



Инфраструктура и процессный подход для обеспечения качества и безопасности операционной системы специального назначения

Докладчики:

Фокин Максим Сергеевич

Тележников Владимир Юрьевич

Операционная система специального назначения «Astra Linux Special Edition» (далее по тексту – операционная система)



Операционная система обеспечивает защиту любой информации, с любым грифом ограничения доступа:

Коммерческая тайна

Конфиденциальная информация

Государственная тайна:

- гриф «секретно»
- гриф «совершенно секретно»
- гриф «особой важности»

И другие

Операционная система функционирует на различных типах устройств с различными процессорными архитектурами



Смартфоны



Планшеты



Ноутбуки



Рабочие станции



Тонкие клиенты



Защищенные спецрешения



Серверы



Мейнфреймы

Российские процессоры

Baikal

Эльбрус

Процессорная архитектура

X86-64

Power

ARM

Эльбрус

Основные направления формирования методологии разработки безопасного системного ПО

Развитие нормативной базы разработки и обеспечения доверия к системному ПО

Периодический анализ уязвимостей в ПО


Моделирование угроз разрабатываемого ПО

Направления формирования методологии

Разработка и верификация формальных моделей управления доступом

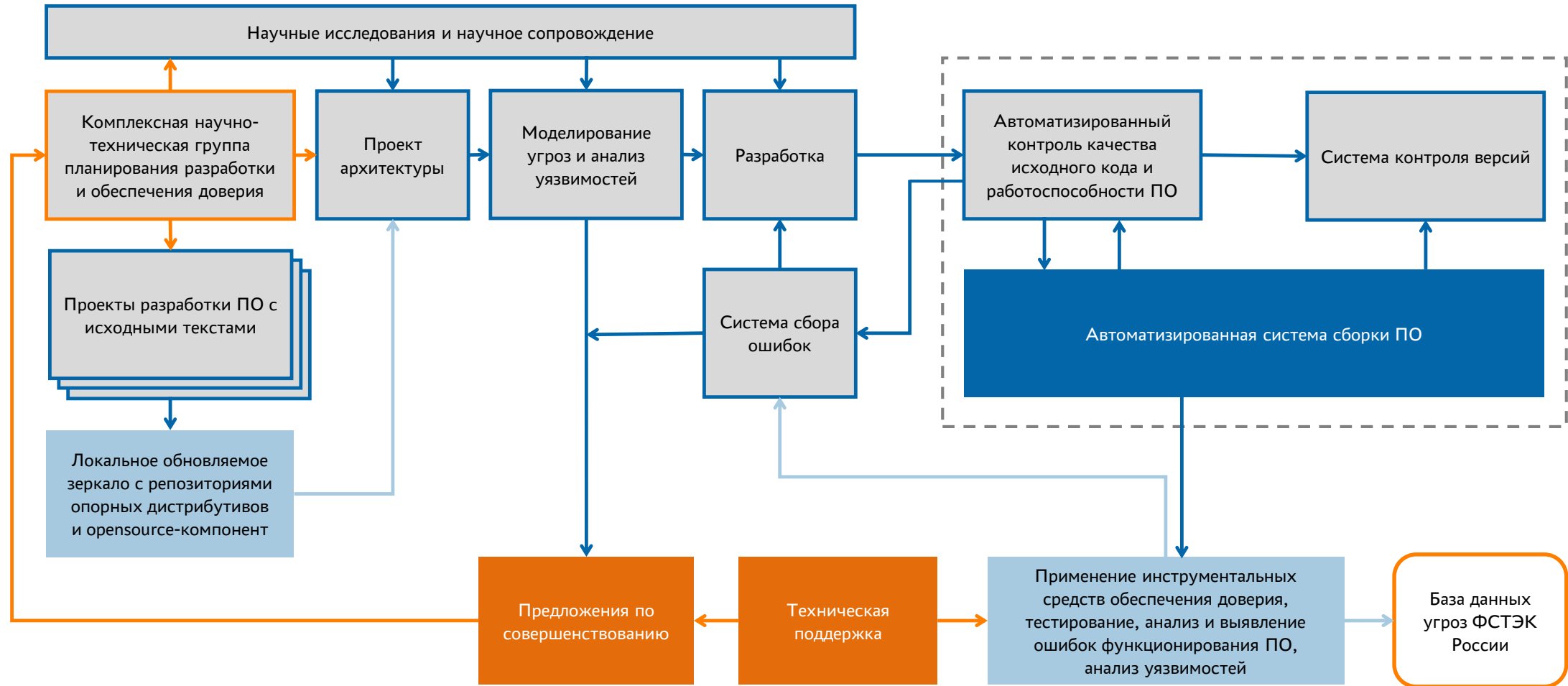
Сбор и аналитическая обработка результатов анализа программного кода системного ПО

