УДК 004

Разработка системы для организации видеонаблюдения на предприятии ООО «Информикс-ДВ»

Азаров Андрей Евгеньевич
Приамурский государственный университет имени Шолом-Алейхема
Студент

Научный руководитель
Глаголев Владимир Александрович
Приамурский государственный университет имени Шолом-Алейхема
к.г.н., доцент кафедры информационных систем, математики и правовой информатики

Аннотация
В данной статье описан проект создания информационной системы по организации видеонаблюдения, включающий полный цикл разработки: проблему, анализ, моделирование, разработка.
Ключевые слова: разработка, видеонаблюдение, информационная система.

Development of a system for the organization of video surveillance in the company "Informix-DV"

Azarov Andrey Evgenevich
Sholom-Aleichem Priamursky State University
Student

Scientific adviser
Glagolev Vladimir Alexandrovich
Sholom-Aleichem Priamursky State University
candidate of geographical Sciences, associate professor of the Department of information systems, mathematics and legal informatics

Abstract
This article describes a project to create an information system for the organization of video surveillance, including the full development cycle: problem, analysis, modeling, development.
Keywords: development, cctv, information system.

История систем видеонаблюдения насчитывает около восьмидесяти лет. За эти восемьдесят лет изменились как технологии, так и общественное отношение к видеонаблюдению. На старте повсеместного внедрения общественных систем видеонаблюдения, в семидесятых годах двадцатого века, люди были против всеобщего слежения. Однако, позже, данные

системы были приняты обществом, так как было доказано на практике, что внедрение систем видеонаблюдения в общественных местах уменьшает уровень преступности в данном месте.

С технической стороны системы видеонаблюдения также прошли определенный путь развития. Первые камеры были черно белыми, далее в 1960-х годах появились первые цветные камеры. Системы видеонаблюдения, разработанные до 1990-х годов, записывали видео на видеокассеты, а после, в массовое распространение начали входить IP камеры – камеры способные передавать сигнал в цифровом виде по интернету. На данный момент камеры видеонаблюдения находятся почти в каждом магазине или общественном месте, также такие камеры используются для регистрации нарушений на дорогах и в некоторых странах массово вводятся различные системы распознавание лиц [12].

В статье журнала «Алгоритм безопасности» И. Подгорный проводит анализ классификации проводов и источников питания подходящих и неподходящих для систем видео наблюдения [7]. Источники питания бывают линейные, импульсные и резервные. Для современных систем видеонаблюдения наилучшим образом подходят импульсные источники питания. Про линейные источники можно сказать, что из-за слабой устойчивости к помехам и любым другим изменениям питания, данные источники могут легко выйти из строя и также вывести из строя оборудования для видеонаблюдения.

В 2015 году А. Мейв рассматривалась проблема выбора сервера для системы видео наблюдения [5]. Как в 2015 году, так и в настоящее время, не для каждой системы видео наблюдения необходимо покупать дорогостоящее оборудование. На данный момент существуют компактные и недорогостоящие сервера, отделенные от программного обеспечения, и в случаях, когда видеоинформацию необходимо только хранить, но никак не обрабатывать, то можно существенно сэкономить на закупке серверного оборудования. Так как ранее для систем видеонаблюдения серверное оборудование закупалось в комплекте с программным обеспечением или даже своей операционной системой, такие системы стоили намного дороже, чем сейчас сервера отдельно.

В статье В. Танина [11] говорится об обработке видеоинформации с помощью видео аналитики, когда изображение с помощью информационной системы связанной с камерами, обрабатывает видео, захватывает лица, распознаёт их или даже замечает кражу. Подобные функции не новинка, однако, для подобных функций по распознаванию образов необходимы дорогостоящие видеокамеры с высоким разрешением и поддержкой съёмки в темноте, не каждый работодатель готов к таким затратам. Также в статье делается вывод, что камеры необходимо выбирать от цели и дальнейшей эксплуатации, также выбор камеры зависит от разрешения камеры, светочувствительности (для наружных и для внутренних систем видеонаблюдения необходимы разные камеры).

Государственный стандарт России 51558-2014 [13] включает в себя подробную информацию о характеристиках системы видеонаблюдения. В данной работе будет затронуто несколько пунктов касающихся разработки проекта информационной системы видеонаблюдения. В ГОСТ сказано, что для отображения изображений с нескольких видеокамер рекомендуется использовать видеомониторы размера не менее 21" и разрешения не менее FullHD. для 16 камер использовать видеомонитор размером не менее 27" с разрешением не менее 2560x1440 пикселей. Должен присутствовать алгоритм сжатия видеосигнала. Данные требования формируют и повышают часть стоимости установки и разработки системы.

В главе 8, книги «CCTV Networking and Digital Technology» автора V. Damjanovski [14] можно ознакомиться с зарубежным опытом перехода с аналогового сигнала в цифровой, и узнать общую информацию о цифровых камерах, цифровом хранении данных и IP сетях.

В любой компании вопросу безопасности уделяют особое внимание и никогда ему не пренебрегают. Любые вложенные средства для создания безопасности в организации потенциально себя окупают [1-3]. Для разработки информационной системы видеонаблюдения необходимо разработать базу данных, которая будет хранить все необходимые данные для стабильной работы существующего функционала система. Также создаваемая база данных должна быть приведена к третьей нормальной форме.

Из-за существования множество различных проблем результатом работы будет готовая к установке и эксплуатации информационная система для организации видеонаблюдения на платформе Windows и проект, включающий в себя подробное описание всех функций, разработанных в системе, стоимость системы и будет рассчитана экономическая эффективность.

Предметной областью проекта является фирма ООО «Информикс-ДВ» которая осуществляет коммерческую деятельность по обслуживанию и ремонту компьютерного оборудования, которая в данный момент не имеет собственной системы видеонаблюдения.

Создание данной информационной системы направлено на обеспечение увлечения уровня безопасности в организации, в случаях краж или непредвиденных обстоятельств. Видео с камер наблюдения могут являться юридическим доказательством в суде.

Актуальность: Потенциальное предотвращение краж, взломов и других правонарушений. Контроль исполнения техники безопасности сотрудниками. Использование отснятого материала в качестве доказательств в суде в случаях предусмотренных законами российской федерации.

Цель работы: Разработка корпоративной базы данных для информационной системы по организации видеонаблюдения и программного обеспечения системы.

Объект исследования: обеспечение безопасности в организации.

Предмет исследования: Разработка информационной системы по организации видеонаблюдения и базы данных для неё.

