Forensic Alliance

itsec® ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

Надлежащее процессуальное оформление результатов работы DLP-систем

Александра Гончарова
юрист Московской коллегии адвокатов «Юлова и партнеры»,
сооснователь Forensic Alliance

Forensic Alliance

Доказательства должны быть:

1 ДОПУСТИМЫМИ

2 ОТНОСИМЫМИ

3 ДОСТОВЕРНЫМИ

МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ ЮЛОВА И ПАРТНЕРЫ

Допустимость доказательства

- строго формализованное правило, которое предъявляется к

Источнику доказательства

Способу сохранения в нем информации

Его процессуальной форме

Forensic Alliance

Требования к источникам доказательств

«Служебное» и «частное»

Локальные нормативные акты, трудовые договоры и должностные инструкции, разграничивающие «служебное» и «частное», **с запретом на копирование и пересылку** служебной информации

Право распоряжаться информацией

Подписные листы Работника с уведомлением **о праве Работодателя** по своему усмотрению **распоряжаться** информацией из переписки в электронной почте, рабочих чатах, рабочих документов

Коммерческая тайна

Локальные нормативные акты **о запрете на разглашение коммерческой тайны**

МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ ЮЛОВА И ПАРТНЕРЫ

Способы сохранения доказательств

Скриншоты

Фотографирование экрана

Копирование на материальный носитель

Распечатывание файлов, переписки

Хранение в интернете, на сервере, в облачном хранилище

Процессуальная форма доказательств

Письменные доказательства

Вещественные доказательства

ст. 55 ГПК РФ, ст. 74 УПК РФ, ст. 64 АПК РФ, ст. 26.2 КоАП РФ

Письменные доказательства

электронные документы, иные документы, электронные образы документов и т.п., зафиксированные на бумажных носителях

Допустимость

- ✓ **надлежаще оформленный акт,** фиксирующий действия и/или место доказательства (подписи, данные лиц, составивших акт, соответствующее содержание, указание места, времени, ссылка на Приказ о назначении служебной проверки и/или на оказание юридической помощи адвокатом и др.)

- ✓ **нотариально оформленный способ обеспечения доказательства**: протокол, акт осмотра доказательства, акт осмотра информации в интернете и др.

Вещественные доказательства

материальные носители (флешкарты/внешние жесткие диски)

Допустимость

- ✓ **упакованные надлежащим образом**, предотвращающим их несанкционированное вскрытие.

Процессуальная форма доказательств

Материалы служебной проверки

Адвокатское расследование

Осмотр и обеспечение доказательств нотариусом

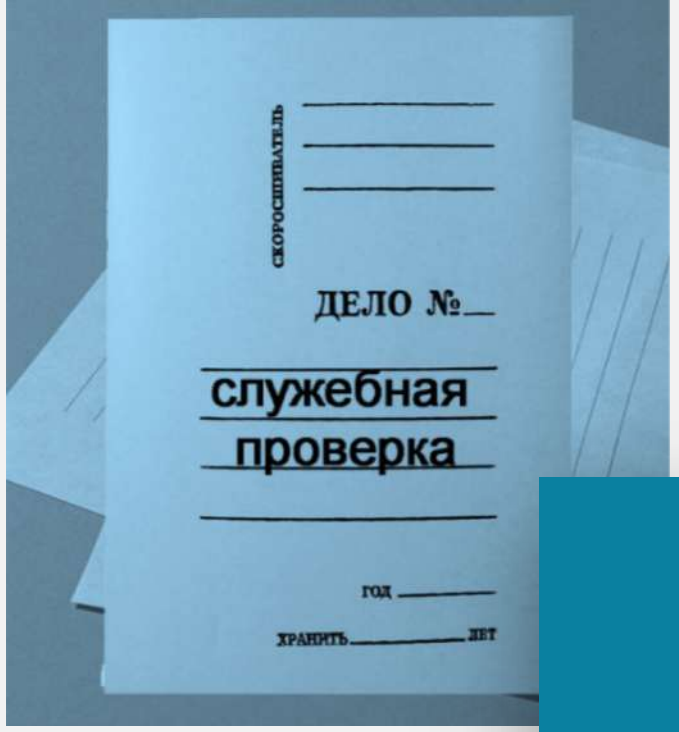
В совокупности с локальными нормативными актами, устанавливающими:

1. **Факт использования** программного комплекса
2. **Цель использования** программного комплекса, в том числе, для хранения сообщений в архиве и информирования о событиях администратора безопасности
3. **Правовое положение о СБ**

Пример:

Руководство «Обеспечение информационной безопасности при эксплуатации средств вычислительной техники и корпоративной вычислительной сети»

