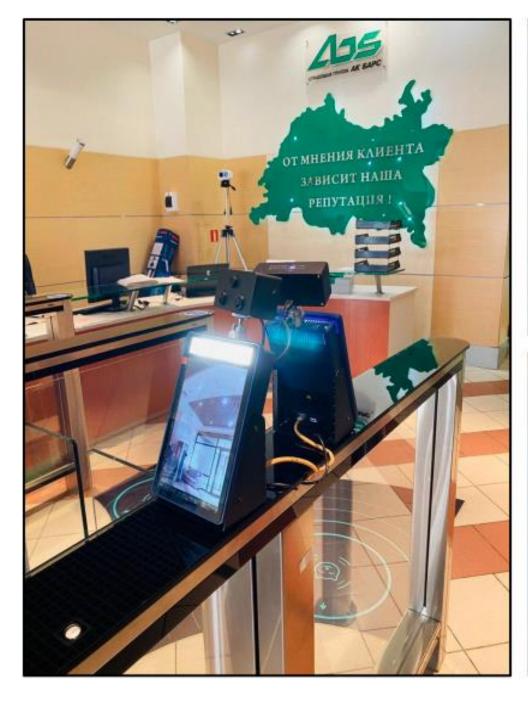
Исследование биометрических терминалов с точки зрения ИБ

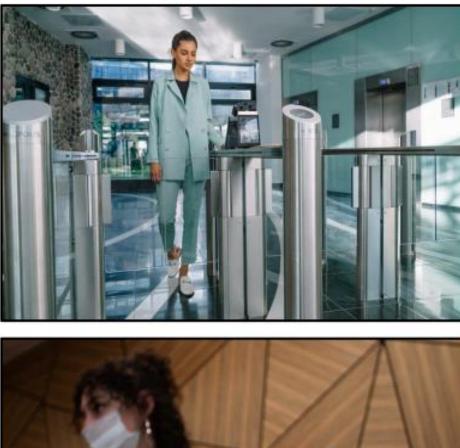
Подготовили:

Шипилова А.С., Платонов А.А., Окунев С.О., Богачёв М.Г., Шмаков Д.Б., Кочаров А.В., Константинов Д.А., Захаров В.А.

Немного о биотерминале

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.