Процесс создания системы видеонаблюдения состоит из нескольких шагов:

– анализ функционала и потребностей системы;
– проектирование базы данных;
– создание файла проекта базы данных;
– создание базы данных (формирование и связывание таблиц, ввод данных);
– создание дизайна ПО;
– связывание файлов дизайна с файлами программного кода;
– создание запросов и управляющих функций;
– автоматизирование формирования отчетов.

Результатом данной работы будет готовая к установке и эксплуатации информационная система для организации видеонаблюдения на платформе Windows и проект, включающий в себя подробное описание всех функций, разработанных в системе, стоимость системы и будет рассчитана экономическая эффективность. Основным практическим результатом работы системы являются записанные видеофайлы на жесткий диск компьютера.

Общий принцип работы любой системы видеонаблюдения всегда одинаковый у любой системы, вне зависимо от целей и организации, в которой производится видеонаблюдение.

Ниже рассмотрены все возможные действия работы системы и продемонстрированы основные функции.

После установки программного обеспечения на компьютер программное обеспечение информационной системы, к компьютеру подключают необходимое количество ip и веб камер. Ip камеры подключаются к сетевой карте через маршрутизатор, web камеры подключатся через usb-хаб.

Администратор системы по умолчанию имеет логин и пароль – admin, admin. При первом входе, система предлагает сменить пароль. Администратор добавляет подключенные камеры к информационной системе с помощью кнопок «Добавить» - «Web камера».

На рисунке 1 можно рассмотреть окно авторизации программы. При вводе логина и пароля во время каждого введенного символа вызывается функция по проверке данных из формы ввода с данными из базы данных. Логин проверяется в таком виде, в каком его вводит пользователь, а пароль во время ввода хешируются с помощью одностороннего алгоритма md5 и сравнивается с записями пароля в базе данных, которые хранятся только в шифрованном виде.

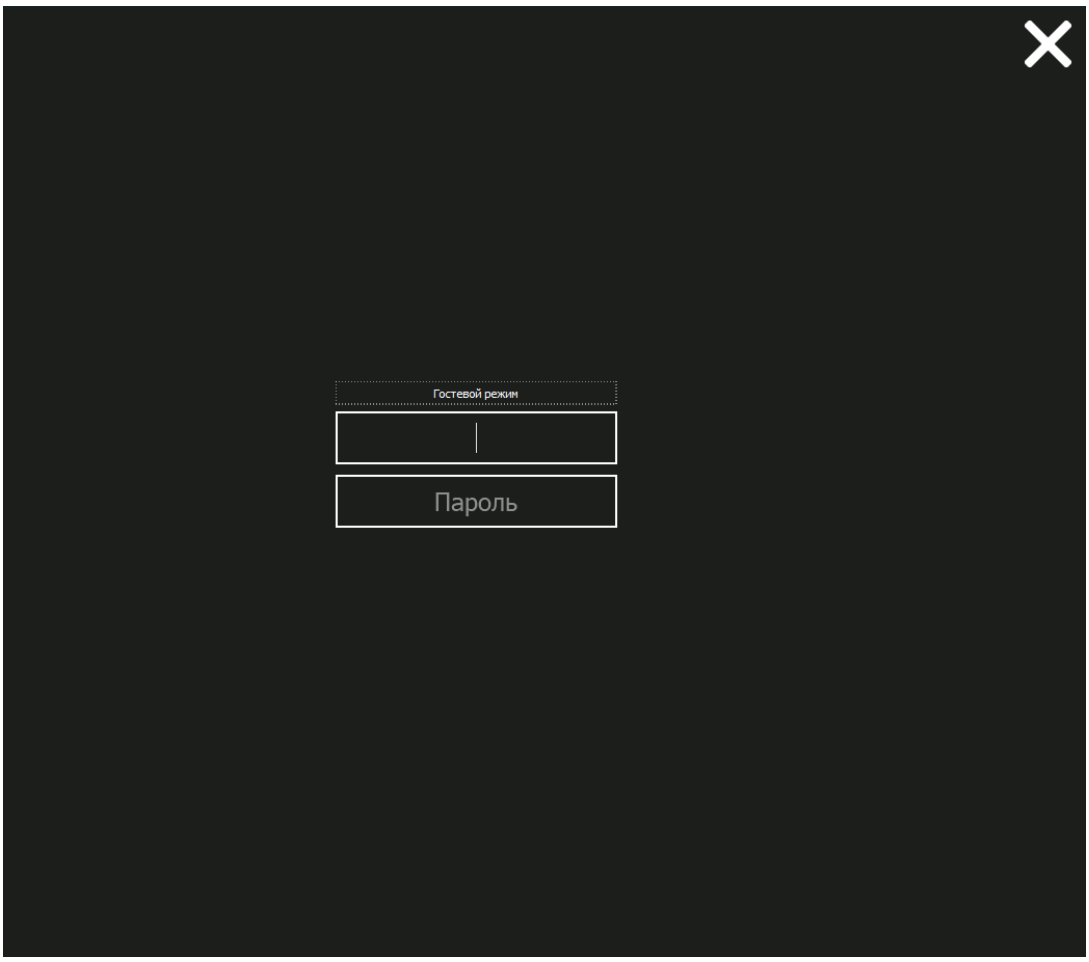

Рис. 1. Окно авторизации

На рисунке 2 изображен главный экран программы, экран открывается после ввода верного логина и пароля. Экран содержит изображения с видео камер в реальном времени, названия камер, кнопку добавить камеру, кнопку открытия видеоплеера, кнопку настроек, кнопку выхода, в правом нижнему углу отображается текущая дата и время, имя пользователя, которое одновременно и является кнопкой, открывающий панель с кнопкой сменить пользователя и открытием центра администрирования по управлению пользователями. В правом нижнем углу программы, есть кнопка, позволяющая редактировать текущую сетку отображения камер.