Статический и динамический анализ программного кода системного ПО

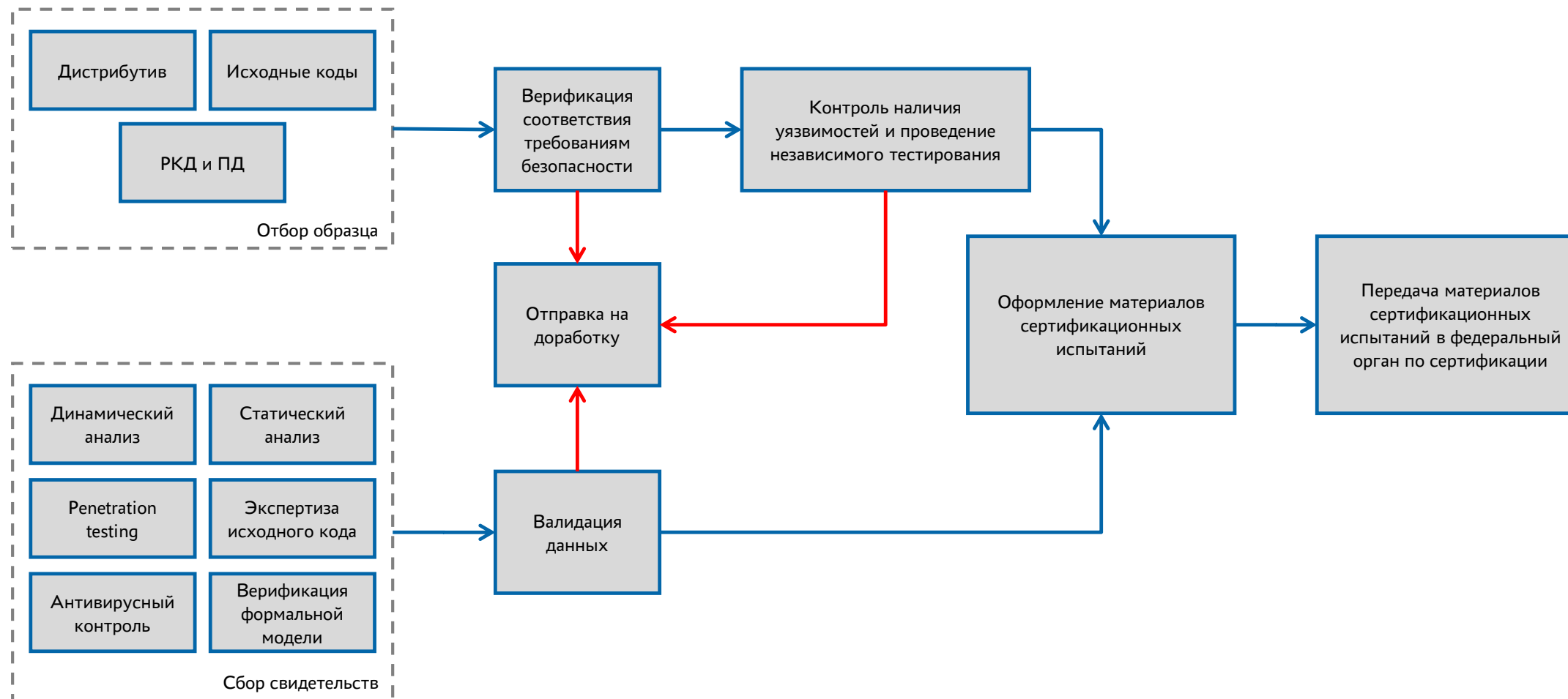
The background is a solid blue color with a subtle, intricate pattern of white lines and dots, resembling a circuit board or a network diagram. In the center-right, there is a faint, glowing white outline of a padlock, which is slightly tilted. The overall aesthetic is technical and digital.


Процессное обеспечение качества и безопасности операционной системы

Процессы обеспечения доверия и контроля качества операционной системы



Проведение сертификационных испытаний





**Научное и техническое сопровождение
обеспечения качества и безопасности
операционной системы**

Инструмент поиска уязвимостей в ПО



VULSCAN | Проекты | Бюллетени | Базы обновлены: 13.02.2022 23:22 | Добро пожаловать, admin! | Выйти

Сканер уязвимостей

Инструмент сканирования пакетов или программ по открытым источникам баз данных уязвимостей

[Создать проект](#)

Таблица всех проектов

| # | Название проекта | Последнее сканирование | Статус | Уязвимости |
|---|------------------|-------------------------|----------------|------------|
| 2 | новый проект | 17 января 2022 г. 16:39 | Отчет готов | 551 |
| 5 | Test_1 | 19 ноября 2021 г. 11:07 | Просканировано | 0 |
| 6 | test_1 | 17 ноября 2021 г. 19:27 | Отчет готов | 173 |
| 7 | Test_2 | 17 ноября 2021 г. 19:27 | Отчет готов | 2243 |

VULSCAN | Проекты | Бюллетени | Базы обновлены: 13.02.2022 23:22 | Добро пожаловать, admin! | Выйти

2

Дата создания проекта: 7 декабря 2021 г.
Дата начала последнего сканирования: 14 января 2022 г. 18:53
Дата окончания последнего сканирования: 14 января 2022 г. 19:05

Добавление бюллетеней

Добавление обновлений безопасности с закрытыми уязвимостями к следующему сканированию

Базовые:

Пользовательские:

Запуск сканирования

Проведено сканирований: 5

[Запустить сканирование](#)

Дополнительно

Скачивание архива полного отчета или предоставление доступа к результатам проекта

[Скачать отчет](#)

Статус сканирования

Дополнительная информация о сканировании

Статус сканирования: Просканировано

100%



VULSCAN | Проекты | Бюллетени | Базы обновлены: 13.02.2022 23:22 | Добро пожаловать, admin! | Выйти

Обновление базы данных уязвимостей

Нажми кнопку обновить чтобы обновить, нажми кнопку удалить чтобы удалить, не нажимай ничего если ничего не надо

[Обновить БД](#) [Удалить БД](#) [Обновить бюллетени](#)

Статус обновления

Статус: готово к обновлению!

100%

Загружено уязвимостей

| Debian | NIST | БДУ |
|--------|--------|-------|
| 33169 | 180246 | 37489 |

Последнее обновление БД уязвимостей

| Дата, время | Продолжительность |
|------------------|-------------------|
| 13.02.2022 23:22 | 1335 сек. |

Последнее обновление БД бюллетеней

| Дата, время | Продолжительность | Количество |
|------------------|-------------------|------------|
| 14.02.2022 00:00 | 34 сек. | 36 |

Последние загруженные уязвимости

| Cve id | Описание | Комментарий разработчика | Вектор CVSS2: |
|----------------|---|-------------------------------------|--------------------------|
| CVE-2022-24961 | In Portainer Agent before 2.11.1, an API server can continue running even if not associated with a Portainer instance in the past few days. | Информация по устранению уточняется | Базовая оценка CVSS-2: - |

Инструмент поиска уязвимостей в ПО. Таблица результатов



Таблица всех пакетов

Добавить пакет

Загрузить пакеты через файл

Удалить выбранные

Показать 10 пакетов

| # | Наименование ПО | Версия ПО | Подтвержденные уязвимости | | Требуют анализа | | Дополнительные уязвимости | | Устраненные | Неактуальные |
|-----|-----------------|-----------------------|---------------------------|---------------|-----------------|---------------|---------------------------|---------------|-------------|--------------|
| | | | Критические | Некритические | Критические | Некритические | Критические | Некритические | | |
| 166 | binutils | 2.28-5 | 55 | 78 | | | | 1 | 24 | |
| 206 | busybox | 1.22.0-19 | 12 | 2 | 1 | 1 | 13 | 1 | 6 | |
| 253 | check | 0.10.0-3 | 8 | 11 | | | 1983 | 1750 | 311 | |
| 204 | bullet | 2.83.7+dfsg-5 | 7 | | | | 3 | 7 | 1 | |
| 261 | chicken | 4.11.0-1 | 6 | | | | | | | |
| 52 | apache2 | 2.4.25-3+deb9u9 | 4 | 8 | | | 3 | 9 | 4 | |
| 106 | at | 3.1.20-3 | 3 | | | | 1568 | 810 | 113 | |
| 176 | bluez | 5.43-2+deb9u2 | 3 | 14 | 2 | 1 | 18 | 20 | 4 | |
| 205 | bundler | 1.13.6-2 | 3 | | 1 | | 2 | | | |
| 170 | blender | 2.79.b+dfsg0-1~deb9u1 | 2 | 1 | | 1 | | | | |