Forensic Alliance

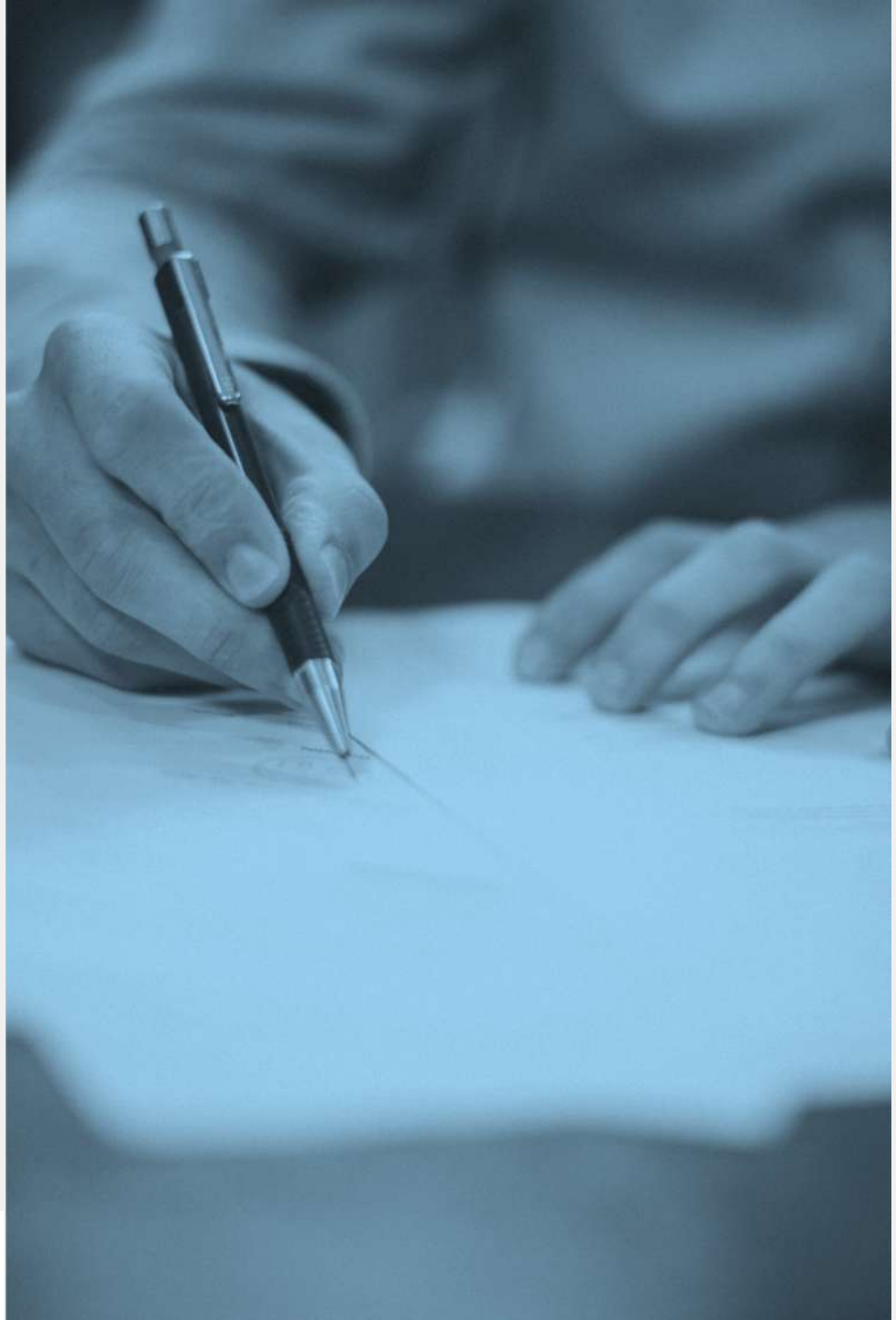


Служебная проверка

- Повод
- Назначение
- Письменные доказательства
- Вещественные доказательства
- Заключение специалистов (экспертов)
- Материалы фото- и киносъемки, аудио- и видеозаписи
- Зафиксированные DLP-системами инциденты

МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ ЮЛОВА И ПАРТНЕРЫ

Forensic Alliance



Субъекты проведения служебной проверки

- ✓ **Надлежащим образом** уполномоченные работники проверяемого лица
- ✓ Адвокаты

МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ ЮЛОВА И ПАРТНЕРЫ

Дело №33-90/11

Кассационное определение Судебной коллегии по гражданским делам Верховного Суда Удмуртской Республики

Дано:

Отправка **сообщения**, содержащего банковскую тайну, **зафиксированная DLP-системой**, что подтверждено **актом по факту выполнения копий с экрана**

Доводы работника:

1. **не доказано,** что информация **была использована**
2. с моего почтового адреса, но **не мной**

ДОКАЗАТЕЛЬСТВА РАБОТОДАТЕЛЯ

1. **Факт использования** программного комплекса
2. **Цель использования** программного комплекса, в том числе, для хранения сообщений в архиве и информирования о событиях администратора безопасности
3. Служебная записка начальника отдела информационной безопасности
4. Служебная записка директора
5. Акт о результатах служебного расследования

Дело №33-90/11

Довод работника:

1. не доказано, что информация из письма **была использована**

Опровергнут:

- **нормативным актом РД 45.134-2000:**

«сообщение с одного почтового сервера на другой отправляется только в том случае, если принимающий почтовый сервер сообщает о готовности принять электронное сообщение с посылающего почтового сервера и адресат на принимающем почтовом сервере существует»

- **ответом провайдера:**

«почтовый адрес, на который была зафиксирована отправка сообщения находился в активном состоянии, что подразумевает поступление на него электронных сообщений со всех внешних адресов».

Дело №33-90/11

Довод работника:

2. **С моего** почтового адреса**, но не мной**

НЕ ОПРОВЕРГНУТ

Работодателем не представлено доказательств тому, что сообщение было отправлено непосредственно работником, зафиксирован лишь факт отправки с электронного адреса, открытого на имя работника

ВЫВОДЫ СУДА

1. Поскольку информация попала в обладание третьего лица, то есть фактически стала ему известна, **факт разглашения считается установленным**, поскольку не имеет юридического значения факт прочтения сотрудниками третьего лица электронного сообщения и последующее удаление почтового адреса, на который сообщение поступило, поскольку разглашение окончено с момента поступления информации в обладание третьего лица
2. **Отсутствуют доказательства вины работника** в разглашении информации, DLP-система зафиксировала только факт отправки сообщения с электронного адреса, **но не лицо**

