АО «НТЦ ИТ РОСА»

Система управления средой виртуализации ROSA Virtualization

Описание процедур устранения недостатков

Листов 16

АННОТАЦИЯ

Данный документ содержит описания процедуры отслеживания недостатков безопасности Системы управления средой виртуализации ROSA «Virtualization» (далее по тексту — СУСВ или изделие), корректирующих действий по их устранению и процедуры доведения информации об этих действиях до пользователей изделия.

В документе представлена информация, удовлетворяющая требованиям компонента доверия ALC_FLR.1.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. Идентификация документа

Название: СУСВ ROSA «VIRTUALIZATION». Описание процедур устранения недостатков.

Версия: 1.0.

Идентификация объекта оценки (ОО): Система управления средой виртуализации ROSA «Virtualization».

1.2. Назначение документа

Настоящий документ содержит:

- документацию процедур устранения недостатков изделия;
- регламент процедуры отслеживания всех известных недостатков безопасности в каждом релизе изделия;
- регламент применения в компании ООО «НТЦ ИТ РОСА» процедур описания каждого недостатка безопасности с точки зрения его сути и последствий;
- регламент идентификации корректирующих действий с целью оценки возможности применения процедур устранения недостатков безопасности;
- перечень корректирующих действий, необходимых для устранения недостатков безопасности;
- перечень методов, используемых для оповещения пользователей изделия о недостатках изделия;
- перечень методов, используемых для оповещения пользователей изделия об устранении недостатков изделия, с приведением материалов исправлений и руководств по внесению исправлений.

2. ПРОЦЕДУРЫ УСТРАНЕНИЯ НЕДОСТАТКОВ ИЗДЕЛИЯ

2.1. Документация процедур устранения недостатков изделия

В соответствии с требованиями документа «РСЮК.ДП.003-2019 Разработка программного изделия» в ООО «НТЦ ИТ РОСА» разработана процедура устранения недостатков, которая в данном случае совпадает с технологией выпуска обновлений и процедурой оперативной доработки, описанными в документе «Описание процедуры предоставления обновлений для проведения внешнего контроля» РСЮК.10201-01 93 07. Технология процедуры устранения недостатка приведена на рисунке 3 и в целом аналогична процедуре «Оперативная доработка изделия в ходе эксплуатации», описанной в «РСЮК.ДП.003-2019 Разработка программного изделия».

Процедура устранения недостатков начинается с начала оперативной доработки, инициированной анализом недостатка, выявленного в ходе проведения процедур отслеживания. Общая схема процедуры оперативной доработки приведена на рисунке 1.

Рисунок 1

Схема процесса «Разработка технического решения» приведена на рисунке 2.