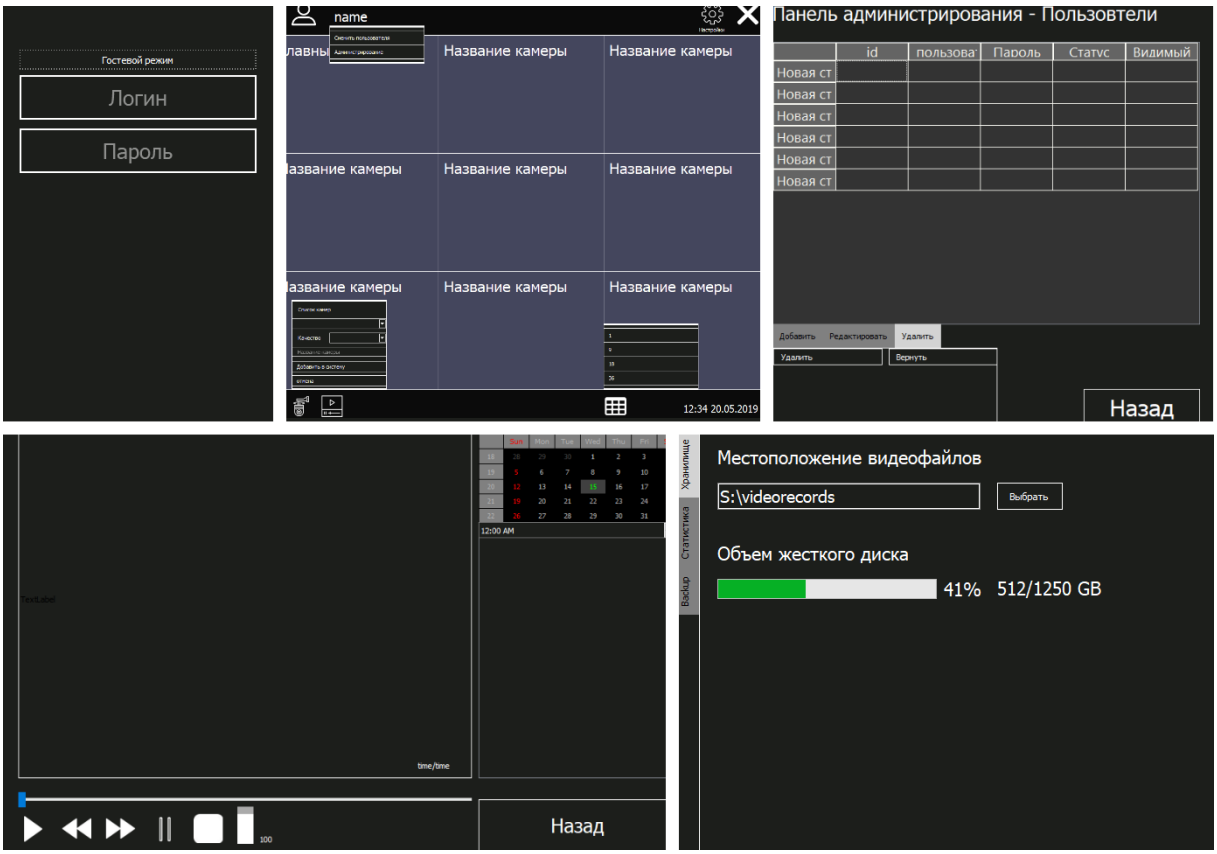

Рис. 2 Внешний вид форм программы

Следующий этап: описание классов с помощью объектно-ориентированной парадигмы языка python. На каждую форму создаётся отдельный класс: MainWindow, Player, Users, Settings.

Для каждого класса написаны функции, к которым имеется доступ вне данного класса. Для главного окна – функции авторизации, проверки прав доступа, работы с камерами, переименование камер, вывод изображения с камер на экран. Для плеера – функции просмотра файлов с папки, включение и отключение видео, пауза, перемотка, изменение громкости. Для окна администрирования раздела пользователей были реализованы следующий функции – просмотр всех активных пользователей, регистрация новых пользователей, удаление старых пользователей, редактирование данных о пользователях. Модуль settings включает в себя следующие выдавать информацию о объёме жесткого диска, местоположении хранения видеофайлов, информация о количество пользователей системы, информация о общей длительности всех записанных видео, количество видео, возможность сделать резервную копию файлов базы данных и функция восстановления базы данных.

Также реализовано множество различных функций, не зависящих друг от друга: добавление новой камеры, редактирование свойств любой подключенной камеры, редактирование сетки изображений, смена активного пользователя

Подключение и работа с базой данных осуществляется с помощью, встроенной СУБД sqlite и команд языка Python.

В заключении, с помощью встроенных утилит, файлы с расширением .py компилируются в .exe программу и далее с помощью программы Inno Setup создаётся готовый инсталлятор, который впоследствии создаст файлы деинсталляции, что непременно является преимуществом для будущего контроля над программой и компьютером.

Общий принцип работы любой системы видеонаблюдения всегда одинаковый у любой системы, вне зависимо от целей и организации, в которой производится видеонаблюдение.

Ниже рассмотрены все возможные действия работы системы и продемонстрированы основные функции.

После установки программного обеспечения на компьютер программное обеспечение информационной системы, к компьютеру подключают необходимое количество ip и веб камер. Ip камеры подключаются к сетевой карте через маршрутизатор, web камеры подключатся через usb-хаб.

Администратор системы по умолчанию имеет логин и пароль – admin, admin. При первом входе, система предлагает сменить пароль. Администратор добавляет подключенные камеры к информационной системе с помощью кнопок «Добавить» - «Web камера».

На рисунке 3 можно рассмотреть окно авторизации программы. При вводе логина и пароля во время каждого введенного символа вызывается функция по проверке данных из формы ввода с данными из базы данных. Логин проверяется в таком виде, в каком его вводит пользователь, а пароль во время ввода хешируются с помощью одностороннего алгоритма md5 и сравнивается с записями пароля в базе данных, которые хранятся только в шифрованном виде.