Пакеты с 1 до 10 (всего 424)

Предыдущая 1 2 3 4 5 ... 43 Следующая

Инструмент поиска уязвимостей в ПО. Представление информации об уязвимости



Выбранные элементы в

Показать уязвимостей Поиск:

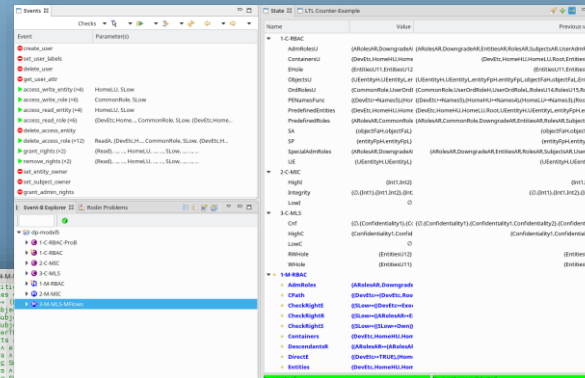
| № | Идентификатор уязвимости | Описание и ссылка на источник информации | Оценка уязвимости | Эксплоит | Рекомендации | Исправленные версии | Комментарии |
|----------------------------|--|---|--|--|---|---|-------------|
| <input type="checkbox"/> 2 | BDU:2017-02053 CVE-2017-1000251 | <p>Уязвимость компонента модуля L2CAP пакета программ, реализующих стек протоколов Bluetooth, позволяющая нарушителю выполнить произвольный код. Уязвимость компонента модуля L2CAP пакета программ BlueZ, реализующих стек протоколов Bluetooth, связана с переполнением буфера. Эксплуатация уязвимости позволяет нарушителю, действующему удалённо, контролировать размер буфера и выполнять произвольный код</p> <p>https://www.armis.com/blueborne</p> <p>https://access.redhat.com/security/vulnerabilities/blueborne</p> <p>https://nvd.nist.gov/vuln/detail/CVE-2017-1000251</p> <p>https://security-tracker.debian.org/tracker/CVE-2017-1000251</p> <p>https://www.exploit-db.com/exploits/42762/</p> | <p>Базовая оценка CVSS-3: 8</p> <p>Вектор CVSS-3: AV:A/AC:L /PR:L/UI:N /S:U/C:H/I:H/A:H</p> <p>Уровень опасности CVSS-3: Высокий уровень опасности</p> <p>Базовая оценка CVSS-2: 8.3</p> <p>Вектор CVSS-2: AV:A/AC:L /Au:N/C:C /I:C/A:C</p> <p>Уровень опасности CVSS-2: Высокий уровень опасности</p> | <p>https://www.exploit-db.com/exploits/42762</p> | <p>Использование рекомендаций:</p> <p>Для Linux:</p> <p>Обновление программного обеспечения до 4.13.1 или более поздней версии</p> <p>Для Astra Linux:</p> <p>Обновление программного обеспечения (пакета linux) до 4.9.30-2+deb9u5 или более поздней версии</p> <p>Для Debian:</p> <p>Обновление программного обеспечения (пакета linux) до 4.9.30-2+deb9u5 или более поздней версии</p> <p>Свернуть «</p> | <p>с 5.46 включительно (bluez)</p> <p>с 4.13.1 включительно (linux)</p> | |

Верификация формальной модели и ее реализации в программном коде операционной системы



| | | <code>access_read(x, y, r)</code> | |
|-----|--------|---|--|
| 1.1 | x, y | $x \in S$, если $y \in E \cup R \cup NR \cup AR$, то существует $r \in R \cup AR$: $\{x, r, read\} \in AA$, (если $y \in E$, то $\{y, read\} \in PA$) и существует контейнер $c \in C$ такой, что $execute_container(c, x, y) = true$, и не существует запрещающей роли $nr \in NR$ такой, что $\{x, nr, read\} \in AA$ и $\{y, read\} \in PA(nr)$, [если $y \in R \cup NR \cup AR$, то $\{y, read\} \in APA(n)$, [если $y \in R \cup AR$, то для всех $nr \in constraint(y)$ верно $\{x, nr, read\} \in AA$] | если $y \in E$, то $A' = A \cup \{x, y, read\}$, если $y \in R \cup NR \cup AR$, то $AA' = AA \cup \{x, y, read\}$ |
| 1.2 | x' | $x' \in S$ [если $y \in R \cup NR \cup AR$, то $i(y) \leq i(x)$, для $e \in E$] либо $\{x, e, read\} \in A$, либо $\{x, e, write\} \in A$, [если $y \in R \cup NR \cup AR$ и $i(y) > i_low$, то $\{x, i_entity, write\} \in A$] | - |
| 2.1 | c_y | [если $y \in E \setminus DB_E$, то $c_y = \emptyset$], [если $y \in DB_E$, то или $\{x, y, postges_admin_role, read\} \in AA$, или существует $r \in DB_R$: $\{x, r, read\} \in AA$, $c_y \in DB_PRIVILEGES$, $read \in db_rights(c_y)$, $\{db_entity(y), read\} \in DB_PA(y)$, и существует контейнер $c \in C \setminus DB_C$ такой, что $execute_container(c, x, y) = true$], [если $y \in DB_R$, то $y \neq public_role$, $c_y = \emptyset$ и или $\{db_login(y) = \emptyset$, существует $r \in AR$: $\{x, r, read\} \in AA$, $\{y, read\} \in DB_APA(n)$, или $\{x, postges_admin_role, read\} \in AA$ или $y \leq db_login(x)$] | если $y \in DB_E$, то $A' = A \cup \{x, db_entity(y), read\}$, если $y \in DB_R$, то если $db_login(x) = \emptyset$, то $\{db_login(y) = y, AA' = AA \cup \{x, y, read\}$, $\{x, public_role, read\}$], иначе $\{AA' = \{AA \cup \{x, y, read\} \setminus \{x, y, read\} \in AA$; $y \in DB_R \setminus \{public_role, y\}\}$ |
| 2.2 | - | если $y \in DB_R$, то [для $e \in E$] либо $\{x, e, read\} \in A$, либо $\{x, e, write\} \in A$, [и $i(y) \leq i(x)$, и если $y \neq public_role$, то $i(y) = i(db_login(x))$], (если $i(y) > i_low$, то $\{x, db_i_entity, write\} \in A$] | - |

МРОСЛ ДП-модель в математической нотации (более 500 страниц описания)