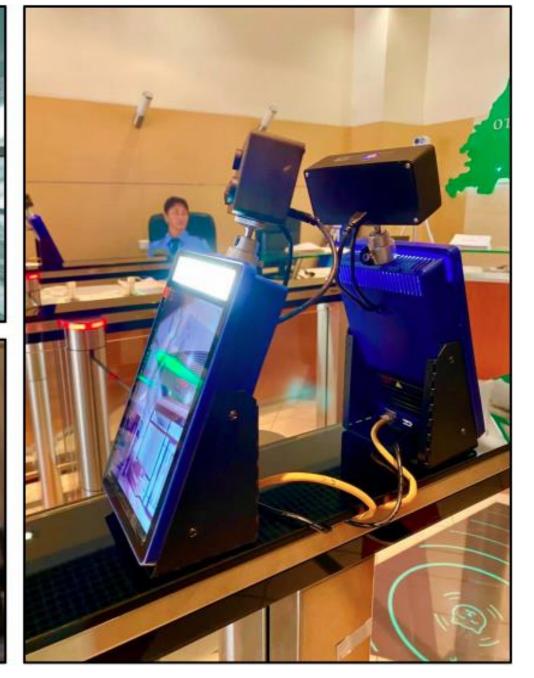
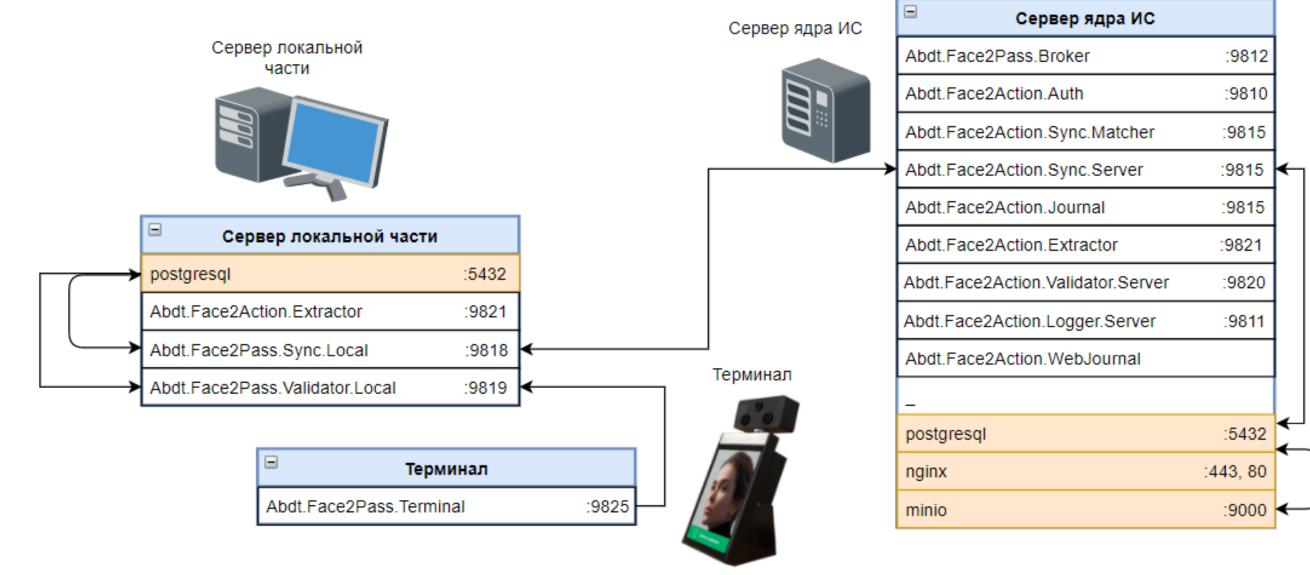


Схема взаимодействия

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).





Модель угроз

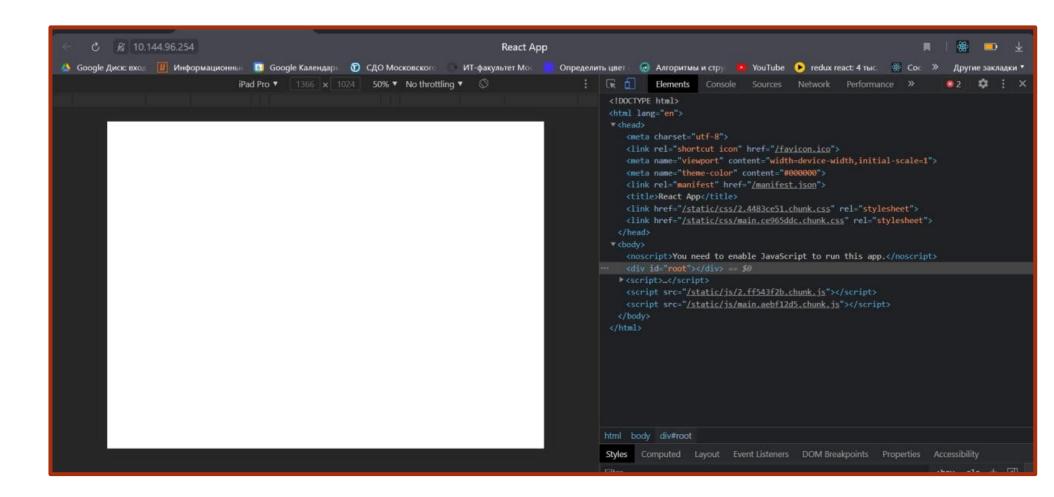
Модель угроз разрабатывалась на протяжении всего проекта и, в итоге, стала крайне валидной моделью ёмко отражающей все угрозы и их релевантность в отношении биотерминала.