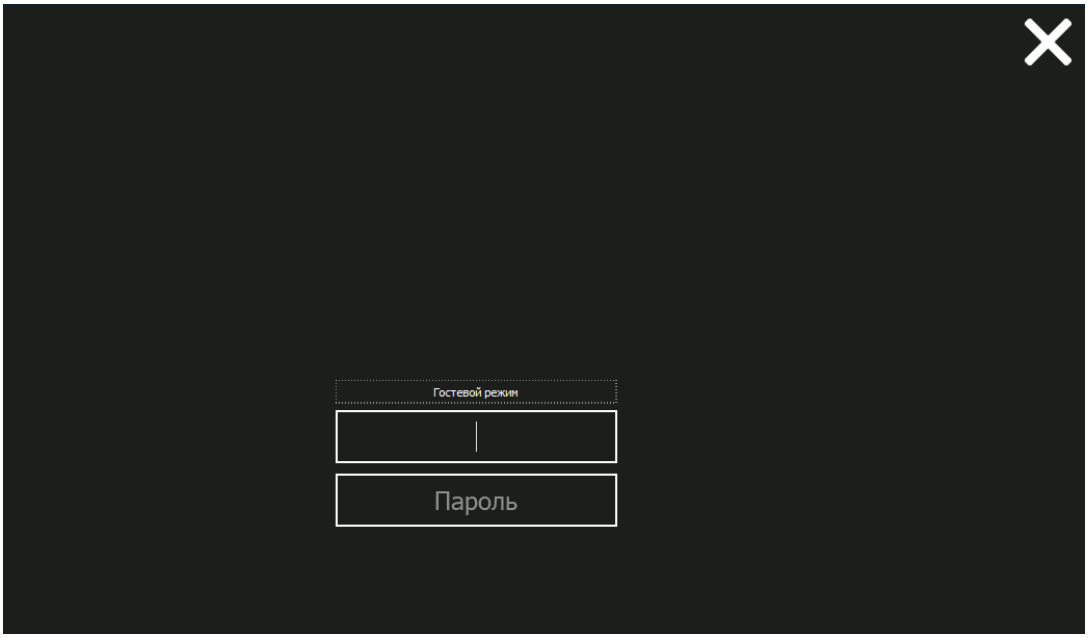

Рис. 3. Окно авторизации

На рисунке 4 изображен главный экран программы, экран открывается после ввода верного логина и пароля. Экран содержит изображения с видео камер в реальном времени, названия камер, кнопку добавить камеру, кнопку открытия видеоплеера, кнопку настроек, кнопку выхода, в правом нижнему углу отображается текущая дата и время, имя пользователя, которое одновременно и является кнопкой, открывающий панель с кнопкой сменить пользователя и открытием центра администрирования по управлению пользователями. В правом нижнем углу программы, есть кнопка, позволяющая редактировать текущую сетку отображения камер.

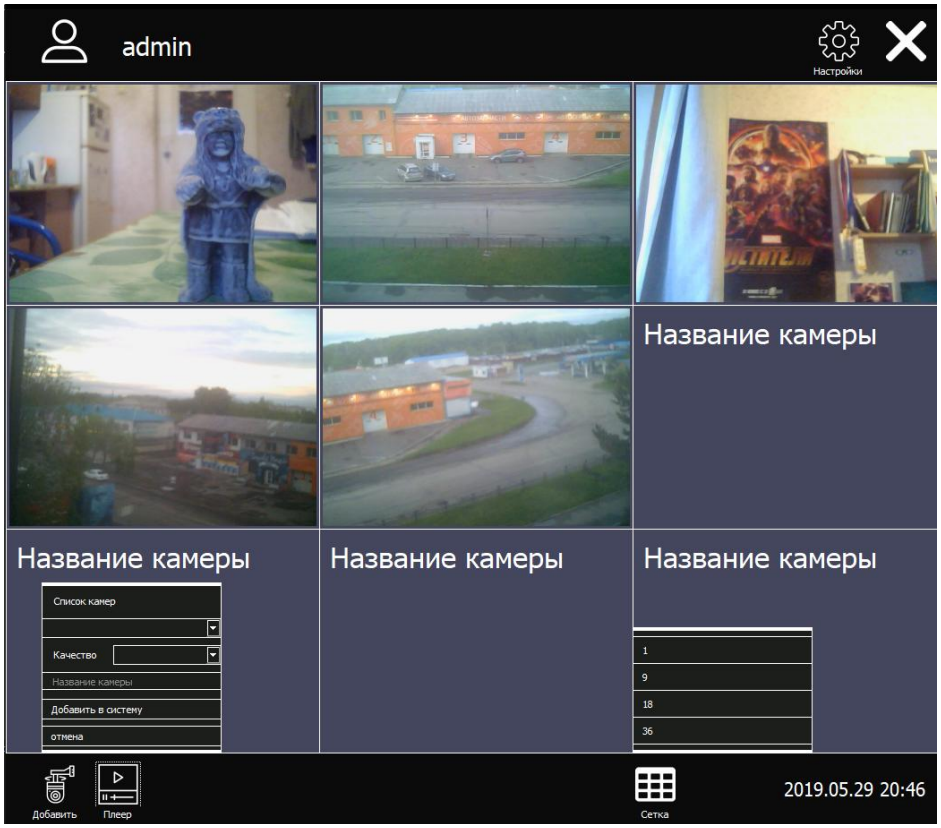

Рис. 4. Главное окно программы

Администратор имеет возможность регистрировать новых пользователей и устанавливать им различные права доступа. Чтобы открыть панель администрирования – Пользователи, необходимо нажать на имя пользователя и выбрать элемент выпадающего меня Администрирование. С помощью данного интерфейса можно просматривать текущих пользователей, редактировать их логины и пароли, изменять их права доступа и удалять пользователей. Согласно рекомендациям по проектированию информационных систем, накопленные данные и созданные существующие учетные данные лучше не удалять, а помечать их как архивные и нейтрализовать к ним доступ из системы.