Forensic Alliance

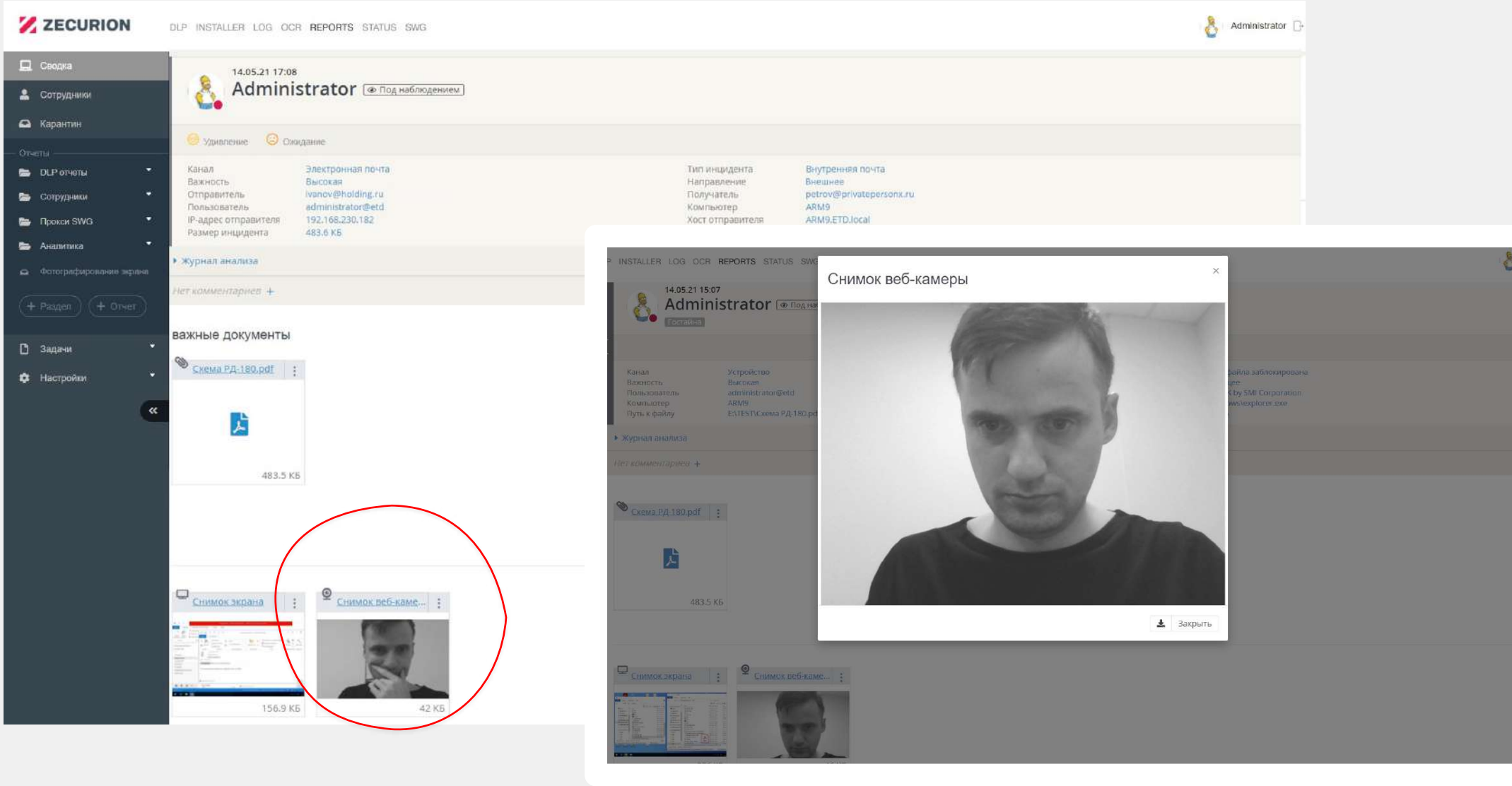
Дело №33-90/11

1. Доводы Работника о нарушении его прав на неприкосновенность частной жизни, защиту персональных данных в связи с проведенной проверкой не обоснованы
2. Работодатель осуществлял контроль за использованием своих информационных ресурсов, использование которых предусмотрено только в связи со служебной деятельностью работника
3. Работодатель в результате проверки не нарушил требования ч. 3 ст. 86 ТК РФ, так как не добывал никакой информации о персональных данных истца без его ведома, данная проверка связана с осуществлением мероприятий по информационной безопасности общества.

