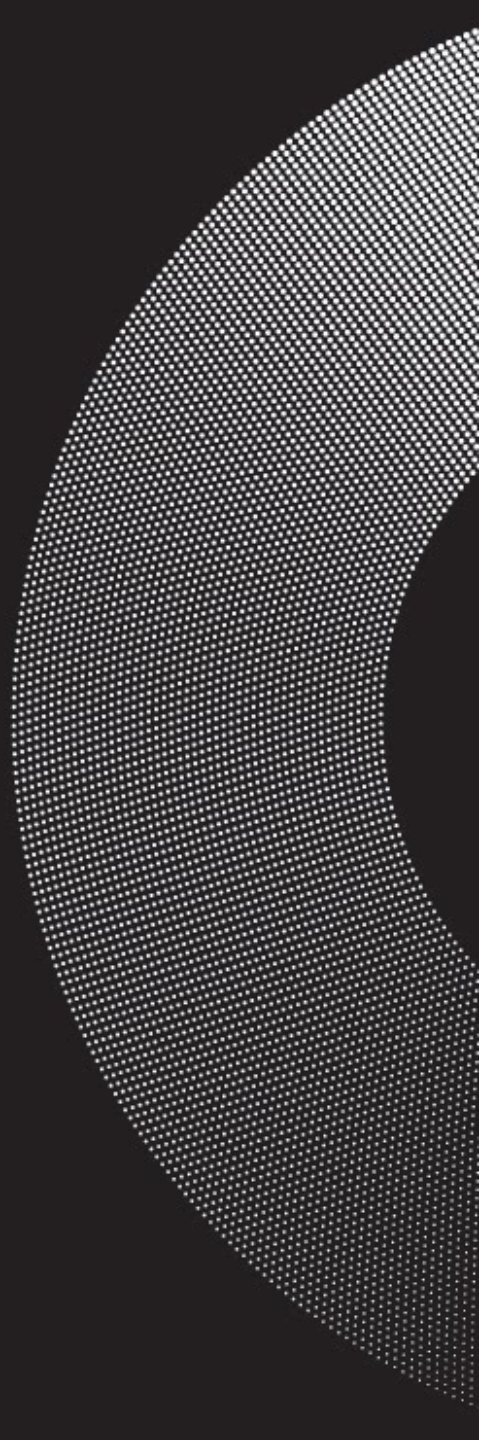
Исследования биометрических терминалов с точки зрения ИБ



московский политех

Аннотация

Основная цель работы была направлена на изучение ИС с терминалом распознавания лица "Ак Барс" модели POS

Данный проект актуален, потому что биометрические системы активно используются компаниями для обеспечения безопасности, в том числе информационной.

В ходе работы была развернута и изучена ИС биотерминала, разработаны схема взаимодействия её частей, модели угроз и руководство по защите ИС.

Со всем можно ознакомиться в GitHub репозитории, ссылка на который будет представлена в конце презентации.

Задачи каждого участника

Шипилова Анастасия

1. Изучение и развертывание ИС биотерминала,
2. Траблшутинг,
3. Общение с заказчиком

Платонов Артём

1. Изучение и развертывание ИС биотерминала,
2. Траблшутинг,
3. Механическая модернизация семпла,
4. Развертывание и работа с БД,
5. Общение с заказчиком

Кочаров Арсений

1. Траблшутинг,
2. Тестирование,
3. Развертывание и работа с БД,
4. Общение с заказчиком

Задачи каждого участника

Окунев Степан

Ведение Сайта отчёта,
Схема взаимодействия,
Руководство по защите ИС.
Отчетность

Богачёв Максим

Руководство по защите ИС.
Отчетность

Шмаков Данила

Руководство по защите ИС.
Схема взаимодействия,
Отчетность

Задачи каждого участника

Захаров Василий

Модель угроз POS

Константинов Денис

Модель угроз СКУД

Основное содержание

Про биотерминал

Inoface 7 – это инновационный терминал для биометрической идентификации по геометрии лица. Терминал с успехом решает задачи по организации систем контроля и управления доступом и учета рабочего времени.