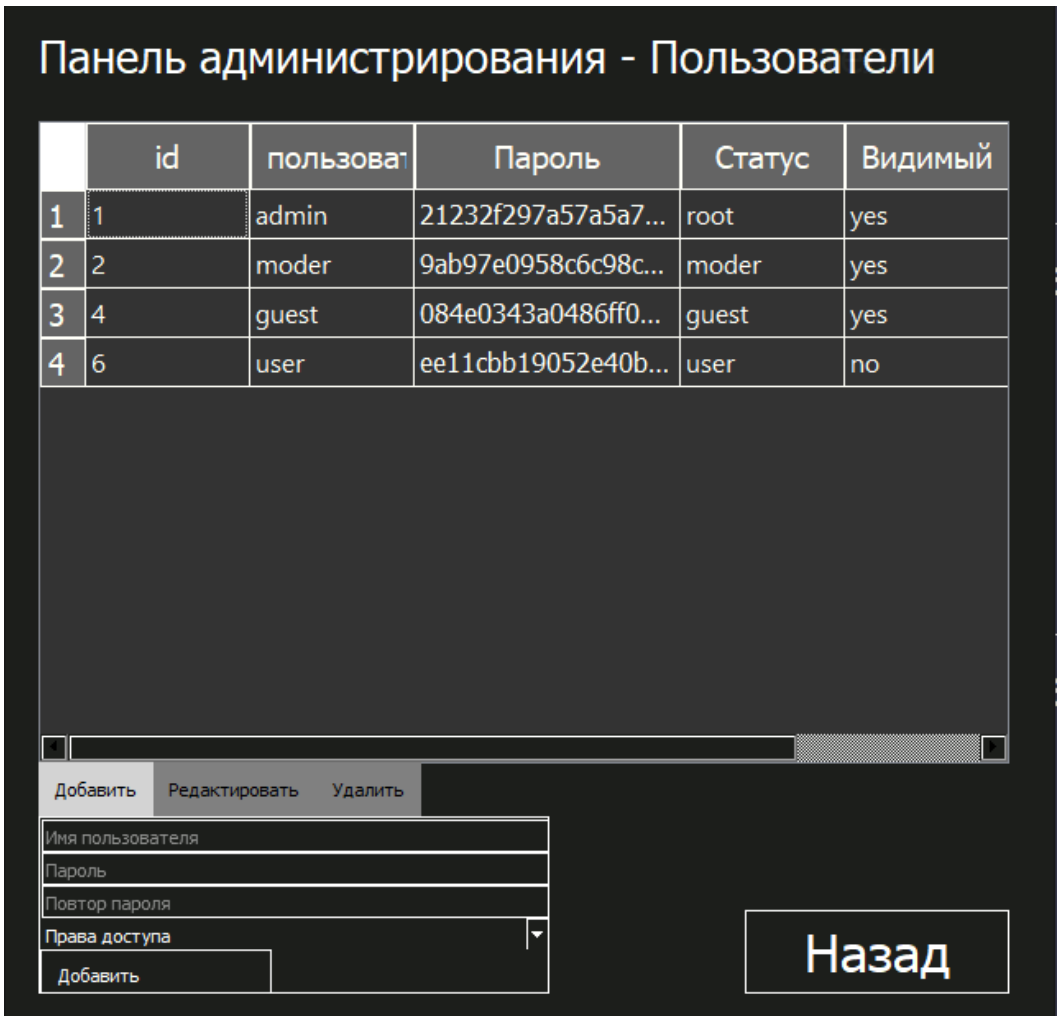

Рис. 5. Панель администрирования - Пользователи

Если нажать на имя пользователя, появится всплывающие окно, в котором будут определенные функции, меняющиеся в зависимости от прав доступа. У администратора появится две функции: «Сменить пользователя» и «Администрирование».

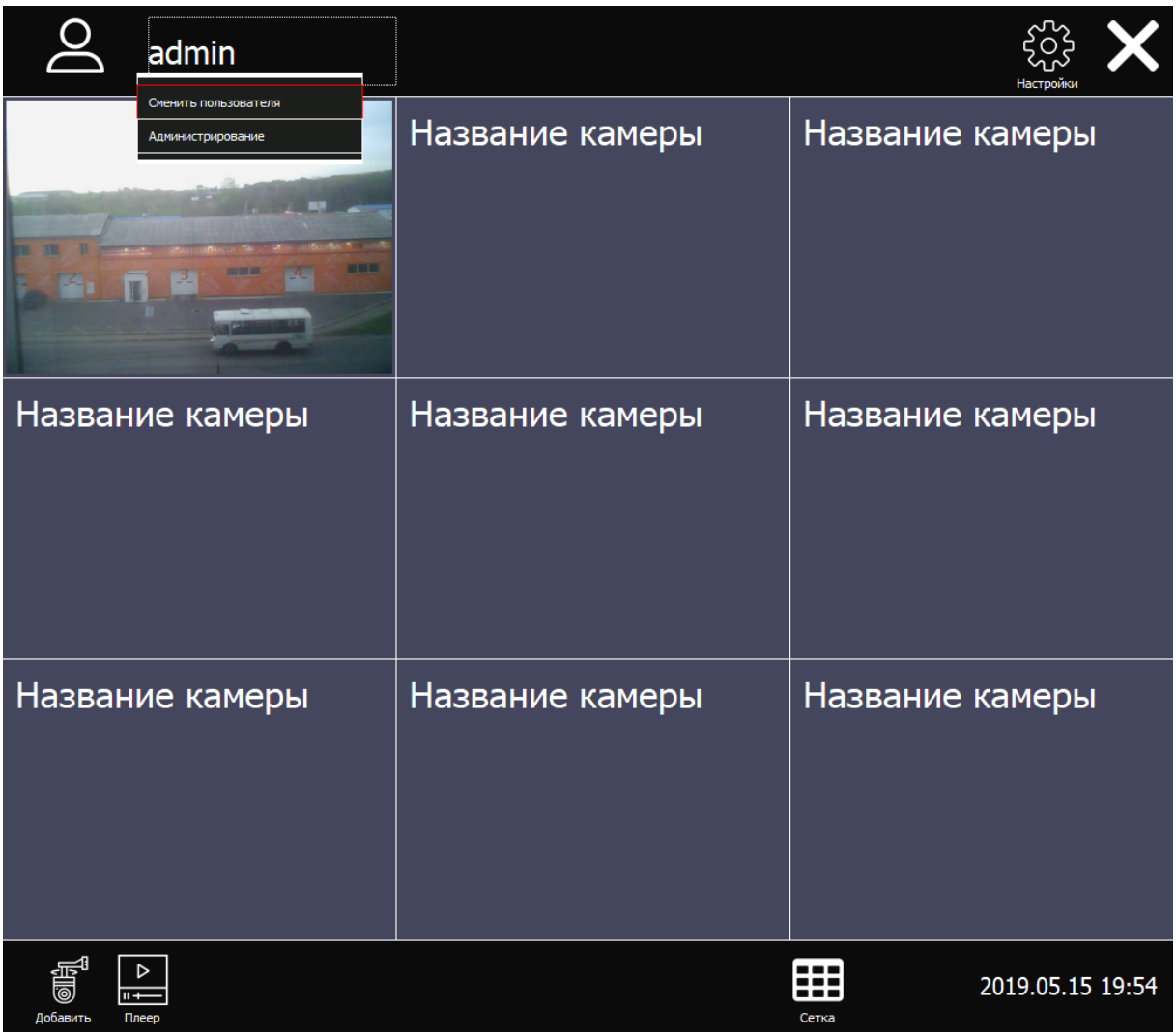

Рис. 6 Функция сменить пользователя появляется при нажатии на логин

На рисунке 6 изображен вариант сетки – 1, когда одна камера отображается на всю рабочую область системы.