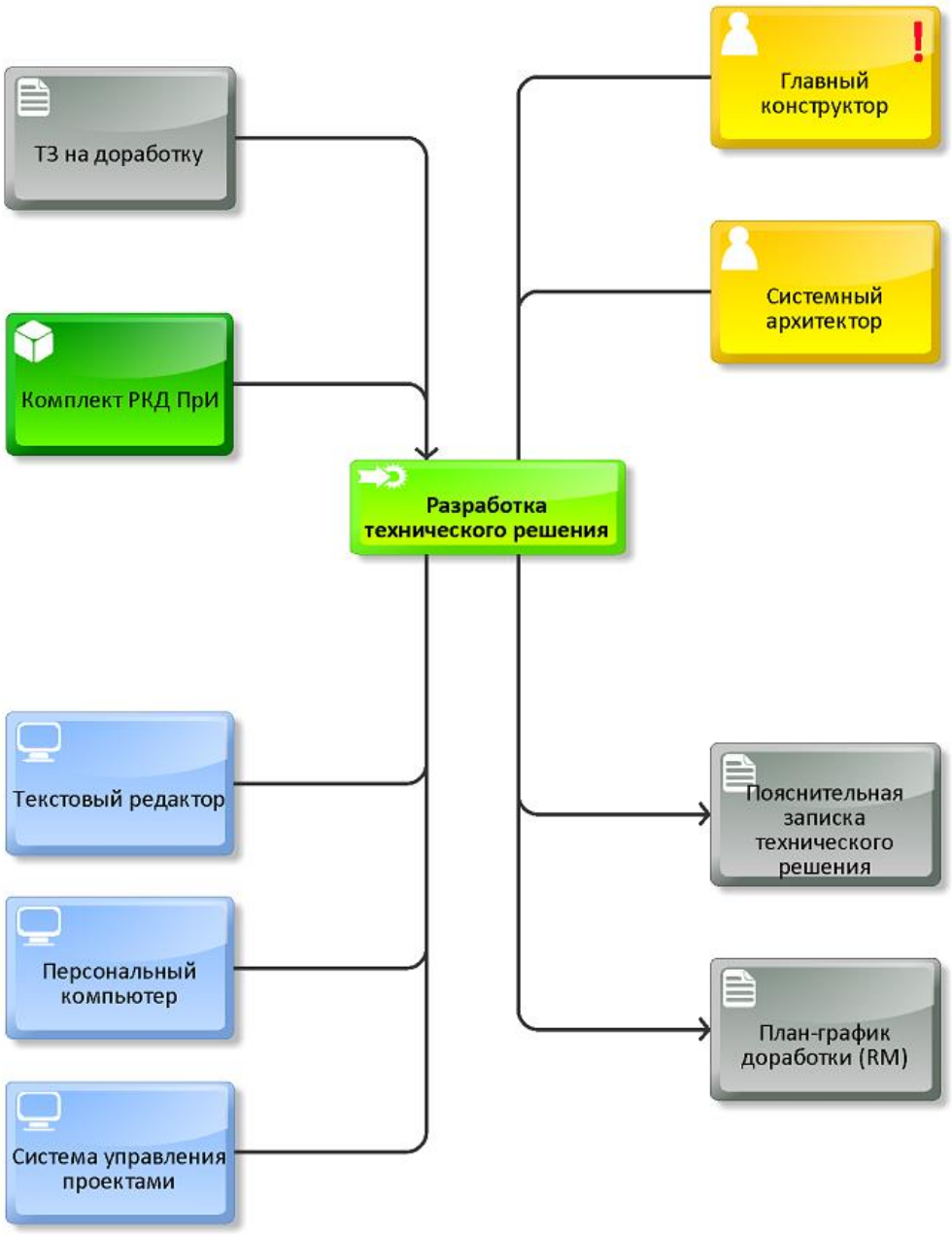

Рисунок 2

Схема процесса «Устранение недостатка (доработка изделия)» приведена на рисунке 3.