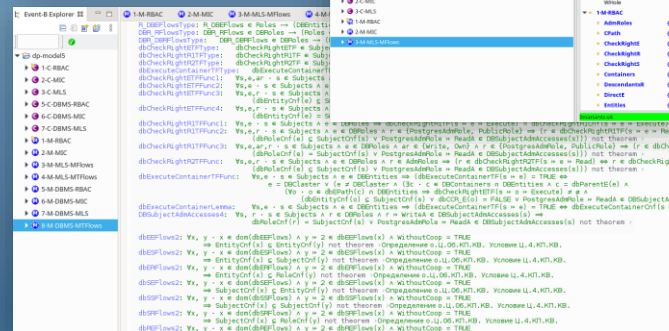


МРОСЛ ДП-модель в формализованной нотации на языке метода Event-B:

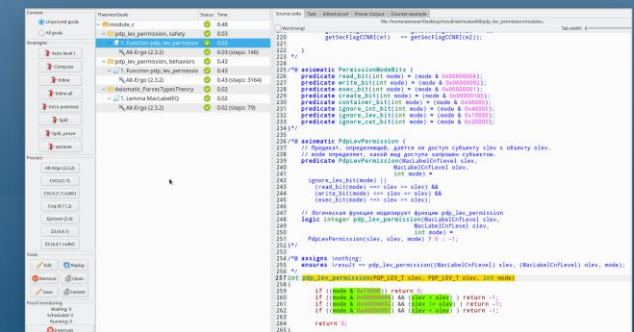
- базовая (более 30 тыс. строк кода);
- экспериментальная (редуцированная);
- адаптированная для системных вызовов управления доступом в Операционной системе

Верификация МРОСЛ ДП-модели в формализованной нотации:

- дедуктивно инструментом Rodin;
- по методу проверки моделей (model checking) инструментом ProB.



Дедуктивная верификация спецификаций на языке ACSL функций подсистемы безопасности PARSEC инструментом Frama-C



Статический анализ кода операционной системы с применением Svace, Clang SA, Cppcheck, АК-ВС 3.0

ASTRA LINUX
просмотр исходников

МЕНЕДЖЕР ФАЙЛОВ:

- <<< utils-common
- CMakeLists.txt
- _Makefile
- getparsec.c
- ls.c
- setparsec.c

```
318 #ifdef SETPMAC
319     mac_t mac = NULL;
320     cmd_t cmd = cmd_init_setmac();
321     if (!cmd)
322         goto fexit;
323     mac = mac_init(MAC_TYPE_OBJECT);
324     if ((p = strchr(*text_p, '\n'))
```

DEREF_AFTER_NULL.EX
Описание: After having been compared to NULL value at setparsec.c:316, pointer 'text_p' is dereferenced at setparsec.c:324.
Средство анализа: Svace 3.2.0
CWE: -----
Bugtracker: BT-1347
Статус: Подтверждено
Параметры анализа: svace warning all true

DEREF_AFTER_NULL.EX
Описание: After having been compared to NULL value at setparsec.c:316, pointer 'text_p' is dereferenced at setparsec.c:324 by calling function 'strchr'.
Средство анализа: Svace 3.2.0
CWE: -----
Bugtracker: BT-1347
Статус: Подтверждено
Параметры анализа: svace warning all true

nullPointerRedundantCheck
Описание: Either the condition 'if(text_p&&*text_p)' is redundant or there is possible null pointer dereference: text_p.
Средство анализа: Cppcheck 1.86
CWE: 476
Bugtracker: BT-1347
Статус: Подтверждено
Параметры анализа: cppcheck --enable=warning,unusedFunction,performance -f --suppress=unknownMacro

```
325     *p = 0;
```

СПИСОК ОШИБОК:

- COMMENTED_SOURCE_CODE:270 Svace static
- COMMENTED_SOURCE_CODE:279 Svace static
- COMMENTED_SOURCE_CODE:284 Svace static
- DEREF_AFTER_NULL.EX:324 Svace static
- DEREF_AFTER_NULL.EX:324 Svace static
- nullPointerRedundantCheck:324 Cppcheck static

ПАРАМЕТРЫ:

Критичность: Средняя

Статус: Подтверждено

Bug tracker: BT - 1347

Применить

Средство

Выбрать [tname+type]

Svace - статический анализатор кода

Cppcheck - статический анализатор кода

Clang - статический анализатор кода

Анализ CVE

АК-ВС

Syzkaller - фаззер уровня ядра ОС

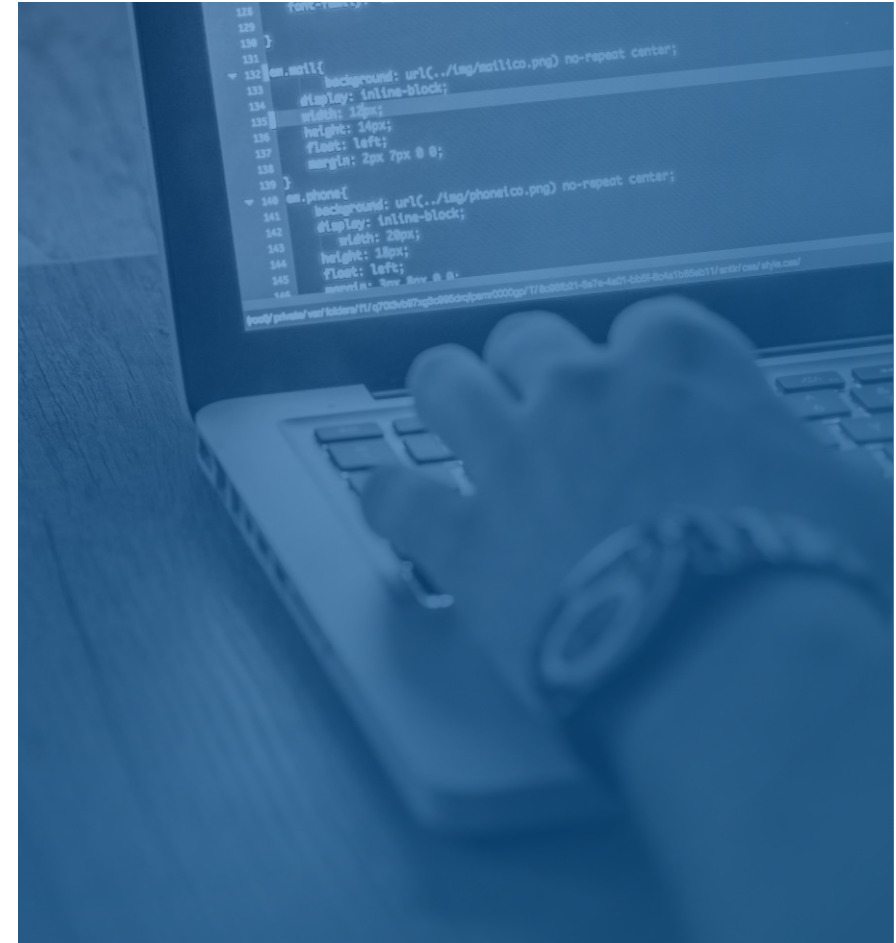
Syzcrawler - среда регрессионного фаззинг-тестирования