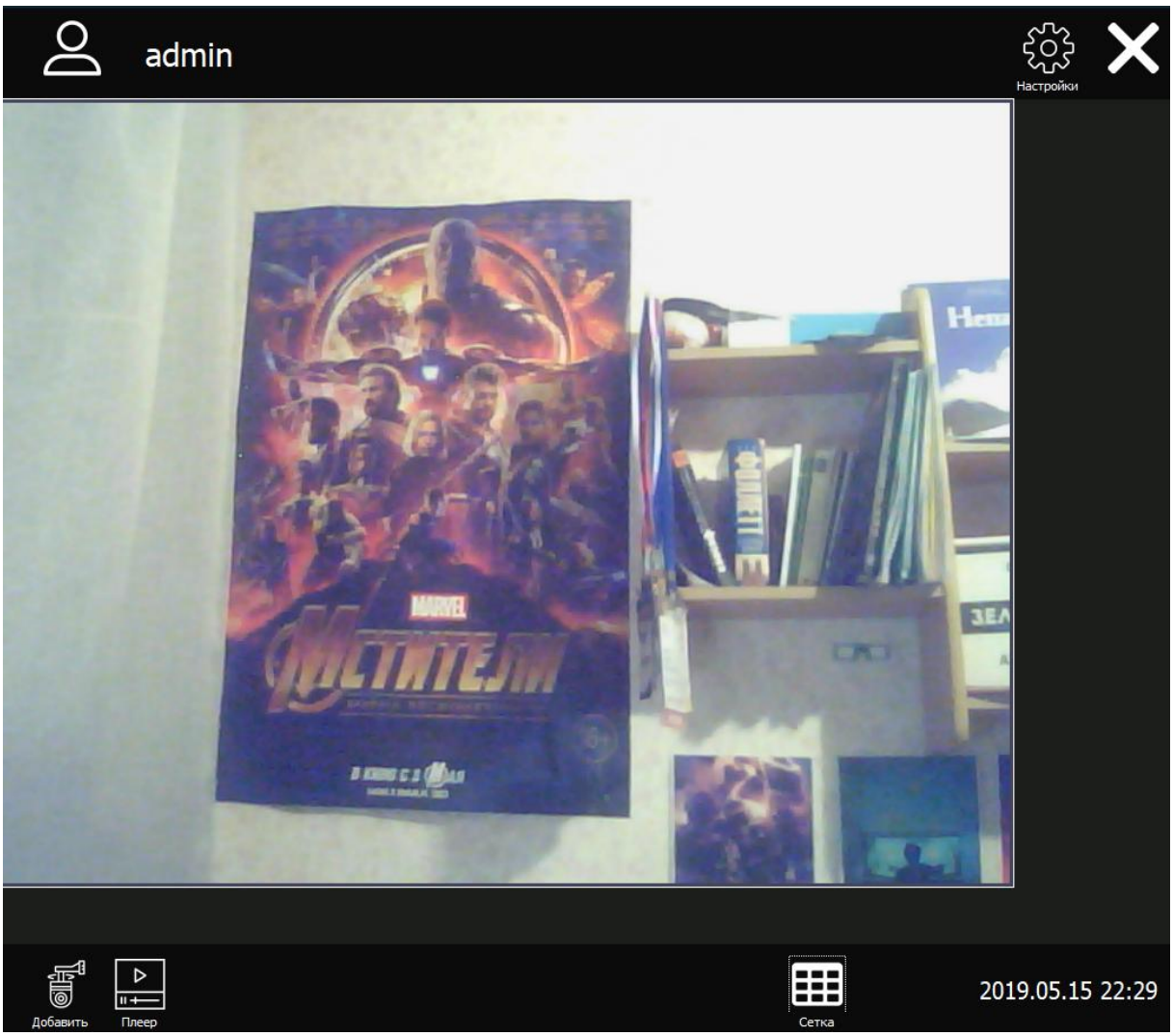

Рис. 7. Смена сетки камеры на 1 камеру

Ни одна система видеонаблюдения не обходится без встроенного видео плеера, который позволяет просматривать снятый и накопленный видеоматериал. На рисунке 7 изображен видеоплеер со следующими функциями: проигрывание видео, пауза, остановка, перемотка, изменение громкости (при условии, что в камере был микрофон и звуки записывались), поиск видео с помощью календаря.

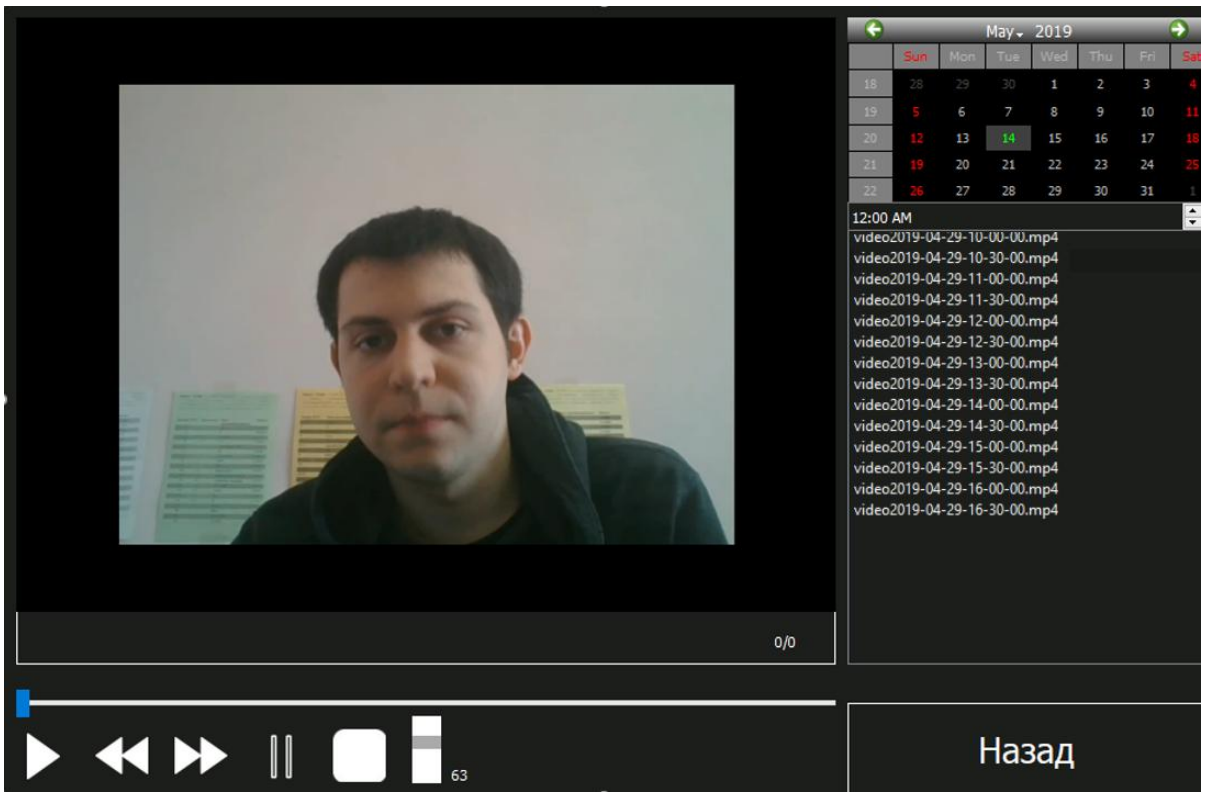

Рис. 8. Встроенный видеоплеер

В главном окне программы, в правом верхнем углу интерфейса программы отображается иконка шестеренки, которая открывается по нажатию на неё окно настройки программы. Окно настройки программы включает в себя следующие функции: модуль «Хранилище» с информацией о объёме жесткого диска и местоположении хранения видеофайлов, модуль «Статистика» с информацией, хранящейся в базе данных – количество пользователей, общая длительность записанных видео, количество видео, модуль «Backup» с возможностью сделать резервную копию файлов базы данных и функцией восстановления данной базы. На рисунке 9 изображено окно настройки открытое на вкладке «Хранилище».