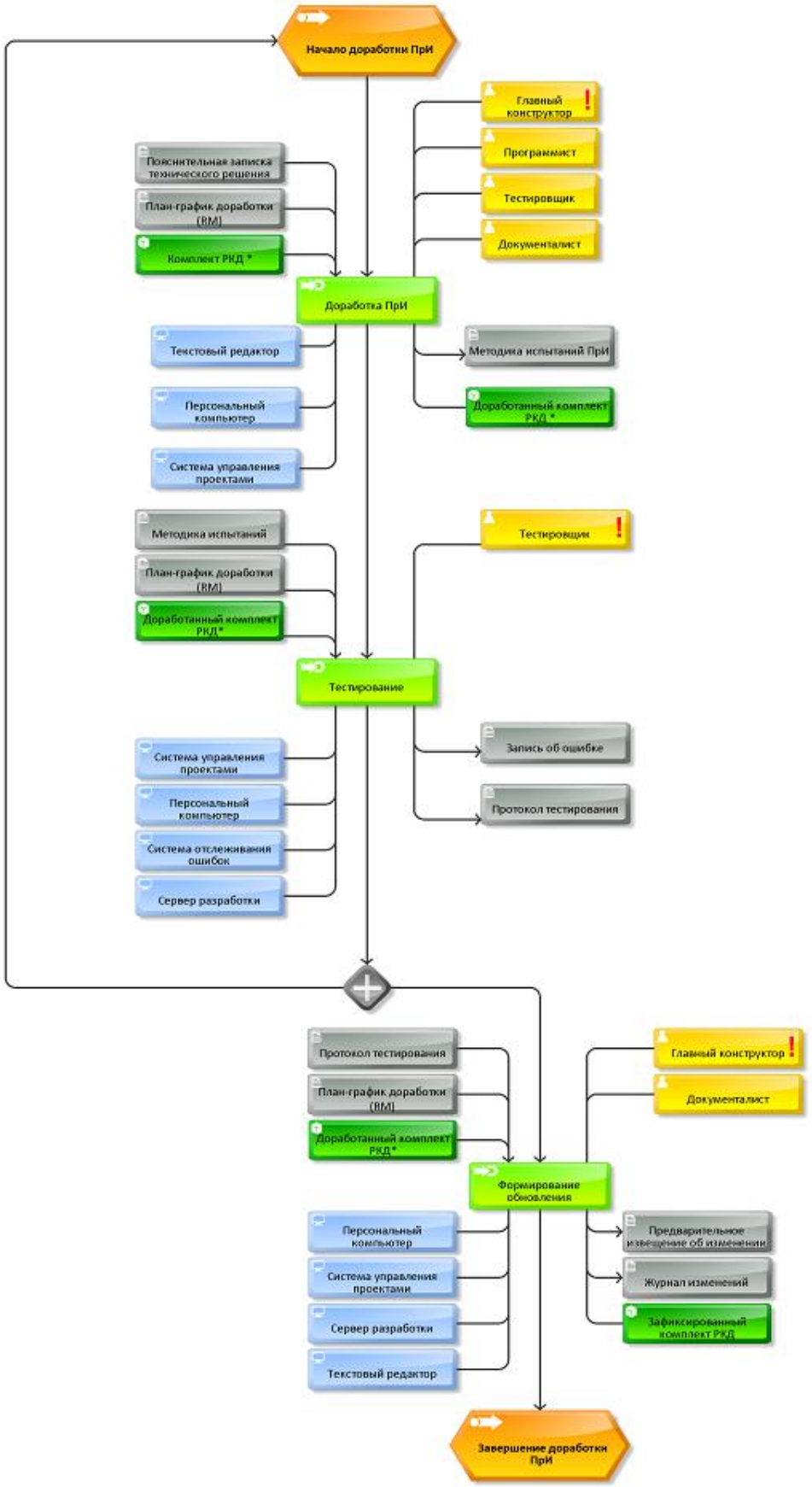

Рисунок 3

2.2. Регламент процедур отслеживания недостатков изделия

Отслеживание недостатков изделия производится в том числе на основании методик, изложенных в документе «Свидетельство анализа уязвимостей» РСЮК.10201-01 93 08. Помимо этого используются другие методы отслеживания, перечисленные ниже, а именно:

1) Отслеживание недостатков путем проверки наличия уязвимостей на основании информации из общедоступных баз данных уязвимостей. Предполагает поиск информации об уязвимостях конкретной СУСВ семейства ROSA «VIRTUALIZATION» и аналогичных СУСВ в следующих источниках:

- в базе данных уязвимостей в составе банка данных угроз безопасности информации (www.bdu.fstec.ru);
- на интернет-ресурсах компании-разработчика (https://www.rosalinux.ru/support/, http://wiki.rosalab.com/ru/index.php/Security_Bulletin, http://wiki.rosalab.ru/ru/index.php/%D0%9A%D0%B0%D1%82%D0%B5%D0%B3%D0%BE%D1%80%D0%B8%D1%8F:Security_Advisories)
- в иных источниках и средствах массовой информации (www.securitylab.ru, www.exploit-db.com, cve.mitre.org, nvd.nist.gov, www.cvedetails.com, www.kb.cert.org, vigilance.fr, technet.microsoft.com/en-us/security/bulletin и др.).

В качестве идентификаторов для поиска известных (подтвержденных) уязвимостей используются: название, версия, архитектура СУСВ ROSA «VIRTUALIZATION»; наименование компании-разработчика (ООО «НТЦ ИТ РОСА»).

Для поиска известных (подтвержденных) уязвимостей изделия выполняютмя запросы вида:

- «уязвимости СУСВ ROSA VIRTUALIZATION»;
- «уязвимости НТЦ ИТ РОСА»;
- «vulnerability Rosa».

Для поиска потенциальных уязвимостей изделия выполняются запросы вида:

- «уязвимости Linux»;
- «уязвимости ядра Linux»;
- «Linux kernel vulnerability».