Для ядра и модулей безопасности, функционирующих в пространстве ядра операционной системы:

- SYZKALLER
- SYZCRAWLER

Для остальных компонентов операционной системы:

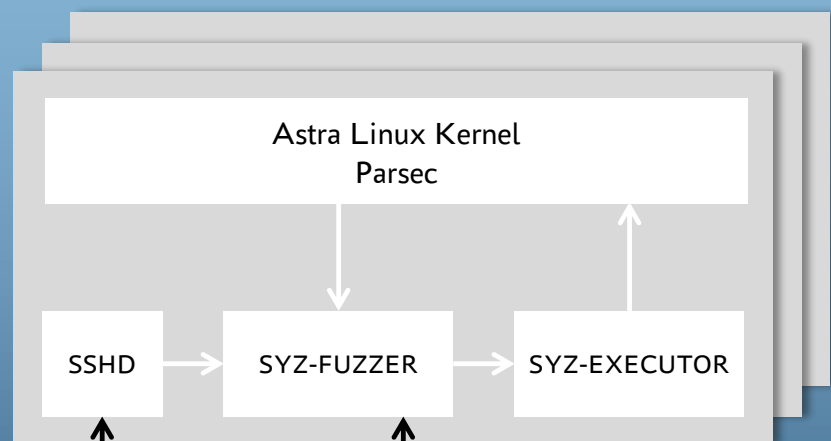
- Программный комплекс Crusher (ИСП РАН)
- Среда символьного выполнения S2E, KLEE
- Фаззер AFL / AFL++
- Фаззер Libfuzzer



Динамический анализ кода операционной системы с использованием стенда Syzkaller4astra



Виртуальные машины с операционной системой



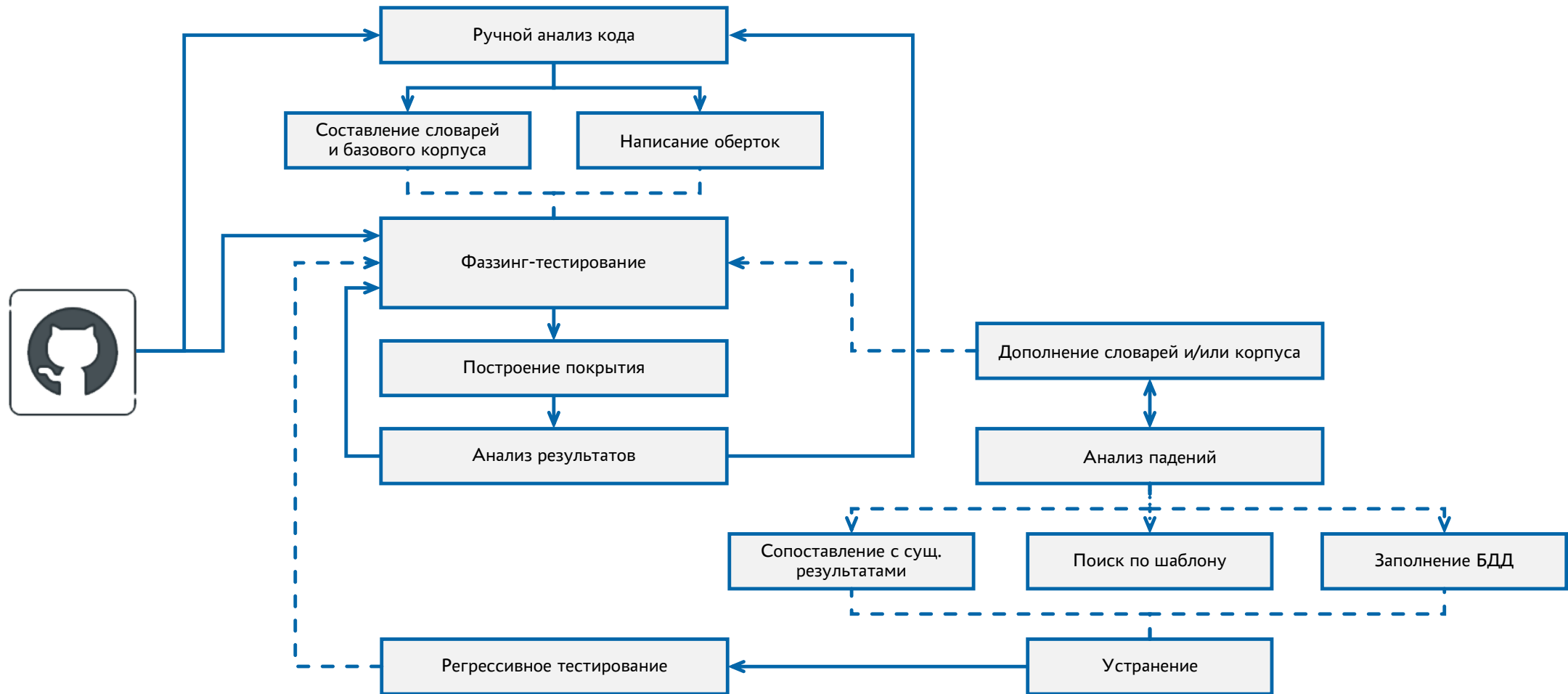
База данных результатов тестирования Расчет покрытия кода