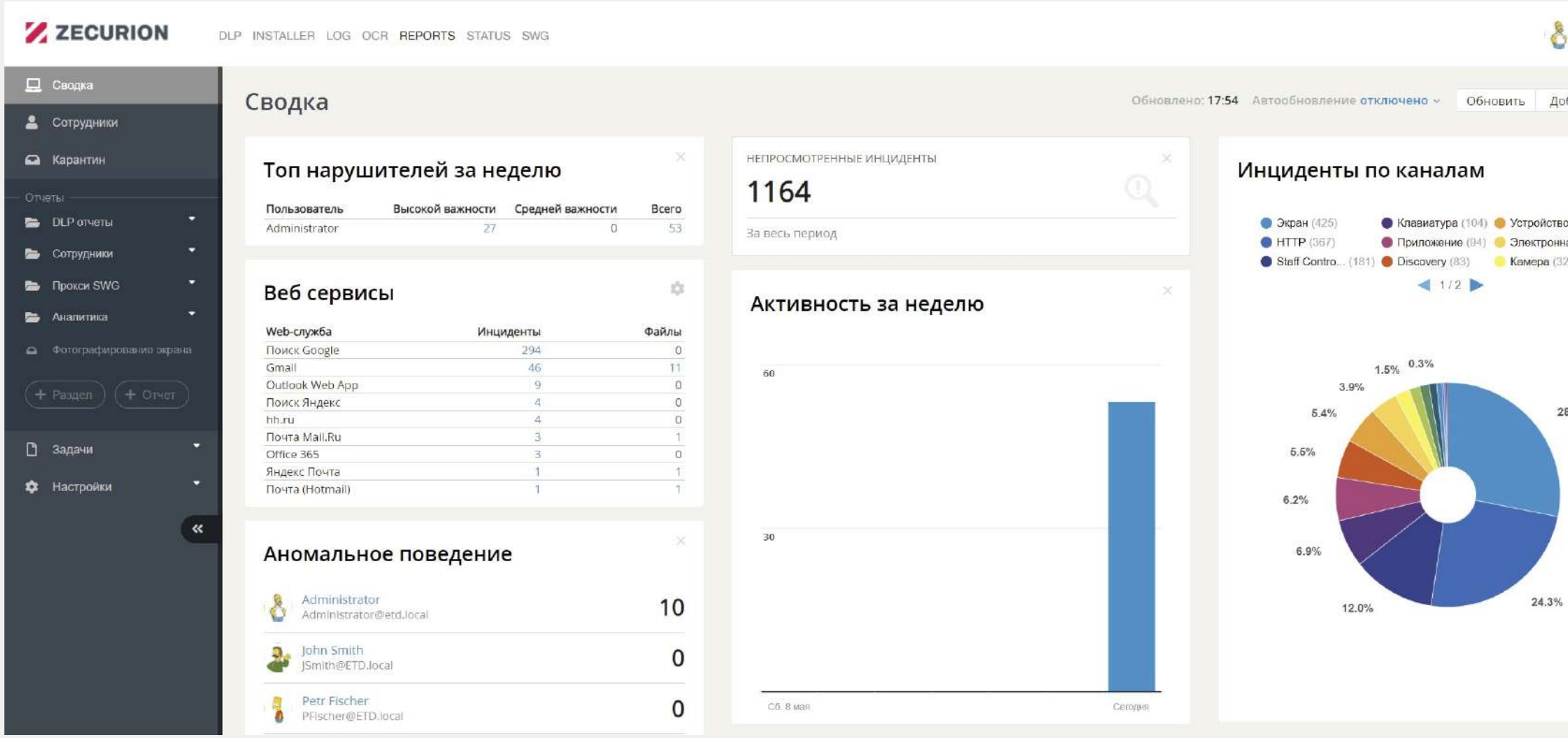
МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ ЮЛОВА И ПАРТНЕРЫ

ВЫВОДЫ СУДА

Что делать?


ZECURION
DLP INSTALLER LOG OCR REPORTS STATUS SWG
Administrator
Сводка
Сотрудники
Карантин
Отчеты
DLP отчеты
Сотрудники
Прокси SWG
Аналитика
Фотографирование экрана
+ Раздел
+ Отчет
Задачи
Настройки
14.05.21 17:08
Administrator
Под наблюдением
Удивление
Ожидание
Канал Электронная почта
Важность Высокая
Отправитель ivanov@holding.ru
Пользователь administrator@etd
IP-адрес отправителя 192.168.230.182
Размер инцидента 483.6 КБ
Тип инцидента Внутренняя почта
Направление Внешнее
Получатель petrov@privatepersonx.ru
Компьютер ARM9
Хост отправителя ARM9.ETD.local
Журнал анализа
Нет комментариев +
важные документы
Схема РД-180.pdf
483.5 КБ
Снимок экрана
156.9 КБ
Снимок веб-каме...
42 КБ
14.05.21 15:07
Снимок веб-камеры
Закрыть

Стартовая страница



Подотчет по всем инцидентам

ZECURION DLP INSTALLER LOG OCR REPORTS STATUS SWG

Сводка
Сотрудники
Карантин
Отчеты
DLP отчеты
Сотрудники
Прокси SWG
Аналитика
Фотографирование экрана
+ Раздел + Отчет
Задачи
Настройки

Сводка > Подотчет за 14.05.2021

Обновлено: 18:00 Автообновление отключено Обновить

Подотчет за 14.05.2021

Вид стандартный

выделить все Быстрый поиск... Сортировка время снача

Administrator → Petr Fischer Гостайна 17:08
Схема РД-180.pdf **Внутренняя почта** важные документы *В письме высылаю документ...*

Administrator → Petr Fischer Гостайна 17:06
Схема РД-180.pdf **Внутренняя почта** Важные документы *В письме высылаю документы. Возможно...*

Administrator → Petr Fischer Гостайна 17:06
Схема РД-180.pdf **Внутренняя почта** Важные документы *В письме высылаю документы. В...*

Administrator на ARM9 Staff Control 17:01
Вход пользователя в систему

Administrator → Petr Fischer Гостайна 15:44
Внутренняя почта гос тайна

Administrator Гостайна 15:10
Схема РД-180.pdf **Внутренняя почта** Важный документ *Документ содержит гос тайна*

Administrator → USB DISK by SMI Corporation Гостайна 15:07
Схема РД-180.pdf **Запись файла заблокирована**

Administrator → USB DISK by SMI Corporation Гостайна 15:04
Схема РД-180.pdf **Запись файла заблокирована**

Zecurion Reports. Версия 6.0.0.3457

14.05.21 17:08
Administrator Под наблюдением
Гостайна

Удивление Ожидание

Канал	Электронная почта	Тип инцидента	Внутренняя почта
Важность	Высокая	Направление	Внутреннее
Отправитель	administrator@etd.local	Получатель	pfischer@etd.local
Пользователь	administrator@etd	Компьютер	ARM9
IP-адрес отправителя	192.168.230.182	Хост отправителя	ARM9.ETD.local
Размер инцидента	483.6 КБ		