Графический процессор: Архитектура NVIDIA Maxwell™ со 128 ядрами

Процессор: Четырехъядерный процессор ARM® Cortex®-A57 MPCore

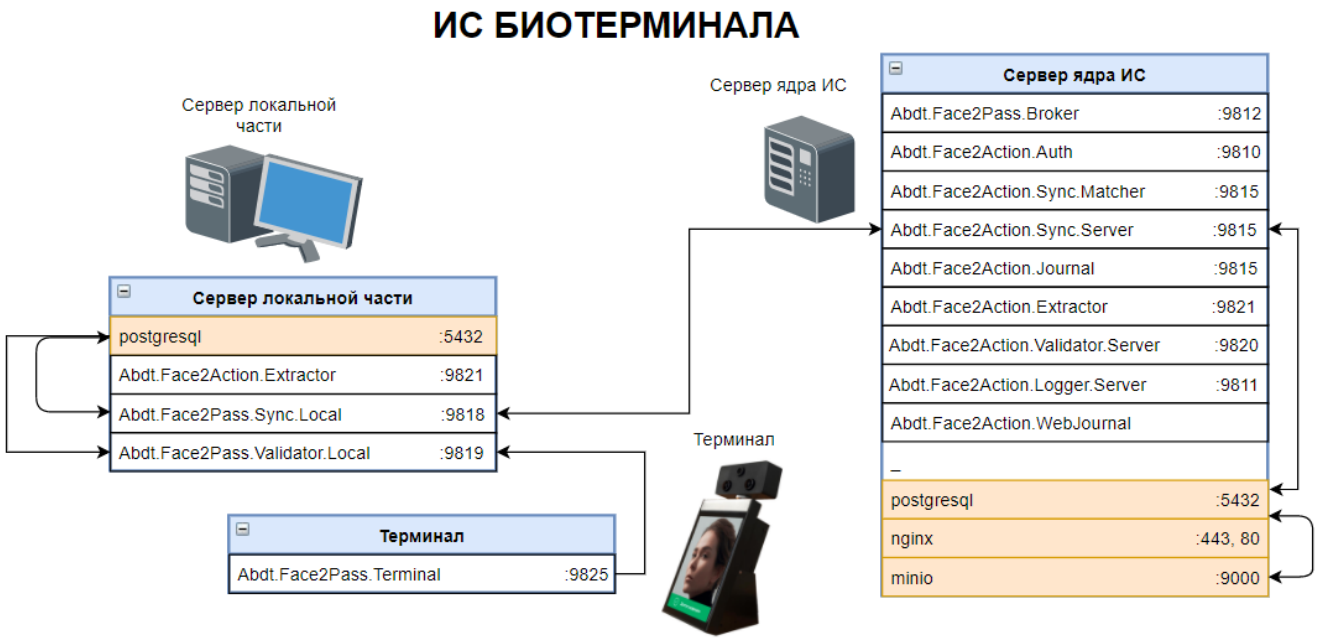
Экран: 7"дисплей с разрешением 1920*1080 (Full HD)

Камеры: Синхронизированная стерео-камера 1500p, ИК-камера 720p

Основное содержание

Схема взаимодействия ИС терминала

Изучая документацию и общаясь с разработчиками, которые предоставили нам биотерминал и связанное с ним ПО, мы построили схему взаимодействия его информационной системы.
Она состоит из самого терминала, локального сервера, центрального сервера (ядра).
На схеме показано с чем взаимодействуют конкретные приложения ИС и на каких портах они располагаются



Основное содержание

Модель угроз

Модель угроз разрабатывалась на протяжении всего проекта и, в итоге, стала крайне валидной моделью ёмко отражающей все угрозы и их релевантность в отношении биотерминала.

