КРЭТ
АЭРОПРИБОР-ВОСХОД

Внедрение на производственном предприятии DLP-системы «СерчИнформ КИБ»

Заместитель генерального директора
по информационным технологиям и информационной безопасности

Тагиль Вадим Олегович

КРЭТ
АЭРОПРИБОР-ВОСХОД

Заказчик: АО «АП Восход»

Руководитель проекта от Заказчика:

Тагиль Вадим Олегович
Заместитель генерального директора по информационным технологиям

ИТ-Поставщик: ООО «СерчИнформ» - в части поставки программного обеспечения, специалисты АО «АП Восход» - в части реализации проекта.

Год завершения проекта: 2024

Сроки выполнения проекта: декабрь 2023 – октябрь 2024

Масштаб проекта: 800 АРМ

География: ул. Ткацкая 19, ул. 2-ая Владимирская, д.62Б

Человеко-часы: 5328 часов

КРЭТ
АЭРОПРИБОР-ВОСХОД

О предприятии

АО «АП Восход» уже 80 лет создает аэрометрическое, радиоэлектронное и навигационное оборудование для авиационной и космической техники Российской Федерации. Приборы и системы установлены на всех отечественных военных и гражданских самолетах, а также на вертолетах, космических и беспилотных летательных аппаратах. Предприятие имеет достойную историю и внесло значительный вклад в авиационную и ракетно-космическую отрасль государства.

С 2012 года АО «АП Восход» входит в состав АО «Концерн Радиоэлектронные технологии» Госкорпорации «Ростех».

В 2018 году в состав АО «АП Восход» вошло не менее значимое предприятие в оборонно-промышленном комплексе России - АО «МКБ «Компас».

Ткацкая,19

2-я Владимирская улица, 62Б

КРЭТ
АЭРОПРИБОР-ВОСХОД

Описание проекта

Проект направлен на обеспечение информационной безопасности предприятия путём внедрения системы предотвращения утечек данных (Data Loss Prevention, DLP).

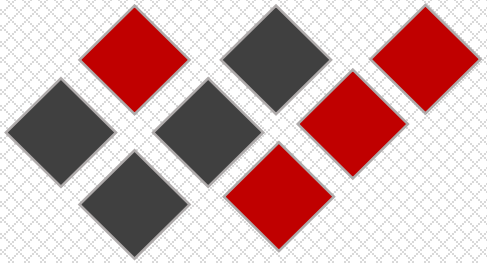
Система контролирует и анализирует все информационные потоки на предприятии, чтобы предотвратить несанкционированный доступ к информации ограниченного доступа и её утечку за пределы корпоративной сети.

Использованное ПО:

- СерчИнформ КИБ 5.2

Серверное оборудование:

Платформа: 440BX Desktop Reference Platform
Процессор: 8 Core 2.90 GHz Intel Xeon(R) Gold 6226(R)
(4 процессора) Установленная память (ОЗУ): 64 Гб



КРЭТ
АЭРОПРИБОР-ВОСХОД

Цели проекта

- Внедрение отечественного программного обеспечения для предотвращения потери/утечки информации;
- Защита конфиденциальных данных от утечек, контроль использования, передачи и хранения информации;
- Сбор статистики действий сотрудников за рабочим компьютером, анализ эффективности коммуникаций и бизнес-процессов;
- Контроль правомерности действий сотрудников (предотвращение шпионажа, нарушения законодательства и пр.).

КРЭТ
АЭРОПРИБОР-ВОСХОД

Этапы проекта

- Разработка плана внедрения и интеграции с существующими системами
- Настройка правил и параметров мониторинга для обнаружения подозрительной активности
- Обучение сотрудников работе с новой системой
- Тестирование и оптимизация работы DLP-системы
- Мониторинг и анализ результатов работы системы для выявления возможных проблем и улучшения эффективности
- Регулярное обновление и совершенствование системы в соответствии с изменениями в бизнес-процессах и требованиями безопасности

КРЭТ
АЭРОПРИБОР-ВОСХОД

Процесс внедрения проекта

После выбора подходящей DLP-системы была произведена подготовка инфраструктуры и настройка интеграции. Этот процесс потребовал провести анализ текущей ИТ-инфраструктуры на совместимость с новой системой безопасности и сделать оценку всех технических ресурсов для готовности поддержки системы.

На следующем этапе выполнялась настройка DLP-системы под конкретные нужды предприятия. Система конфигурировалась для защиты тех данных, которые были оценены как наиболее критичные.
Особое внимание уделялось интеграции DLP с существующими системами безопасности и компонентами ИТ-инфраструктуры. Была проведена интеграция DLP-системы с антивирусным программным обеспечением, что позволило централизованно реагировать на инциденты безопасности.
Завершающий этап интеграции заключался в проведении тестирования, цель которого – убедиться, что все компоненты системы работают согласовано. Тестирование охватывало различные сценарии, включая большие объемы передаваемых данных, возможные сбои соединения и стресс-тестирование отказоустойчивости системы.