Журнал анализа

Нет комментариев +

важные документы

Схема РД-180.pdf
483.5 КБ

В письме высылаю документы. Возможно есть гос тайна

Инцидент: Копирование на флешку

14.05.21 15:07

Administrator Под наблюдением

Гостайна

Канал	Устройство	Тип инцидента	Запись файла заблокирована
Важность	Высокая	Направление	Исходящее
Пользователь	administrator@etd	Устройство	USB DISK by SMI Corporation
Компьютер	ARM9	Процесс	C:\Windows\explorer.exe
Путь к файлу	E:\TEST\Схема РД-180.pdf	Размер инцидента	483.5 КБ

Журнал анализа

Нет комментариев +

Схема РД-180.pdf

483.5 КБ

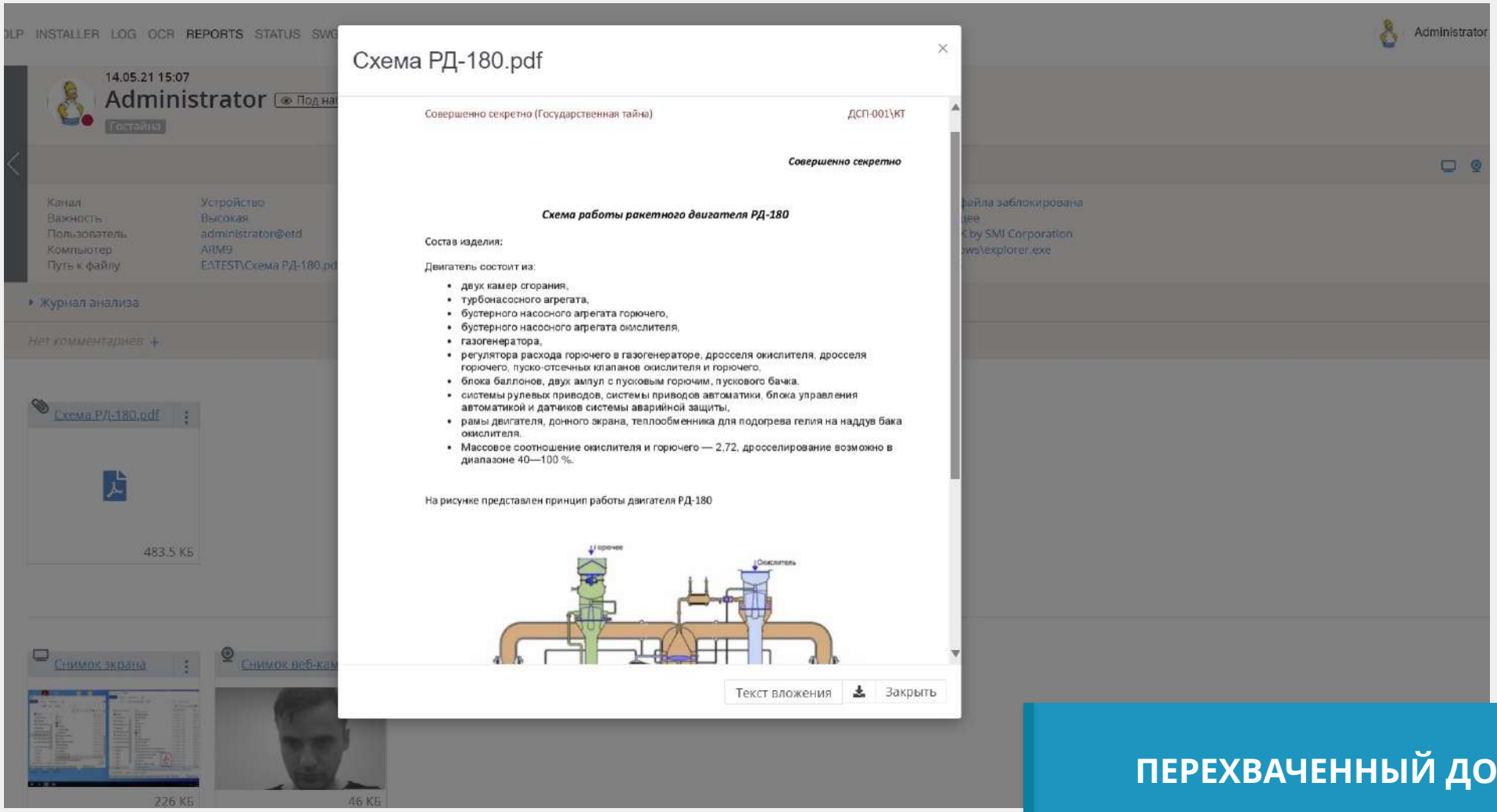
Снимок экрана

226 КБ

Снимок веб-каме...