ID УГ	Название угрозы	Описание угрозы	Источники угрозы	Объект воздействия	Нарушение конфиденциальности (ущерб)	Нарушение целостности (ущерб)	Нарушение доступности (ущерб)	Дата включения угрозы в УБИ	Дата последнего изменения данных
1	Угроза автоматического распространения вредоносного кода в грид-	Угроза заключается в возможности внедрения	Внешний нарушитель со средним потенциалом,	Ресурсные центры грид-	средний	высокий	средний	20.03.2015	20.03.2
2	Угроза агрегирования данных, передаваемых в грид-системе	Угроза заключается в возможности раскрытия	Внешний нарушитель со средним потенциалом	Сетевой трафик	средний			20.03.2015	20.03.2
3	Угроза анализа криптографических алгоритмов и их реализации	Угроза заключается в возможности выявления	Внешний нарушитель со средним потенциалом	Метаданные, системное	средний	высокий		20.03.2015	20.03.2
4	Угроза аппаратного сброса пароля BIOS	Угроза заключается в возможности сброса	Внутренний нарушитель с низким потенциалом	Микропрограммное и		высокий		20.03.2015	20.03.2
5	Угроза внедрения вредоносного кода в BIOS	Угроза заключается в возможности заставить	Внутренний нарушитель с высоким потенциалом	Микропрограммное и	средний	высокий	средний	20.03.2015	20.03.2
6	Угроза внедрения кода или данных	Угроза заключается в возможности внедрения	Внешний нарушитель с низким потенциалом	Системное программное	средний	высокий	средний	20.03.2015	20.03.2
7	Угроза воздействия на программы с высокими привилегиями	Угроза заключается в возможности повышения	Внешний нарушитель со средним потенциалом,	Информационная система,	средний	высокий		20.03.2015	20.03.2
8	Угроза восстановления аутентификационной информации	Угроза заключается в возможности п							
9	Угроза восстановления предыдущей уязвимой версии BIOS	Угроза заключается в возможности							
10	Угроза выхода процесса за пределы виртуальной машины	Угроза заключается в возможности з							
11	Угроза девторизации санкционированного клиента беспроводной сети	Угроза заключается в возможности							
12	Угроза деструктивного изменения конфигурации/среды окружения	Угроза заключается в возможности							
13	Угроза деструктивного использования декларированного функционала	Угроза заключается в возможности							
14	Угроза длительного удержания вычислительных ресурсов пользователями	Угроза заключается в возможности							
15	Угроза доступа к защищаемым файлам с использованием обходного пути	Угроза заключается в возможности п							
16	Угроза доступа к локальным файлам сервера при помощи URL	Угроза заключается в возможности п							
17	Угроза доступа/перехвата/изменения HTTP cookies	Угроза заключается в возможности							
18	Угроза загрузки нештатной операционной системы	Угроза заключается в возможности п							
19	Угроза заражения DNS-кеша	Угроза заключается в возможности							
20	Угроза злоупотребления возможностями, предоставленными	Угроза заключается в возможности							
21	Угроза злоупотребления доверием потребителей облачных услуг	Угроза заключается в возможности н							
22	Угроза избыточного выделения оперативной памяти	Угроза заключается в возможности в							
23	Угроза изменения компонентов системы	Угроза заключается в возможности п							
24	Угроза изменения режимов работы аппаратных элементов компьютера	Угроза заключается в возможности и							
25	Угроза изменения системных и глобальных переменных	Угроза заключается в возможности							
26	Угроза искажения XML-схемы	Угроза заключается в возможности и							
27	Угроза искажения вводимой и выводимой на периферийные устройства	Угроза заключается в возможности							
28	Угроза использования альтернативных путей доступа к ресурсам	Угроза заключается в возможности							
29	Угроза использования вычислительных ресурсов суперкомпьютера	Угроза заключается в возможности							
30	Угроза использования информации идентификации/аутентификации,	Угроза заключается в возможности							
31	Угроза использования механизмов авторизации для повышения	Угроза заключается в возможности п							
32	Угроза использования поддельных цифровых подписей BIOS	Угроза заключается в возможности у							
33	Угроза использования слабостей кодирования входных данных	Угроза заключается в возможности							
34	Угроза использования слабостей протоколов сетевого/локального обмена	Угроза заключается в возможности							
35	Угроза использования слабых криптографических алгоритмов BIOS	Угроза заключается в сложности про							
36	Угроза исследования механизмов работы программы	Угроза заключается в возможности							
37	Угроза исследования приложения через отчёты об ошибках	Угроза заключается в возможности							
38	Угроза исследования вычислительных ресурсов хранилища больших данных	Угроза заключается в возможности							