2) Отслеживание недостатков при помощи сканера уязвимостей OpenVAS с подключенными модулями следующих БД уязвимостей:

- NVT;
- CVE;
- CPE;

- OVAL Definitions;
- CERT-Bund advisores;
- DFN-CERT advisores.

Обновление БД уязвимостей производится регулярно (не реже раза в неделю).

3) Отслеживание недостатков средством АВЗ, входящим в комплект поставки изделия, — программой clamav. Перед проверкой производится полное обновление доступных баз средства АВЗ. Изделие проверяется в варианте установки «по умолчанию»; также проверяются все файлы, расположенные на установочном носителе (носителях) изделия. Обновление баз средства АВЗ производится не реже 1 раза в неделю.

4) Отслеживание недостатков осуществляется коммерческим программным средством с открытым исходным кодом Cisofy Lynis (https://cisofy.com/lynis/).

5) Отслеживание недостатков осуществляется путем тестирования (проверки) изделия при проведении операций жизненного цикла в рамках документа «РСЮК.ДП.003-2019 Разработка программного изделия» в ООО «НТЦ ИТ РОСА».

6) Отслеживание недостатков осуществляется путем получения и анализа рекламаций, а также других материалов информационного характера, поступающих от пользователей (потребителей, заказчиков) изделия в адрес предприятия заявителя (производителя) и/или разработчика. А также материалов, поступающих из уполномоченных (лицензированных) органов и юридических лиц РФ в области контроля качества и информационной безопасности в адрес предприятия заявителя (производителя) и/или разработчика.

2.3. Регламент применения процедур идентификации недостатков изделия

Регламент применения процедур идентификации недостатков безопасности изделия учитывает (но не реализует в полном объеме) правила описания уязвимостей, изложенные в документе «ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».

Информация о выявленном недостатке и его описание публикуются в виде информационного бюллетеня безопасности на общедоступных ресурсах предприятия разработчика по следующим адресам:

https://www.rosalinux.ru/support/

Каждый такой бюллетень безопасности имеет уникальный идентификатор вида «ROSA-SA-01-02-03.456», разделенный дефисами и точкой, где:

- первые 4 буквы (ROSA) идентифицируют разработчика;
- вторые 2 буквы (SA) идентифицируют тип публикации — бюллетень безопасности (Security Advisory);
- первая группа цифр содержит год публикации (после 2000 года);

- вторая группа цифр указывает на месяц года;
- третья группа цифр указывает на день (число);
- после точки нумеруется по порядку конкретный бюллетень за конкретный день (при необходимости, если за этот день было выявлено несколько недостатков).

При описании недостатка учитывается и публикуется следующее:

- уникальный идентификатор (номер) бюллетеня безопасности вида *«ROSA-SA-17-12-23.001*»;
- категория статьи на ресурсе, указывающая, что это бюллетень безопасности (неизменна);
- описание недостатка (уязвимости) вида: *«Возможность компрометации аутентификационной информации пользователя при прохождении аутентификации»*;
- перечень продукции (программного обеспечения) разработчика, к которой относится недостаток (уязвимость), вида: *«СУСВ ROSA VIRTUALIZATION»*;
- степень критичности недостатка с точки зрения разработчика. Всего 5 степеней, от наиболее значимой к наименее значимой: *«Критическая», «Высокая», «Средняя», «Низкая», «Незначительная»*;
- текущий статус недостатка (уязвимости), позволяющий оперативно отслеживать информацию о ходе его (ее) устранения. Всего 5 степеней: *«Устранена», «Нейтрализована», «Информация проверяется», «Ведутся работы по устранению (нейтрализации)», «Не устранена»*;
- список ПО (пакетов, образов, файлов), необходимого к установке в случае устранения недостатка, вида: *«gnome-shell-3.14.4-53.res7c.4.x86_64.rpm»*;
- перечень мероприятий и рекомендаций по нейтрализации недостатка (если применимо), в случае, если устранение по каким-либо причинам невозможно, либо у потребителя (пользователя) нет оперативной необходимости устранять уязвимость;
- данные (в виде гиперссылок) о наличии информации об уязвимости (недостатке) в общедоступных базах данных уязвимостей (если применимо) вида: *«BDU:2016-01584*» или *«CVE-2013-0221*» и т.п.;
- (опционально) дополнительная информация, позволяющая классифицировать недостаток по типу/классу, или иная информация, отражающая, например, способ эксплуатации недостатка.