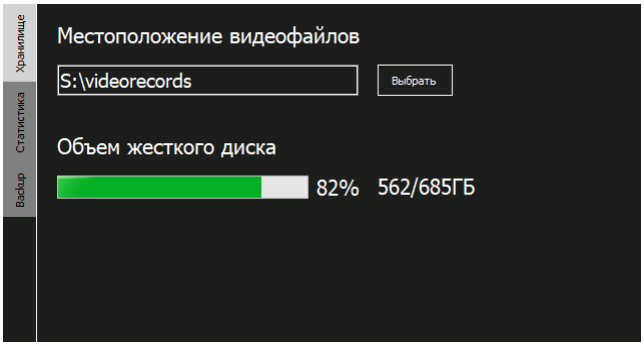

Рис. 9. Окно настройки – вкладка Хранилище

На рисунке 10 изображено окно настройки открытое на вкладке «Хранилище» и «Backup». Backup создаёт резервную копию текущей базы данных в выбранное место пользователя.

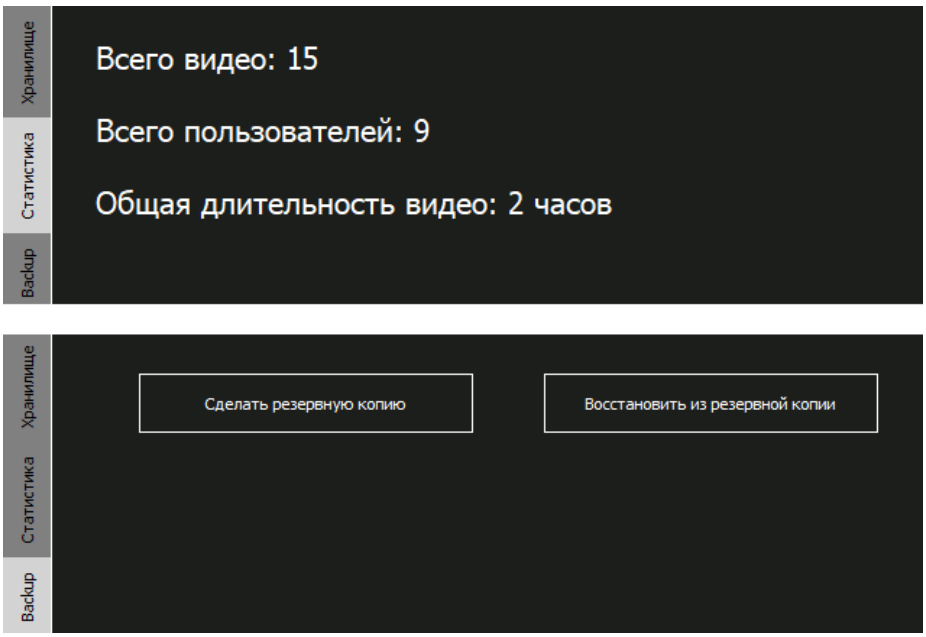

Рис. 10 Окно Статистика и Backup в настройках программы

Для контроля действий пользователей ведётся логирование основных действий: авторизация, выход, открытие плеера, открытие настроек, ошибка неверного ввода пароля. На рисунке 11 продемонстрирована таблица из базы данных с историей действий.

id	login	time	action
	Filter	Filter	Filter
6	user	2019.05.26 1...	Exit
7	admin	2019.05.26 1...	Authorization
8	admin	2019.05.26 1...	Open user wi...
9	admin	2019.05.26 1...	Exit
10	admin	2019.05.26 1...	Wrong passw...
11	admin	2019.05.26 1...	Authorization
12	admin	2019.05.26 1...	Exit
13	admin	2019.05.26 1...	Authorization
14	admin	2019.05.26 1...	Open player
15	admin	2019.05.26 1...	Exit
16	user	2019.05.26 1...	Authorization
17	user	2019.05.26 1...	Open player
18	user	2019.05.26 1...	Exit
19	moder	2019.05.26 1...	Authorization
20	moder	2019.05.26 1...	Exit

Рис. 11 Таблица истории действий пользователей

Расчет надежности – это процесс обнаружения и устранения ошибок программного обеспечения. Методы устранения ошибок делятся на два класса: статические методы, включающие анализ программы без ее выполнения, и методы тестирования, включающие выполнения программы на заданных тестах. Тестирование связано со значительным расходом машинного времени. Независимо от усилий, предпринимаемых на разных фазах разработки программы, для достижения высокой надежности программы необходимо проверить ее. При тестировании системы, основное внимание было уделено поиску ошибок интерактивным методом и методом поиска ошибок пользователями.

Валидация входных данных осуществляется с помощью стандартных средств pyqt: модуля pyqt validator, а также с помощью отдельных функций, написанных на языке python.

Проверка работоспособности валидации входных форм и полей

При создании нового пользователя администратором, системой проводится валидация всех полей. На рисунке 12 результаты работы проверки на валидация данных. Проверяется заполненность всех полей формы, проверка совпадения введенных паролей и проверка, выбраны ли права доступа для пользователя.

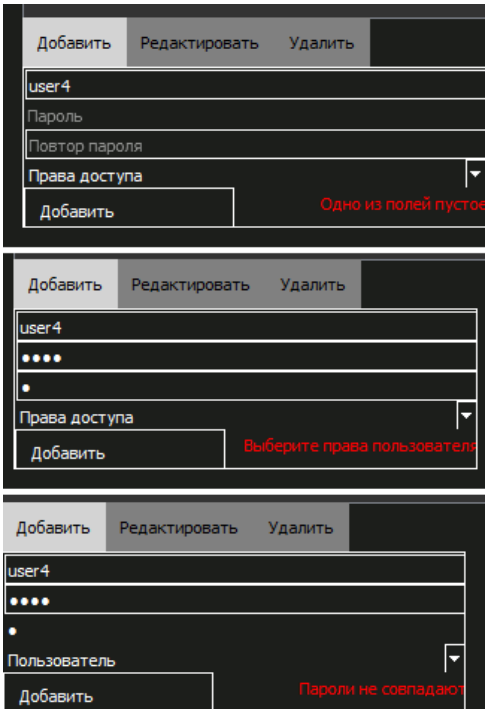

Рис. 12. Валидация полей добавление пользователя

Проверка разграничения доступа

Если попытаться открыть настройки системы, будучи авторизированным обычным пользователем, то можно увидеть, что доступ к разделу с настройками у пользователя отсутствует, данный вариант продемонстрирован на рисунке 13.