| | | | |
|----------------------|------|---------|---|
| ▼ parsec | 60% | of 2096 | int pdp_lev_permission(PDP_LEV_T slev, PDP_LEV_T olev, int mode) |
| ▼ linux-astra/parsec | 61% | of 2071 | { |
| ▼ dp | 82% | of 169 | 49 if ((mode & LEGACY_IGNORE_LEV)) return 0; |
| ▼ pdp_common.c | 82% | of 168 | 48 if ((mode & R_OK) && (slev < olev)) return -EACCES; |
| ▼ pdp_common.h | 100% | of 1 | 48 if ((mode & W_OK) && (slev != olev)) return -EACCES; |
| audit-file.c | 37% | of 135 | 5454 if ((mode & X_OK) && (slev < olev)) return -EACCES; |
| audit-kernel.c | 60% | of 22 | return 0; |
| cap.c | 80% | of 74 | } |
| cmdline.c | --- | of 46 | int pdp_cat_permission(PDP_CAT_T scat, PDP_CAT_T ocat, int mode) |
| crc16.c | --- | of 5 | { |
| logfs.c | --- | of 27 | 5453 if(mode & LEGACY_IGNORE_CAT) return 0; |
| net.c | 48% | of 151 | 48 if((mode&R_OK) && ((scat & ocat) != ocat)) return -EACCES; |
| parsec-fs.c | 85% | of 91 | 48 if((mode&W_OK) && (ocat != scat)) return -EACCES; |
| path.c | 50% | of 6 | 5453 if((mode&X_OK) && ((scat & ocat) != ocat)) return -EACCES; |
| sec-audit.c | 60% | of 220 | return 0; |
| sec-audit.h | 100% | of 1 | } |
| sec-hooks.c | 51% | of 515 | int pdpml_conf_permission(const PDPML_T *s, const PDPML_T *o, int mode) |
| security.c | 72% | of 150 | { |
| security.h | 100% | of 1 | 5454 if(pdp_lev_permission(s->lev,o->lev,mode) pdp_cat_permission(s->cat,o->cat,mode)) { |
| syscalls.c | 88% | of 217 | return -EACCES; |
| userconfine.c | 43% | of 78 | } |
| xattr.c | 73% | of 163 | return 0; |
| parsec_elfrand.c | --- | of 5 | |
| parsec_gost89.c | --- | of 20 | |
| safesetid | --- | of 78 | |

Серверы тестирования

CRASHES + CORPUS

Процесс фазинг-тестирования утилит пользовательского пространства







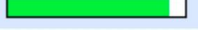
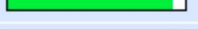
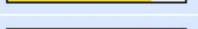

LCOV - code coverage report

Current view: [top level](#)

Test: [cov.info](#)

Date: 2021-11-25 13:15:09

| | Hit | Total | Coverage |
|------------|------|-------|----------|
| Lines: | 2700 | 3101 | 87.1 % |
| Functions: | 226 | 234 | 96.6 % |

| Directory | Line Coverage ↕ | Functions ↕ |
|--|--|-----------------|
| /usr/include/x86_64-linux-gnu/bits |  76.5 % 26 / 34 | - 0 / 0 |
| /usr/include |  100.0 % 2 / 2 | 100.0 % 1 / 1 |
| /usr/include/x86_64-linux-gnu/sys |  100.0 % 1 / 1 | - 0 / 0 |
| lib-aud |  88.6 % 1170 / 1320 | 97.9 % 94 / 96 |
| lib-aud-db-files |  90.9 % 189 / 208 | 100.0 % 11 / 11 |
| lib-aux |  92.5 % 544 / 588 | 100.0 % 42 / 42 |
| lib-base |  81.0 % 235 / 290 | 100.0 % 24 / 24 |
| lib-cap |  80.9 % 511 / 632 | 93.1 % 54 / 58 |

70% – покрытие модулей безопасности PARSEC (поверхности атаки) по базовым блокам;

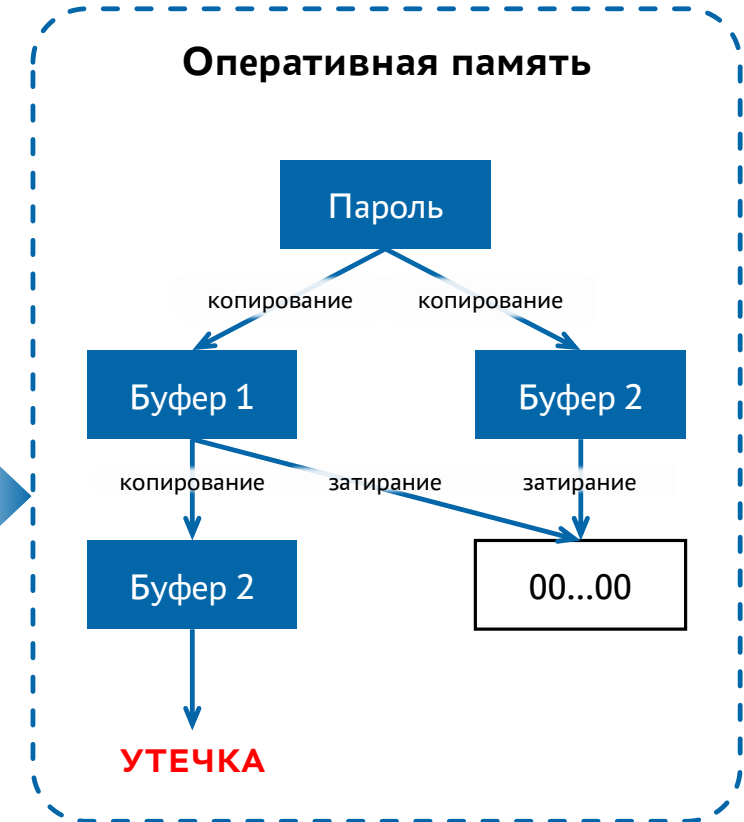
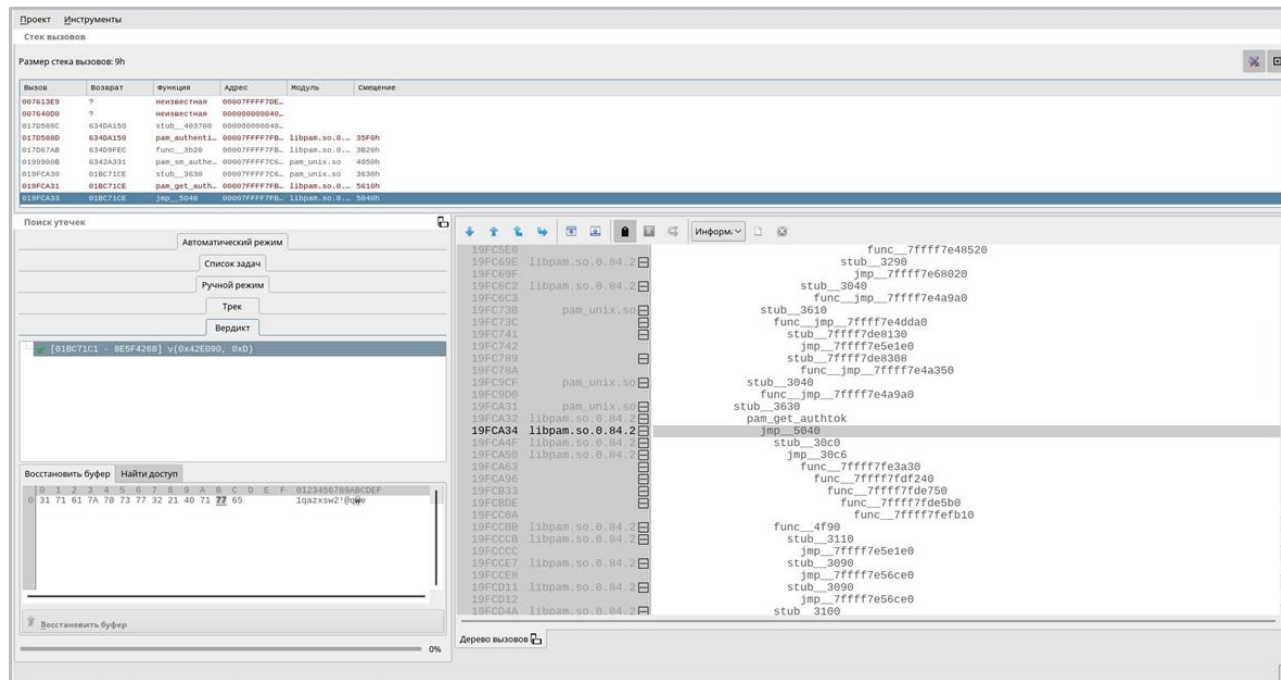
80% – покрытие модулей пользовательского пространства по строкам;