Для удобства пользователей (потребителей) реализован сводный перечень уязвимостей, доступный по адресу: http://wiki.rosalab.com/ru/index.php/Security_Bulletin. Кроме того, предусмотрены механизм поиска и возможность подписки на RSS-канал с

целью наиболее оперативного информирования пользователей (потребителей) о недостатках изделия.

2.4. Регламент идентификации корректирующих действий

Для однозначной идентификации корректирующих действий используется процесс, описанный в документе «РСЮК.ДП.003-2019 Разработка программного изделия» в ООО «НТЦ ИТ РОСА». Процесс идентификации можно представить в виде схем, приведенных на рисунках 4 и 5.

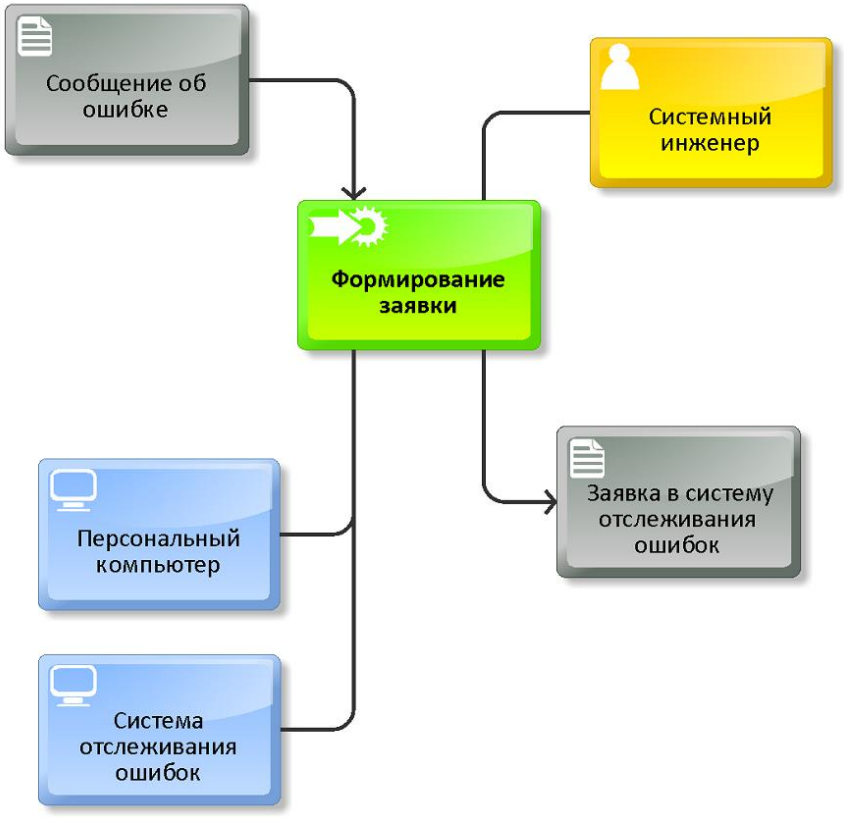

Рисунок 4 — Схема процесса «Формирование заявки»

