедура уведомления об обновлении БРП*

Разработчик с использованием электронных почтовых сообщений направляет в адрес организаций, эксплуатирующих сертифицированное изделие «Информационный манифест», содержащий краткое описание нового типа вторжения и декларацию факта обновления базы решающих правил для обнаружения нового типа вторжения в течение 1 месяца.

Разработчик ведет учет списка атак в документе «Описание новых типов вторжений». Для каждого нового типа вторжения указывается следующая информация: идентификатор, дата внесения в перечень, идентификатор документа «Информационный манифест», описание атаки и ее признаки, статус (изменение в БРП внесено/не внесено). Момент появления нового типа вторжения фиксируется в документах «Информационный манифест» и «Описание новых типов вторжений».

Предприятие-производитель ведет учет покупателей сертифицированного изделия. Выполняется регистрация следующей информации: наименование организации, адрес организации, номер знака соответствия, контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование изделия). Уведомление пользователей о выпуске обновления БРП выполняется с использованием рассылки электронных почтовых сообщений.

*Процедура доставки обновлений БРП*

Процедура предоставления обновлений БРП в общем случае выглядит следующим образом:

1. загрузка обновлений с серверов Поставщика БРП, предоставляющих обновления БРП для Разработчика;
2. проверка целостности загруженных обновлений;
3. обработка БРП;
4. тестирование работоспособности изделия с обновленными правилами;
5. оценка влияния обновленных БРП на функции безопасности изделия;
6. подготовка к отгрузке обновленных БРП:

* формирование архива с БРП;
* формирование файла с контрольной суммой БРП;
* формирование файла с временной меткой;

1. отправка файлов с архивом обновлений на электронные почтовые адреса зарегистрированным организациям.

*Процедура контроля целостности обновлений БРП*

Обновления БРП, успешно прошедшие контроль влияния на безопасность изделия, отправляются в виде файла архива на электронные почтовые ящики зарегистрированных организаций, эксплуатирующих изделие. Контрольная сумма архива, также высылается электронным сообщением. После получение обновления БРП пользователь имеет возможность выполнить контроль его целостности с использованием механизма контрольного суммирования.

5. Обновление изделия

При выпуске обновления (исправление ошибок, улучшение в функционировании компонентов, добавление новых функций безопасности информации или изменение в имеющихся функциях безопасности информации), после испытания средства защиты информации (самостоятельно или с привлечением испытательной лаборатории), производитель изделия с использованием электронных почтовых сообщений направляет в адрес организаций, эксплуатирующих сертифицированное изделие, уведомление о необходимости применения обновления.

После согласования испытаний в ФСТЭК России производитель предоставляет пользователю изделия:

* + бумажную заверенную копию обновленного сертификата (если обновлялся) и извещение о внесении изменений в формуляр;
  + ссылку на файл дистрибутива для обновления версии программного обеспечения;
  + ссылку на архив с электронными копиями измененных эксплуатационных документов.

Сведения о контрольных суммах файла дистрибутива и файла с архивом эксплуатационных документов высылается в бумажном виде в адрес организации, эксплуатирующей изделие, в виде уведомления, подписанного руководителем предприятия – производителя изделия и скрепленного печатью.

Верификация обновления осуществляется путем расчета контрольных сумм файлов дистрибутива с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» по алгоритму «ГОСТ Р 34.11-94» и их сравнения со значениями, указанными в уведомлении.

После верификации файлов дистрибутива изделия пользователю изделия надлежит провести верификацию файла с электронными копиями измененных эксплуатационных документов и сравнить контрольную сумму файла с архивом со значением, указанным в уведомлении.

В разделе формуляра «Особые отметки» необходимо произвести запись о получении и применении файлов обновления.

Предоставленный в электронном виде формуляр должен быть распечатан, в разделе «Особые отметки» должна быть сделана запись о замене формуляра со знаком соответствия системы сертификации на обновленный формуляр. На замененном формуляре следует сделать запись: «Формуляр аннулирован. Знак соответствия системы сертификации (голографическая наклейка) действителен». Замененный формуляр следует хранить вместе с обновленным для сохранения знака соответствия системы сертификации.