ID	Нарушители	Категория нарушителя	Потенциал нарушителя	Возможная мотивация	Предполагаемые возможности *	Возможный класс СКЗИ **
1	Специальные службы иностранных государств (блоков государств)	Внешний нарушитель, Внутренний нарушитель	С Высоким потенциалом	Дискредитация или дестабилизация деятельности предприятия.	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами).	КА
2	Неустановленные внешние субъекты (физические лица)	Внешний нарушитель	С Низким потенциалом	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса).	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках	КС1
3	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний нарушитель	Со Средним потенциалом	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непредумышленные, неосторожные или неквалифицированные действия.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного	КВ
4	Лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	Внутренний нарушитель	С Низким потенциалом	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непредумышленные, неосторожные или неквалифицированные действия.	Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	КС2
5	Пользователи информационной системы	Внутренний нарушитель	С Низким потенциалом	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непредумышленные, неосторожные или неквалифицированные действия.	Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему	КС1
6	Администраторы информационной системы и администраторы безопасности	Внутренний нарушитель	Со Средним потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непредумышленные, неосторожные или неквалифицированные действия.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент	КС3
7	Бывшие работники (пользователи)	Внешний нарушитель	С Низким потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему	КС1
8	Лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ	Внутренний нарушитель	С Низким потенциалом	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непредумышленные, неосторожные или неквалифицированные действия	Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за	КС3

Основное содержание

Руководство по защите

Это документ, описывающий способы реализации угроз и методы защиты от них. Был собран тестовый стенд из 3 виртуальных машин для проведения тестирования на безопасность и реализацию угроз. В документе описаны принципы работы той или иной уязвимости, методы защиты, а также методические указания по реализации атаки.

Конфигурация лабораторного стенда.