72 часа – среднее время устранения выявляемых ошибок в модулях безопасности.

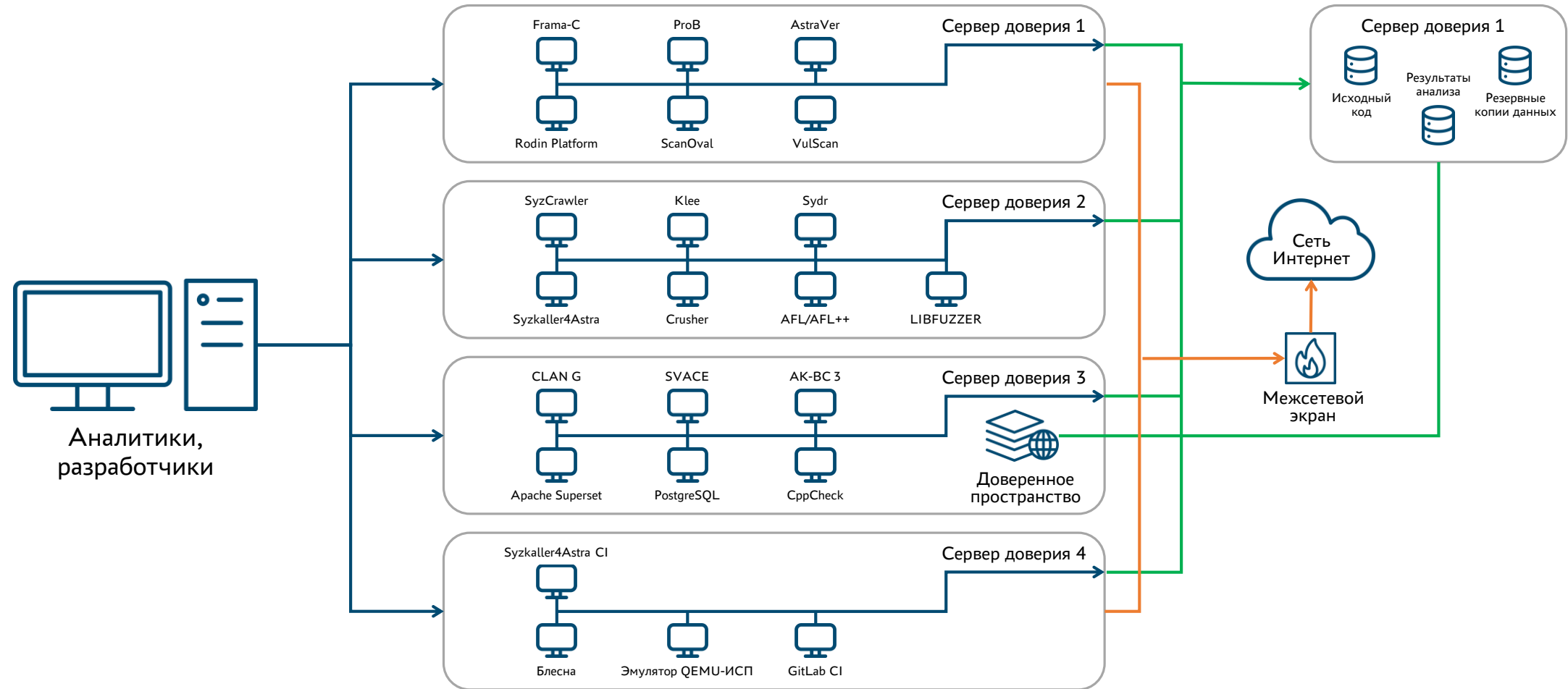
Анализ помеченных данных при сборе трасс программ инструментом БЛЕСНА (ИСП РАН)



Инструмент БЛЕСНА



Масштабируемая структура стенда доверия для верификации и анализа кода операционной системы



Интерфейс базы данных доверия. Вывод информации об ошибках



ASTRA LINUX
ПРОСМОТР ИСХОДНИКОВ

МЕНЕДЖЕР ФАЙЛОВ:

- <<< utils-pdp
- CMakeLists.txt
- ls_pdp.c
- ls_proc.c
- ls_xstrtol.c
- pdp-id.c
- pdp-init-fs
- pdp-init-fs.c
- pdp-ls.c
- pdpl-file.c
- pdpl-ps.c
- pdpl-user.c
- set-fs-ilev.c
- setfattr.c
- unset-fs-ilev

```
2446     size_t i;
2447
2448     for (i = 0; i < files_index; i++) {
2449         free(files[i].name);
2450
2451         free(files[i].linkname);
2452     }
2453 }
2454
2455     files_index = 0;
2456
2457 #if HAVE_ACL
2458     any_has_acl = false;
2459 #endif
2460 #if HAVE_PARSEC
2461     parsec_any_has=0;
2462     parsec_any_max_len=0;
2463 #endif
2464     inode_number_width = 0;
```

DANGLING_POINTER.STRICT
Описание: Several pointers freed in function 'clear_files' are not overwritten. For example, pointer 'files[i]->linkname'
Средство анализа: Svace 3.2.0
CWE: -----
Bugtracker: BT-22564
Статус: Исправлено
Параметры анализа: svace warning all true