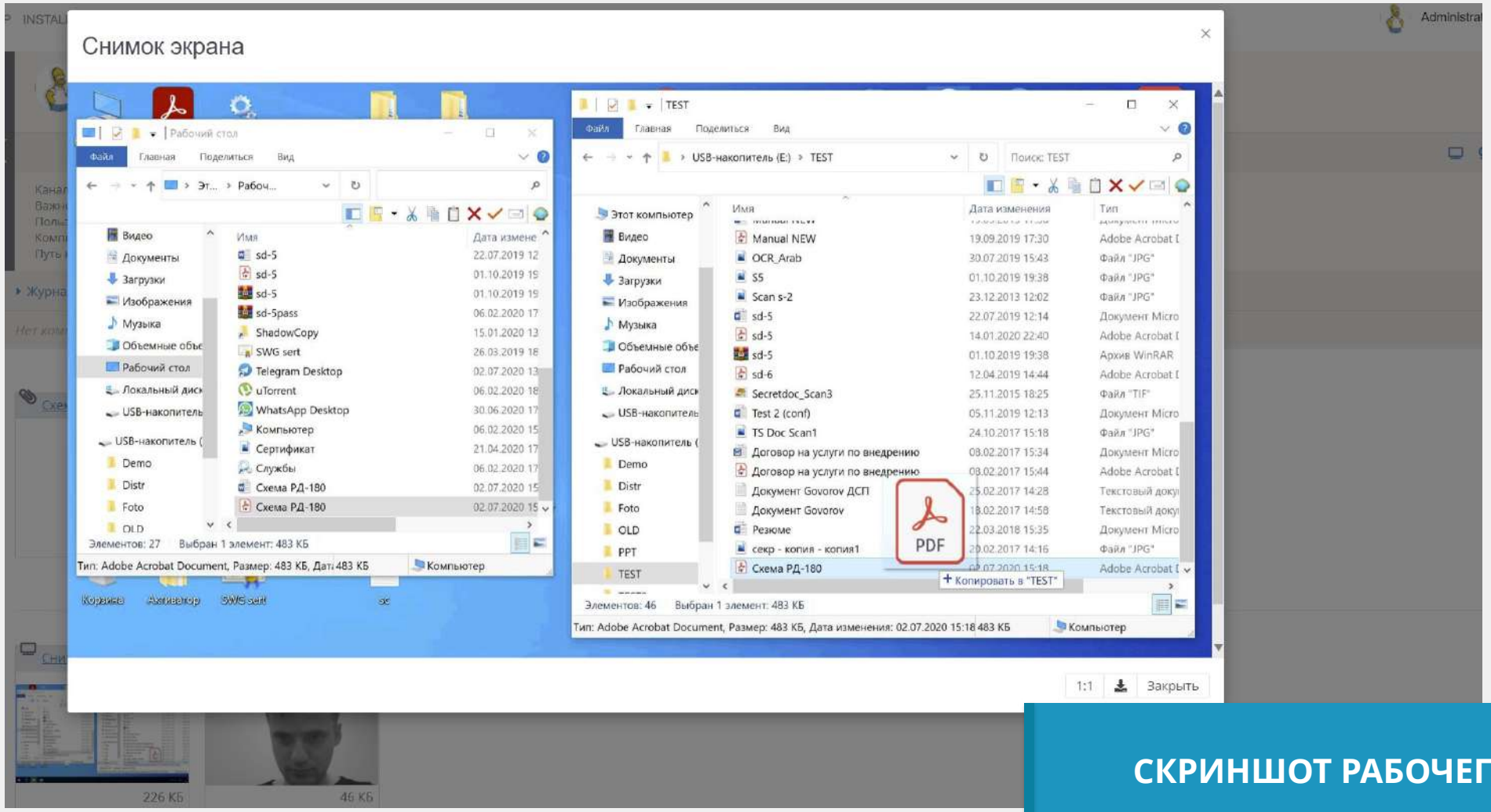
46 КБ

Инцидент: Копирование на флешку



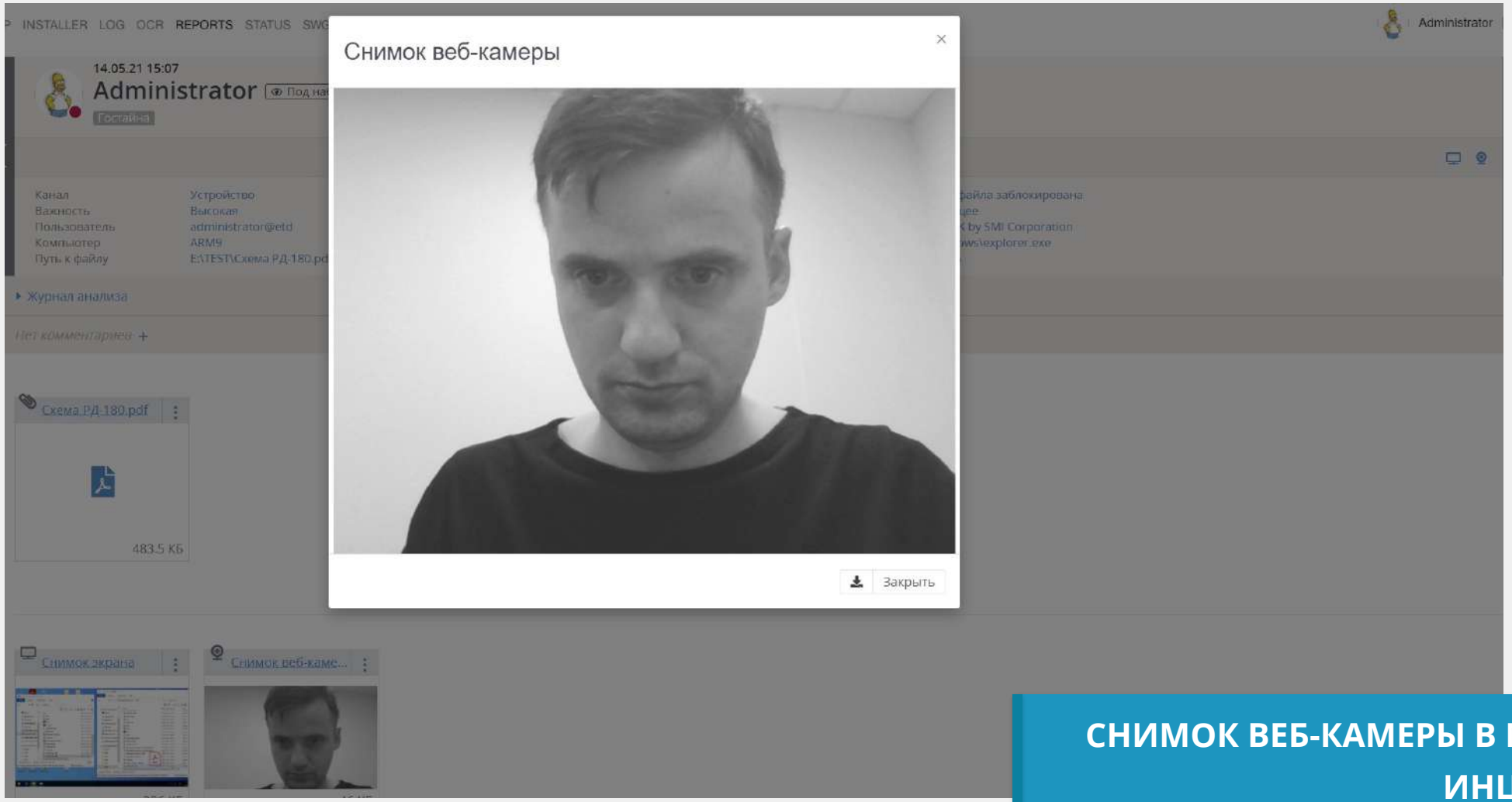
ПЕРЕХВАЧЕННЫЙ ДОКУМЕНТ

Инцидент: Копирование на флешку



СКРИНШОТ РАБОЧЕГО СТОЛА

Инцидент: Копирование на флешку



СНИМОК ВЕБ-КАМЕРЫ В МОМЕНТ ИНЦИДЕНТА

Дело № 2- 720/2018

Решение Ленинского районного суда
г. Ярославля 07 июня 2018 года

ДАНО И ДОКАЗАНО РАБОТОДАТЕЛЕМ

1. На рабочих компьютерах развернута DLP-система « Zecurion». При установке данной системы (в том числе, на компьютер Работника) была создана база данных, содержащая **данные о рабочих компьютерах и учетных записях пользователей** корпоративной вычислительной сети ПАО
2. На компьютере работника установлен модуль системы « Zecurion » - « Zecurion Zlock (Device Control)», который поддерживает **функцию «Теневого копирования»**. При печати содержимого файлов, записи файлов на внешние носители, просмотре и редактировании файлов, данная функция создаёт «теневые копии» (копии файлов) в локальном хранилище для всех пользователей, работающих на данном компьютере. Данные копии хранятся в формате: Дата; Время; Имя файла; Размер; Приложение; Пользователь (Учетная запись под которой производились указанные выше действия над файлом). Далее копии передаются в базу данных на сервере системы « Zecurion », в которой распределяются по каталогам «Дата» и подкаталогам «Учетная запись»

Дело № 2- 720/2018

Решение Ленинского районного суда
г. Ярославля 07 июня 2018 года

ДАНО И ДОКАЗАНО РАБОТОДАТЕЛЕМ

3. Для каждого работника ПАО в целях обеспечения доступа на рабочие компьютеры, доступа к информационным ресурсам ПАО, разграничения прав доступа и журналирования действий, в системе Active Directory создается персональная учетная запись Работников
4. Для Работника была создана учетная запись по именем «RabotnikIvanov»
5. СБ зафиксирована загрузка, использование и хранение Работником файлов, не относящихся к производственной деятельности