ID	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 всаможностями нарушителей с базовым и базовым повышенным потенциалами. Всаможнюсть осуществлять несанкционированный доступ на выделенных (ведомственных и корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Возможность дорыме, поступ и системноми и прикладиом прогламичеми обеспечения.	ка
2	Неустановленные внешние субъекты (физические лица)	Внешний нарушитель	С Низким потенциалом	Идеологические или политические мотивы. Причинение имущественого ущерба путем мощеничества или иным преступным путем. Любопытство или желание самореализации (полутели ление статусса).	Водможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Водможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках в политирующим профессионного применения в простему политирующим истом безопроцесств информации.	KC1
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 разработов. Причинение инущественного ущерба путем обмана или элоупотребления доверием. Непредкамеренные, неосторожные или неквалифицированные действия.	Водможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Водможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Водможность 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 элоупотребления доверием. Непредвамеренные, неосторожные или неквалифицированные действия.	Водможность получить информацию об украиностях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Водможность 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 Водможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны. Водможность создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗЙ 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. Непреднамеренные, неосторожные или неквалифицированные действия.	Водможность получить информацию об украимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Водможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных этак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации этак и реализацию этак на информационную систему	KC1
6	Администраторы информационной системы и администраторы безопасности	Внутренний нарушитель	Со Средним потенциалом	Причинение имущественного ущерба путем мошении-иства или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление украимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Водможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны Водможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованиую в общедоступных источниках Водможность получить информации о ометодах и средствах реализации угрод 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 водможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, запарах истам приведения, с использованием имеющихся в свободном доступе программных средств,	ксз
7	Бывшие работники (пользователи)	Внешний нарушитель	С Низким потенциалом	Причинение имущественного ущерба путем мошеничества или иным преступным путем. Месть за ранее совершенные действия.	Всаможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Всаможность получить виформацию об укавимостях отдельных компонент информационной системы, опубликованияю в общедоступных источниках Всаможность получить виформацию 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	KC1
8	Лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ	Внутренний нарушитель	С Низким потенциалом	Причинение имущественного ущерба путем обмана или элоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Водможность получить неформацию об укранностях отдельных компонент информационной системы, опубликованную в общедоступных источниках Водможность 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 Водможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за поверевым контроличений этом.	ксз