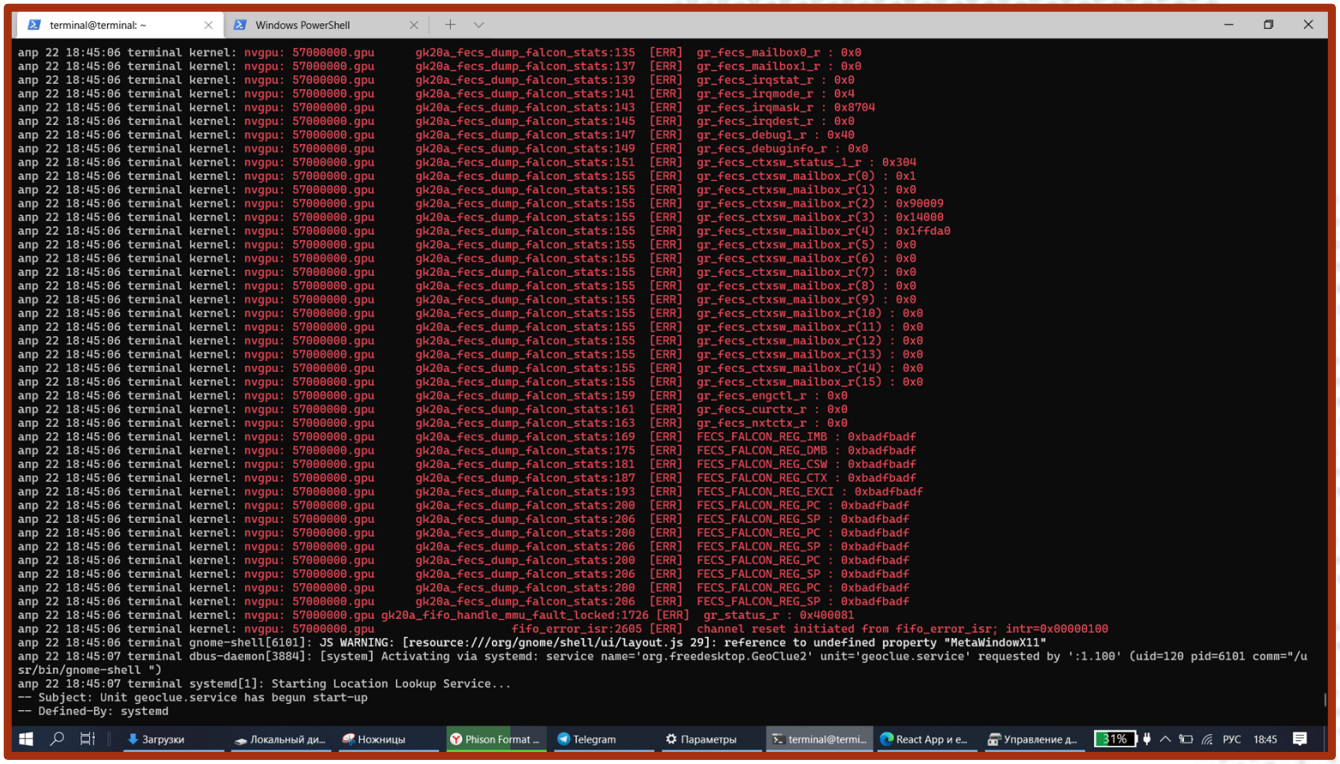
Имя машины	IP-адрес	Mac адрес	Учетная запись	ОС:
Kali	192.168.0.116	08:00:27:ab:08:1c	Для входа в систему: kali/kali	Kali Linux
	192.168.0.115	98:28:A6:10:CA:A5		Win 10
ubunta	192.168.0.117	08:00:27:16:2b:f2	danla/rootroot	Ubuntu

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.116  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:feab:81c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ab:08:1c  txqueuelen 1000  (Ethernet)
        RX packets 124  bytes 13410 (13.0 KiB)
        RX errors 0  dropped 3  overruns 0  frame 0
        TX packets 68  bytes 6998 (6.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