6. Работнику вручено уведомление о проведенной СБ проверке соблюдения им информационной безопасности
7. Наложено дисциплинарное взыскание, снижен размер премии на 10%

Дело № 2- 720/2018

Решение Ленинского районного суда
г. Ярославля 07 июня 2018 года

ДОВОДЫ РАБОТНИКА

1. Не был информирован о проведении проверки, не ознакомлен с ее результатами
2. К уведомлению приложены распечатки текстов, неясного происхождения
3. СБ взяла на себя не свойственные ей функции «корпоративной полиции»
4. Работник не становится собственностью работодателя на период рабочего времени, не теряет права на частную жизнь
5. При проверке использовались технические средства и методы скрытого непрерывного контроля за работником на рабочем месте, что нарушает его право на неприкосновенность частной жизни. О возможности скрытого непрерывного контроля на рабочем не был предупрежден и согласия на это не давал
6. Действиями работодателя **по незаконному вмешательству в его личную сферу, по созданию атмосферы слежки и доносительства, ему причинен моральный вред**

Дело № 2- 720/2018

Решение Ленинского районного суда
г. Ярославля 07 июня 2018 года

ДОКАЗАТЕЛЬСТВА РАБОТОДАТЕЛЯ

1. Правила внутреннего трудового распорядка с запретом на использование **не в служебных целях персональных компьютеров, ресурсов сети Интернет, программного обеспечения, оргтехники и другого оборудования ПАО**
2. Должностная инструкция работника с обязанностью соблюдать требования действующего законодательства и локальных нормативных актов
3. Руководство **«Обеспечение информационной безопасности при эксплуатации средств вычислительной техники и корпоративной вычислительной сети ПАО»**
4. Подписные листы Работника
5. Материалы служебной проверки

Дело № 2- 720/2018

Решение Ленинского районного суда
г. Ярославля 07 июня 2018 года

РУКОВОДСТВО «Обеспечение инф. безопасности»

1. Работникам запрещается:

- хранить личную информацию на выданном оборудовании
- использовать ресурсы сети Интернет для просмотра (загрузки) информации и файлов развлекательного характера, не относящейся к производственной деятельности, а также для загрузки, установки и запуска программного обеспечения, самостоятельно полученного из сети Интернет

2. **Выданное оборудование:**

- является **собственностью общества** и выдается для выполнения работником должностных обязанностей

Дело № 2- 720/2018

Решение Ленинского районного суда
г. Ярославля 07 июня 2018 года

РУКОВОДСТВО «Обеспечение инф. безопасности»

3. Все продукты (информация), произведённые на выданном оборудовании, являются **собственностью общества и могут быть проверены работниками СБ**
4. При установлении фактов, уличающих работника в несанкционированном и/или нецелевом использовании мобильных устройств и носителей информации **инициализируется служебная проверка**
5. Следует учитывать, что **действия Работника протоколируются** и материалы по выявленным нарушениям могут быть представлены руководителям Общества для принятия мер в соответствии с действующим законодательством
6. Пользователь **несет ответственность** за несоблюдение требований руководства

Дело № 2- 720/2018

Решение Ленинского районного суда
г. Ярославля 07 июня 2018 года

МАТЕРИАЛЫ СЛУЖЕБНОЙ ПРОВЕРКИ

1. Служебная записка начальника СБ:
    - выявлены загрузки, использование и хранение файлов развлекательного характера
2. Распоряжение руководителя о назначении проверки работниками СБ соблюдения информационной безопасности при эксплуатации средств вычислительной техники и целевого использования ресурсов сети Интернет
3. Положение об отделе безопасности филиала ПАО:
    - задачами СБ является, в том числе, обеспечение информационной безопасности Общества
    - СБ выполняет функцию организации и проведения контрольных мероприятий, соблюдения ИБ на всех этапах производства, обработки, передачи хранения и получения информации

Дело № 2- 720/2018

Решение Ленинского районного суда
г. Ярославля 07 июня 2018 года

МАТЕРИАЛЫ СЛУЖЕБНОЙ ПРОВЕРКИ

4. Акт осмотра с распечатыванием файлов и копированием их на диск с подписями присутствующих
5. Приказ о снижении премии
6. Опрос сотрудника СБ в ходе проведения проверки: им проводилась проверка, о проверке Работник не уведомлялся в силу специфики работы СБ, в компьютерной системе общества, в том числе и в компьютере Работника установлена программа «Zecurion Zlock», копирующая все файлы, с которыми работает Работник. Под учетной записью Работника может войти в систему только он сам по созданному им самим паролю. По результатам проверки под учетной записью Работника был выявлен 31 файл как факт использования автоматизированного рабочего места в непроизводственных целях

Иные примеры судебной практики

Дело № 8Г-1197/2021

Определение судебной коллегии по гражданским делам третьего кассационного суда от 10 марта 2021., г. Санкт-Петербург

Работником было скопирована информация со служебного компьютера на съемный носитель для личного пользования.

Суд признал это нарушением.

Дело № 1-62/2019

Пригоров Дзержинского районного суда г. Новосибирска от 26 февраля 2019 года

Два работника – настоящий и бывший – осуждены за разглашение коммерческой тайны.

Дело № 22-2097/2020

Апелляционное постановление Кемеровского областного суда на приговор г. Кемерово 19 июня 2020 года

Работник осужден за незаконное использование конфиденциальной информации, содержащей коммерческую тайну при пересылке информации со служебного компьютера на личный электронный адрес

Forensic Alliance

Области практики

- Корпоративное право
- Налоговое право
- Административное право
- Хозяйственное право
- Уголовное право
- Сопровождение процедур банкротства
- Правовая поддержка при взаимодействии с контролирующими органами
- Правовой аудит деятельности компаний
- Форензик-расследования

МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ
ЮЛОВА И ПАРТНЕРЫ

Адвокаты МКА «Юлова и партнеры» практикуют в области права с конца 80-х – начала 90-х годов

Основана в 2009 году

МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ
ЮЛОВА И ПАРТНЕРЫ

Forensic Alliance

Наши доверители

Адвокатам Коллегии доверяют защиту своих интересов как небольшие компании, так и крупные российские и транснациональные корпорации и холдинговые структуры.

Среди частных клиентов Коллегии многие успешные предприниматели, а также люди, добившиеся признания в различных областях общественной жизни.

Уголовное право: экономические преступления - **7-е место**

Уголовное право: должностные преступления - **6-е место**

СОГЛАСИЕ страхование

ИНТЕКО

IKEA

ДОМ РФ БАНК

ENKA

DHL

Mercedes-Benz FashionWeek RUSSIA

Schindler

SIEMENS

Deloitte.

hp

Honeywell

DB SCHENKER

банк российский капитал

ВОСТОЧНЫЙ БАНК

TELE2

M&M MILITZER & MÜNCH

BSGV Банк Сосьете Женераль Восток ГРУППА СОСЬЕТЕ ЖЕНЕРАЛЬ

МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ ЮЛОВА И ПАРТНЕРЫ

Telegram-каналы

https://t.me/forensictoday

Новости о мошенничествах и корпоративных преступлениях в России

https://t.me/forensicalliance

Канал о форензик-расследованиях, корпоративных преступлениях, мошенничествах, материалы экспертов Forensic Alliance

Forensic Alliance

МОСКОВСКАЯ КОЛЛЕГИЯ АДВОКАТОВ
ЮЛОВА И ПАРТНЕРЫ

Александра Гончарова

+7 915 005 00 55

goncharova.aleksandra@gmail.com

https://yulova.ru/

https://forensicalliance.ru/