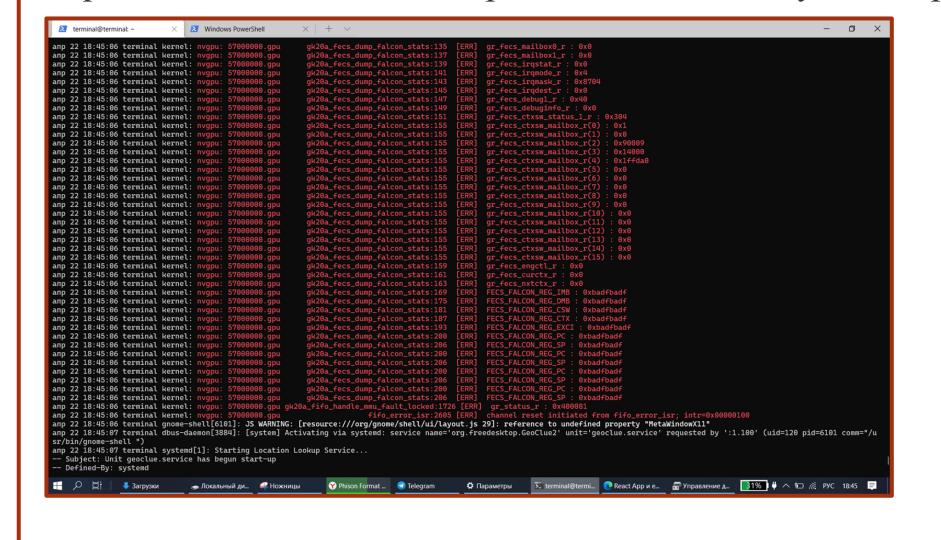
				_	Нарушение конфиденциа	Нарушение целостност	Нарушение доступност	Дата включения	Дата последня
ID AL.,	Название угрозы	Описание угрозы	Источники угрозы	Объект воздействи:	льности (ущерб)	(Ущер)	(ущері 🔻	угрозы в I УБИ —	изменень данных
1	Угроза автоматического распространения вредоносного кода в грид-	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 annapaтного 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 подбора	Внешний нарушитель с низким потенциалом,	Системное программное	средний			20.03.2015	20.03.2
9	Угроза восстановления предыдущей уязвимой версии BIOS	Угроза заключается в возможности	Внутренний нарушитель с низким потенциалом	Микропрограммное	средний	высокий	средний	20.03.2015	20.03.2
10	Угроза выхода процесса за пределы виртуальной машины	Угроза заключается в возможности запуска	Внешний нарушитель со средним потенциалом,	Информационная система,	средний	высокий	средний	20.03.2015	20.03.2
11	Угроза деавторизации санкционированного клиента беспроводной сети	Угроза заключается в возможности	Внешний нарушитель с низким потенциалом,	Сетевой узел			средний	20.03.2015	20.03.2
12	Угроза деструктивного изменения конфигурации/среды окружения	Угроза заключается в возможности	Внутренний нарушитель с низким потенциалом	Системное программное	средний	высокий	средний	20.03.2015	20.03.2
13	Угроза деструктивного использования декларированного функционала	Угроза заключается в возможности	Внутренний нарушитель с низким потенциалом	Микропрограммное		высокий		20.03.2015	20.03.2
14	Угроза длительного удержания вычислительных ресурсов пользователями	Угроза заключается в возможности	Внешний нарушитель с низким потенциалом,	Информационная система,			средний	20.03.2015	20.03.2
15	Угроза доступа к защищаемым файлам с использованием обходного пути	Угроза заключается в возможности получения	Внешний нарушитель с низким потенциалом,	Объекты файловой системы	средний			20.03.2015	20.03.2
16	Угроза доступа к локальным файлам сервера при помощи URL	Угроза заключается в возможности передачи	Внешний нарушитель со средним потенциалом	Сетевое программное	средний			20.03.2015	20.03.2
17	Угроза доступа/перехвата/изменения HTTP cookies	Угроза заключается в возможности	Внешний нарушитель с низким потенциалом	Прикладное программное	средний		средний	20.03.2015	20.03.2
18	Угроза загрузки нештатной операционной системы	Угроза заключается в возможности подмены	Внутренний нарушитель с низким потенциалом	Микропрограммное	средний	высокий	средний	20.03.2015	20.03.2
19	Угроза заражения DNS-кеша	Угроза заключается в возможности	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое	средний			20.03.2015	20.03.2
20	Угроза злоупотребления возможностями, предоставленными	Угроза заключается в возможности	Внутренний нарушитель с низким потенциалом	Облачная система,	средний	высокий	средний	20.03.2015	20.03.2
21	Угроза злоупотребления доверием потребителей облачных услуг	Угроза заключается в возможности нарушения	Внешний нарушитель с низким потенциалом	Облачная система	средний	высокий		20.03.2015	20.03.2
22	Угроза избыточного выделения оперативной памяти	Угроза заключается в возможности выделения	Внешний нарушитель с низким потенциалом,	Аппаратное обеспечение,			средний	20.03.2015	20.03.2
23	Угроза изменения компонентов системы	Угроза заключается в возможности получения	Внутренний нарушитель с низким потенциалом	Информационная система,		высокий	средний	20.03.2015	20.03.2
24	Угроза изменения режимов работы аппаратных элементов компьютера	Угроза заключается в возможности изменения	Внутренний нарушитель с высоким потенциалом	Микропрограммное и		высокий	средний	20.03.2015	20.03.2
25	Угроза изменения системных и глобальных переменных	Угроза заключается в возможности	Внутренний нарушитель со средним потенциалом	Системное программное	средний	высокий	средний	20.03.2015	20.03.2
26	Угроза искажения XML-схемы	Угроза заключается в возможности изменения	Внешний нарушитель со средним потенциалом,	Сетевой узел, сетевое		высокий	средний	20.03.2015	20.03.2
27	Угроза искажения вводимой и выводимой на периферийные устройства	Угроза заключается в возможности	Внешний нарушитель с высоким потенциалом,	Системное программное		высокий		20.03.2015	20.03.2
28	Угроза использования альтернативных путей доступа к ресурсам	Угроза заключается в возможности	Внешний нарушитель с низким потенциалом,	Сетевой узел, объекты	средний			20.03.2015	20.03.2
29	Угроза использования вычислительных ресурсов суперкомпьютера	Угроза заключается в возможности	Внешний нарушитель с низким потенциалом,	Вычислительные узлы			средний	20.03.2015	20.03.2
30	Угроза использования информации идентификации/аутентификации,	Угроза заключается в возможности	Внешний нарушитель со средним потенциалом,	Средства защиты	средний	высокий	средний	20.03.2015	07.07.2
31	Угроза использования механизмов авторизации для повышения	Угроза заключается в возможности получения	Внешний нарушитель с низким потенциалом,	Системное программное	средний			20.03.2015	20.03.2
32	Угроза использования поддельных цифровых подписей BIOS	Угроза заключается в возможности установки	Внешний нарушитель со средним потенциалом	Микропрограммное и		высокий		20.03.2015	20.03.2
33	Угроза использования слабостей кодирования входных данных	Угроза заключается в возможности	Внешний нарушитель со средним потенциалом,	Системное программное		высокий	средний	20.03.2015	20.03.2
34	Угроза использования слабостей протоколов сетевого/локального обмена	Угроза заключается в возможности	Внешний нарушитель с низким потенциалом,	Системное программное	средний			20.03.2015	20.03.2
35	Угроза использования слабых криптографических алгоритмов BIOS	Угроза заключается в сложности проверки	Внешний нарушитель с высоким потенциалом	Микропрограммное	средний	высокий	средний	20.03.2015	20.03.2
36	Угроза исследования механизмов работы программы	Угроза заключается в возможности	Внешний нарушитель со средним потенциалом,	Системное программное	средний		средний	20.03.2015	20.03.2
37	Угроза исследования приложения через отчёты об ошибках	Угроза заключается в возможности	Внешний нарушитель со средним потенциалом,	Системное программное	средний			20.03.2015	20.03.2
38	Уголога исцеплация выцислительных песиосле упацилина большиу данных	Vrnosa заключается в возможности впеменного	Вилтренций изглинитель с низумм потеннизиом	Ииформациониза система			спелиий	20.03.2015	20.03.7