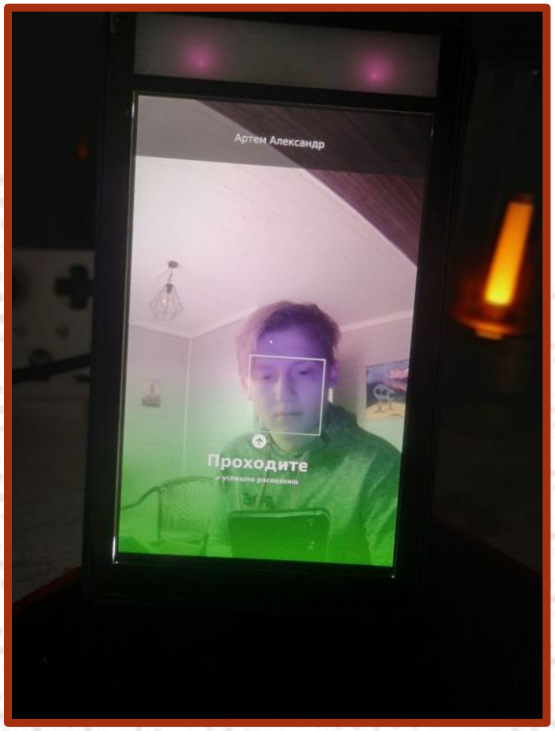
Основное содержание

Проблемы с которыми сталкивались

При развертывании ПО биотерминала мы столкнулись с рядом проблем в работе лог-паса и сертификатов сервера nginx, но благодаря хорошей командной работе мы быстро с ними справились.
Пользователь зарегистрирован, однако биотерминал не распознавал его как зарегистрированного пользователя, выдавая ошибки следующего содержания. Эта проблема отняла больше времени, но ее тоже удалось решить.



```
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:135  [ERR]  gr_fecs_mailbox0_r : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:137  [ERR]  gr_fecs_mailbox1_r : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:139  [ERR]  gr_fecs_irqstat_r : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:141  [ERR]  gr_fecs_irqmode_r : 0x4
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:143  [ERR]  gr_fecs_irqmask_r : 0x8704
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:145  [ERR]  gr_fecs_irqdest_r : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:147  [ERR]  gr_fecs_debug1_r : 0x40
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:149  [ERR]  gr_fecs_debuginfo_r : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:151  [ERR]  gr_fecs_ctxsw_status_1_r : 0x304
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(0) : 0x1
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(1) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(2) : 0x90009
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(3) : 0x14000
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(4) : 0x1ffda0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(5) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(6) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(7) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(8) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(9) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(10) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(11) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(12) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(13) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(14) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:155  [ERR]  gr_fecs_ctxsw_mailbox_r(15) : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:159  [ERR]  gr_fecs_engctl_r : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:161  [ERR]  gr_fecs_curctx_r : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:163  [ERR]  gr_fecs_nxtctx_r : 0x0
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:169  [ERR]  FECS_FALCON_REG_IMB : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:175  [ERR]  FECS_FALCON_REG_DMB : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:181  [ERR]  FECS_FALCON_REG_CSW : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:187  [ERR]  FECS_FALCON_REG_CTX : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:193  [ERR]  FECS_FALCON_REG_EXCI : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:200  [ERR]  FECS_FALCON_REG_PC : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:206  [ERR]  FECS_FALCON_REG_SP : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:200  [ERR]  FECS_FALCON_REG_PC : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:206  [ERR]  FECS_FALCON_REG_SP : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:200  [ERR]  FECS_FALCON_REG_PC : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:206  [ERR]  FECS_FALCON_REG_SP : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:200  [ERR]  FECS_FALCON_REG_PC : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu      gk20a_fecs_dump_falcon_stats:206  [ERR]  FECS_FALCON_REG_SP : 0xbadfbadf
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu gk20a_fifo_handle_mmu_fault_locked:1726 [ERR]  gr_status_r : 0x400081
апр 22 18:45:06 terminal kernel: nvgpu: 57000000.gpu                   fifo_error_isr:2605 [ERR]  channel reset initiated from fifo_error_isr; intr=0x00000100
апр 22 18:45:06 terminal gnome-shell[6101]: JS WARNING: [resource:///org/gnome/shell/ui/layout.js 29]: reference to undefined property "MetaWindowX11"
апр 22 18:45:07 terminal dbus-daemon[3884]: [system] Activating via systemd: service name='org.freedesktop.GeoClue2' unit='geoclue.service' requested by ':1.100' (uid=120 pid=6101 comm="/u
sr/bin/gnome-shell ")
апр 22 18:45:07 terminal systemd[1]: Starting Location Lookup Service...
-- Subject: Unit geoclue.service has begun start-up
-- Defined-By: systemd
```



Итоги работы

Сайт проекта:
http://pd-2021-1.std-850.ist.mospolytech.ru

GitHub
https://github.com/Steper2000/biotherm_spring2021

Спасибо
за внимание!

московский
политех