SEGV on unknown address
Описание: SEGV on unknown address
Средство анализа: AFL 2.68c
CWE: -----
Bugtracker: BT-24261
Статус: Исправлено
Параметры анализа: -----

СПИСОК ОШИБОК:

- core.UndefinedBinaryOperatorResult:2437 Clang static
- DANGLING_POINTER.STRICT:2450 Svace static
- SEGV on unknown address:2450 AFL
- allocaCalled:2524 Cppcheck static
- PROC_USE.VULNERABLE:2760 Svace static
- security.insecureAPI.strcpy:2760 Clang static

ПАРАМЕТРЫ:

Фильтры Таблица Перекрестный запрос

Дата 5

Статус 5

Пользователь 6

Баг-трекер 6

Количество результатов запроса: 17

Дистрибутив 5

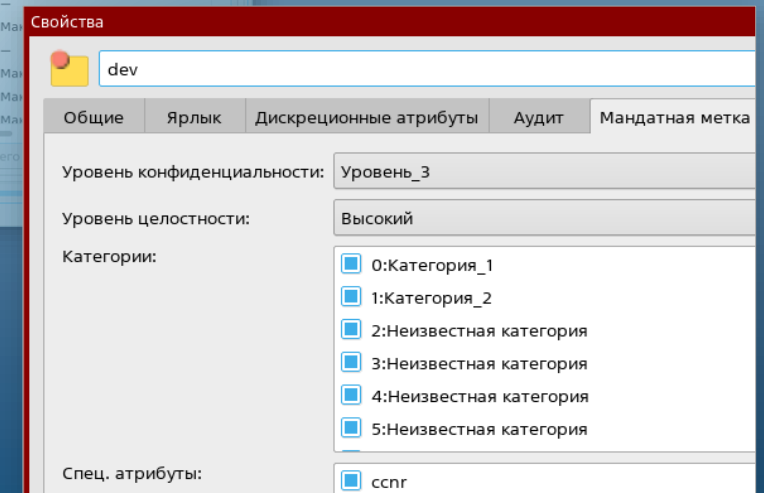
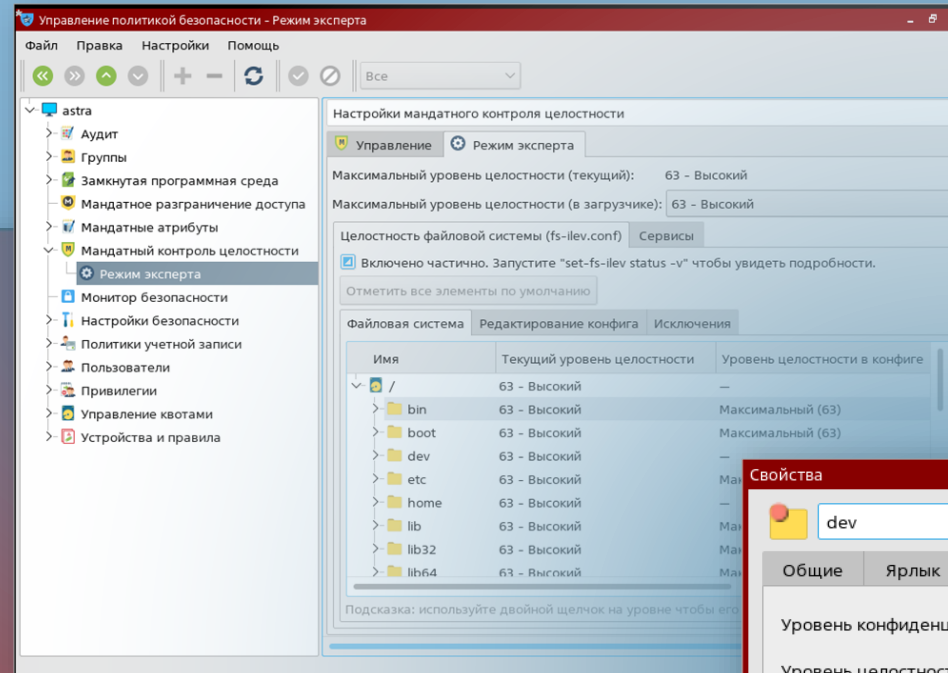
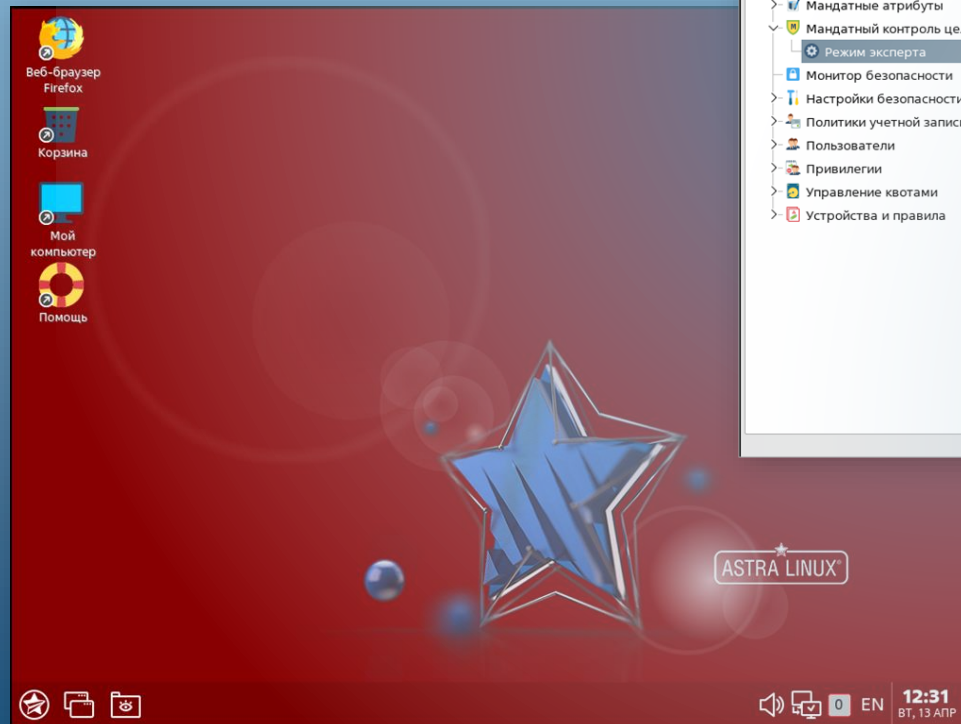
Название пакета 5

Средство 5

Критичность 6

Версия пакета 5

Реализация с применением методологии верифицированного механизма защиты операционной системы





Спасибо за внимание!