При возникновении проблем с установкой или работой изделия необходимо обратиться за помощью в службу технической поддержки по телефону в Москве:   
+7 (495) 984-33-64.

6. Устранение уязвимостей

Процедура устранения уязвимостей изделия должна обеспечивать возможность обновления программного обеспечения изделия для устранения актуальных уязвимостей, имеющих критический характер для функционирования изделия. Устранение уязвимостей должно производиться производителем изделия с использованием организационно-технических процедур представленных ниже.

Производитель периодически, не реже одного раза в месяц, должен проводить поиск известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях. В качестве общедоступных источников в первую очередь должна использоваться база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), а также следующие дополнительные источники:

* + банк данных уязвимостей CVE (http://cve.mitre.org/);
  + банк данных уязвимостей Tenable research team (https://www.tenable.com/sc-dashboards);
  + и другие.

Поиск информации в базах данных по уязвимостям изделия проводят с целью проверки соответствия изделия требованиям, указанным в документах «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Производитель должен провести анализ выявленных уязвимостей изделия.

При анализе уязвимостей необходимо учитывать следующие критерии:

* + тип ошибки;
  + версию программного обеспечения изделия, подверженную уязвимости;
  + уровни опасности уязвимости:
  + критическая (Critical);
  + высокая (High);
  + средняя (Medium);
  + низкая (Low);
  + информацию об устранении.

В случае выявления информации об уязвимости изделия из различных источников и отсутствия информации об этой уязвимости в базе данных уязвимостей (далее по тексту БДУ), производитель предоставляет информацию о данной уязвимости в ФСТЭК России для размещения в БДУ.

При выявлении уязвимостей изделия производитель должен осуществить следующие мероприятия:

* + подготовить дистрибутив с устраненными уязвимостями;
  + уведомить пользователей об уязвимостях изделия путем рассылки электронных почтовых сообщений.
  + довести информацию до пользователей изделия об организационно-технических мерах по устранению в нем уязвимостей;
  + производитель оповещает пользователей изделия о необходимости установки обновленной версии изделия;
  + производитель обеспечивает гарантированную доставку пользователям изделия файла с обновленной версией изделия;
  + пользователь изделия обновляет программное обеспечение с соответствующими отметками в разделах формуляра;
  + в случае внесения в изделие изменений, связанных с устранением уязвимостей или обновлением баз данных, необходимых для реализации функций безопасности изделия, производитель обязан провести испытания средства защиты информации самостоятельно или с привлечением испытательной лаборатории;
  + по результатам проведенных испытаний изделия в связи с внесением в него изменений производитель представляет материалы испытаний в ФСТЭК России;
  + после согласования материалов испытаний в ФСТЭК России производитель должен предоставить пользователю изделия:
  + бумажную заверенную копию обновленного сертификата (если обновлялся) и извещение о внесении изменений в формуляр;
  + ссылку на файл дистрибутива для обновления версии программного обеспечения;
  + ссылку на архив с электронными копиями измененных эксплуатационных документов.

Сведения о контрольных суммах файла дистрибутива и файла с архивом эксплуатационных документов высылается в бумажном виде в адрес организации, эксплуатирующей изделие, в виде уведомления, подписанного руководителем предприятия – производителя изделия и скрепленного печатью.

* + в случае невозможности устранения уязвимостей изделия, в том числе путем применения обновления, производитель разрабатывает ограничения по применению изделия, которые незамедлительно доводит до испытательной лаборатории;
  + если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, производитель незамедлительно и гарантированно с подтверждением доводит его до пользователей;
  + производитель вносит необходимые изменения в эксплуатационную документацию и направляет ее совместно с заключением испытательной лаборатории в ФСТЭК России. Пользователи реализуют указанное ограничение по применению изделия;
  + если пользователь не может реализовать ограничение по применению изделия он прекращает его применение;
  + если уязвимость не устраняется путем установления ограничений по применению, производитель незамедлительно и гарантированно с подтверждением сообщает об этом всем пользователям и в ФСТЭК России. Пользователи прекращают применение изделия.