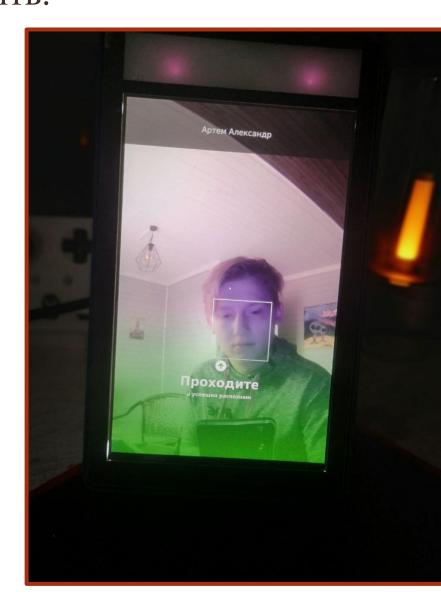
Проблемы с которыми сталкивались

При развертывании ПО биотерминала мы столкнулись с рядом проблем в работе лог-паса и сертефикатов 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.





Итоги

Сайт о проекте



GitHub

В ходе работы была развернута и изучена ИС биотерминала, разработаны схема взаимодействия её частей, модели угроз и руководство по защите ИС. На протяжении семестра мы вели GitHub репозиторий и сайт о проекте.