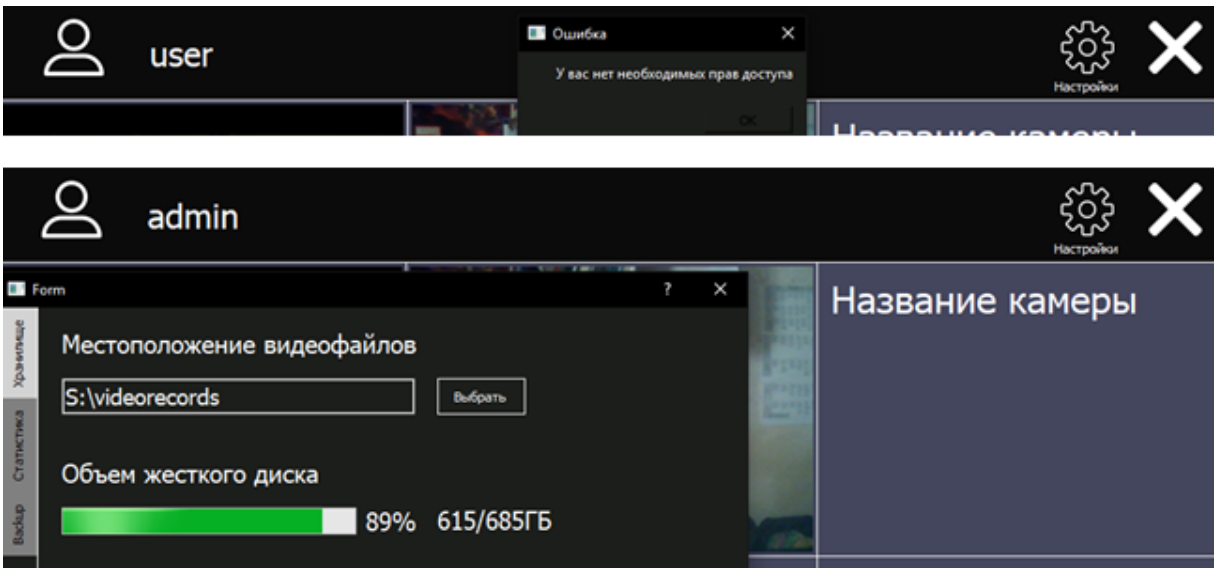

Рис. 13. Доступ к настройкам

Разграничение доступа влияет не только на работу доступа к настройкам системы, но и доступу к модулю администрирования. Если авторизоваться под администратором, то при нажатии на имя пользователя, откроется панель с двумя пунктами, пункт «Сменить пользователя» и пункт «Администрирования», если авторизуемый является обычным пользователем, то будет доступно только одно поле «Сменить пользователя». Данная проверка разграничения прав доступа изображена на рисунке 14

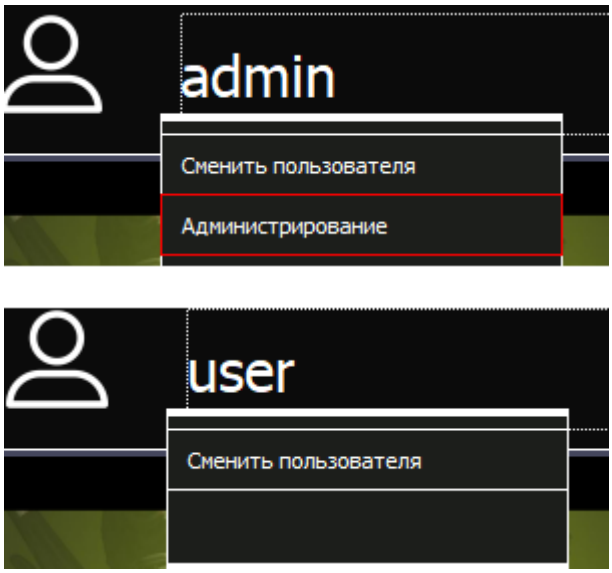

Рис. 14. Доступ к разделу администрирования

Также существуют и физические ограничения с работой системы, связанные с типами используемого оборудования, если использовать только web камеры, то максимум можно использовать только около двадцати камер на мощном компьютере, иначе очень сильно падает частота кадров из-за нагрузки потоков видео через обычный провод. Для IP камер такие

ограничения также существуют, но менее значимы по сравнению с web камерами.

Библиографический список

1. Алешин А. П. Техническое обеспечение безопасности бизнеса. М.: Дашков и К, 2010.
2. Антощук С. Г. и др. Моделирование алгоритмов анализа аварийных ситуаций при видеонаблюдении за дорожным движением //Електротехнічні та комп'ютерні системи. 2011. №. 2. С. 76-81
3. Ибатуллин Л. Р. Система видеонаблюдения и сетевое обеспечение в офисном помещении : дис. Южно-Уральский государственный университет, 2018.
4. Лыткин А. IP-видеонаблюдение. – 2011.
5. Мейев А. Выбор сервера для системы видеонаблюдения // Алгоритм безопасности. 2015. №3. С. 42-43.
6. Никитин В., Ефимов М. Особенности использования видеокомпрессии MPEG-4 в сетевом видеонаблюдении //Алгоритм безопасности. 2006. №. 2. С. 16-19.
7. Подгорный И. Организация питания для систем видеонаблюдения // Алгоритм безопасности. 2011. №6. С. 18-19.
8. Прокудин В. В. Видеонаблюдение как важный элемент противодействия посягательствам на честь и достоинство сотрудников УИС //Ведомости уголовно-исполнительной системы. 2015. №. 4. С. 25.
9. Смоленков Г. С. Проектирование системы IP–видеонаблюдения: дис. – Сибирский федеральный университет, 2018.
10. Соловьева-Опошнянская А. Ю. Видеонаблюдение как механизм обеспечения безопасности личности //Право и управление. XXI век. 2015. №. 2. С. 140-
11. Танин В. Поговорим о понятиях? Или профессиональный взгляд на IP-видеонаблюдение // Алгоритм безопасности. 2014. №6. С. 16-17.
12. Хаустов С. Н. Современные системы видеонаблюдения, этапы развития //Вестник Воронежского института МВД России. 2008. №. 1
13. ГОСТ Р 51558-2014 // Единая база ГОСТов РФ URL: http://gostexpert.ru/gost/gost-51558-2014 (дата обращения: 27.11.2018).
14. Damjanovski V. CCTV Networking and Digital Technology. 3 изд. Амстердам: Elsevier, 2014. 616 с.