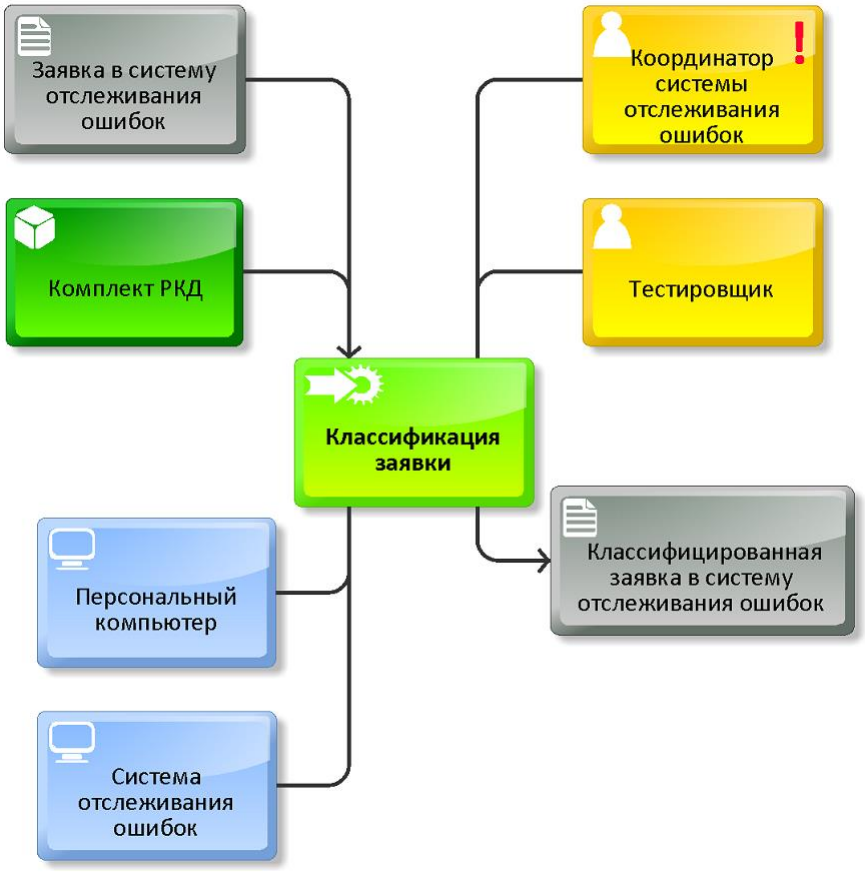

Рисунок 5 — Схема процесса «Классификация заявки»

Кроме того, при идентификации корректирующих действий обязательно учитывается тип недостатка (уязвимости). Например:

- уязвимость (недостаток) кода;
- уязвимость (недостаток) реализации;
- ошибка компилятора (интерпретатора);
- ошибка конфигурирования;
- ошибка документирования;
- ошибка среды выполнения;
- манипулирование данными и др.

2.5. Перечень корректирующих действий

Реализация корректирующих действий подразумевает, что после выполнения процедуры идентификации корректирующих действий будет учтен тип предпринимаемых действий для исправления недостатка (уязвимости). В перечень корректирующих действий входят:

- уведомление пользователей (потребителей) изделия о недостатке (уязвимости) изделия;

- изменение программной документации (в т. ч. текста программы);
- изменение среды выполнения изделия;
- изменение эксплуатационной документации на изделие;
- введение ограничений на применение изделия;
- введение дополнительных мер защиты, которые необходимо предпринять при эксплуатации изделия.

2.6. Методы оповещения пользователей о недостатках изделия

К методам оповещения пользователя относятся следующие:

1) Оповещение пользователей через официальные ресурсы компании-разработчика:
   - https://www.rosalinux.ru/support/
2) Оповещение пользователей о выходе обновлений электронным письмом. Официальный адрес электронной почты предприятия-разработчика — support@rosalinux.ru.
3) Официальное оповещение пользователя письмом в установленном порядке делопроизводства, принятым на территории Российской Федерации.

Также потребитель может самостоятельно получить информацию о выходе обновлений через службу технической поддержки предприятия-производителя/предприятия-разработчика по тел. +7 495 137-88-66 или по электронной почте support@rosalinux.ru

2.7. Методы оповещения пользователей об устранении недостатков изделия

Методы оповещения пользователя об исправлении изделия в основном совпадают с методами оповещения пользователя о недостатках изделия. Также в перечень этих методов входит:

4) Получение обновлений из официального репозитория компании-разработчика (заявителя, производителя), автоматизированного с учетом наличия в изделии менеджера пакетов (управления программ).

Для доступа к репозиториям ПО может требоваться персонифицированный ключ, ограничивающий получение обновлений (исправлений) третьими лицами. Персонифицированные ключи поставляются потребителю вместе с получением лицензии на использование изделия при покупке (получении) изделия в установленном порядке либо при тестировании. Персонифицированные ключи также могут в любой момент быть отозваны предприятием-разработчиком при нарушении пользователем порядка эксплуатации изделия.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АВЗ — антивирусная защита.

СУСВ — система управления средой виртуализации.

ПО — программное обеспечение.

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего	№	Входящий №	Подп.	Дата
	измененных	замененных	новых	аннулированных					