КРЭТ
АЭРОПРИБОР-ВОСХОД

Уникальность проекта

«СерчИнформ КИБ» предлагает больше возможностей, чем классическая DLP. Благодаря аналитическим инструментам, а также ориентации не только на данные, но и на пользователя, система:

- Защищает от последствий, связанных с утечками информации;
- Стимулирует соблюдение трудовой дисциплины и рабочего регламента;
- Помогает повысить продуктивность персонала;
- Позволяет управлять лояльностью коллектива.

Система в режиме реального времени анализирует все, что происходит на предприятии АО «АП Восход». Перехват сохраняется и позволяет восстанавливать детали прошедших событий, если возникает необходимость расследования.

- Каналы связи – Электронная почта, мессенджеры, форумы, облачные хранилища и др.
- Действия сотрудников – Занятость за компьютером, поведение, криминальные тенденции и тд.
- Хранимую информацию – Ее нахождение в «правильных» сетевых папках, на «разрешенных» компьютерах и т.д.

КРЭТ
АЭРОПРИБОР-ВОСХОД

Сложности реализации проекта

- Необходимость адаптации и настройки под специфические процессы
- Ложные срабатывания и ошибки в классификации данных
- Необходимость обновления программного и аппаратного обеспечения в части АРМ для более точного соответствия задачам DLP
- Необходимость изменения привычных рабочих процессов с учетом требований DLP-системы
- Потребность в формировании большого количества политик информационной безопасности

КРЭТ
АЭРОПРИБОР-ВОСХОД

Ключевые контуры охвата DLP-системы на предприятии

КРЭТ
АЭРОПРИБОР-ВОСХОД

Компоненты DLP

MailController
Записывает всю переписку по электронной почте

IMController
Записывает чаты и фиксирует вложения в социальных сетях и мессенджерах

DeviceController
Фиксирует данные, передаваемые пользователями на внешние устройства

PrintController
Отслеживает содержание документов, отправляемых на печать

CloudController
Контролирует файлы, перемещаемые из / в облачные хранилища

FTPController
Фиксирует данные, отправленные или полученные по FTP, включая зашифрованное соединение (FTPS)

AlertCenter
Управляет настройкой политик безопасности, позволяет создавать правила и планировать аудиты

ReportCenter
Визуализирует действия пользователей по всем каналам связи, все события внутри системы и связи между сотрудниками

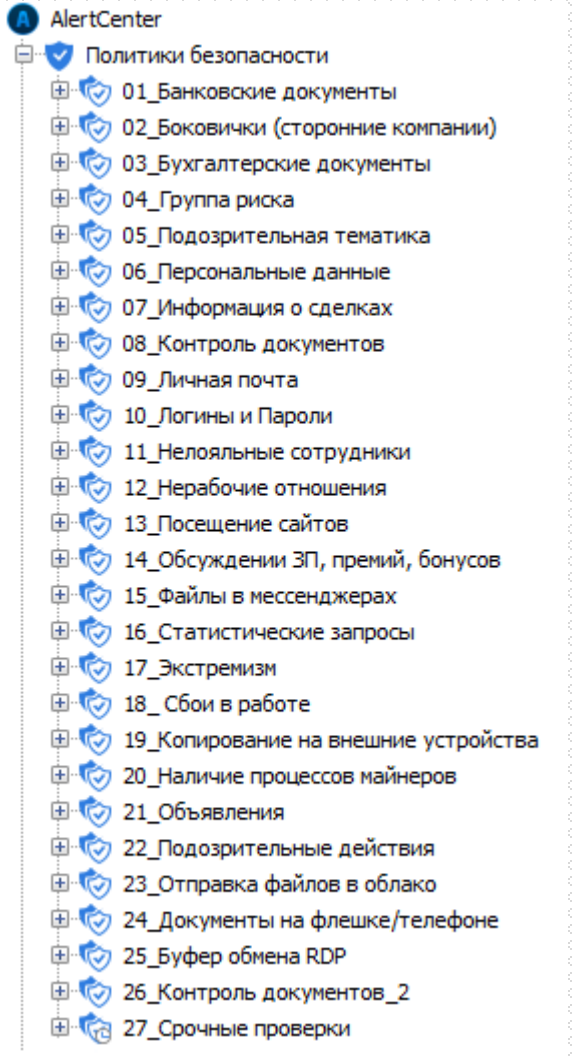
HHTPController
Фиксирует файлы и сообщения, передаваемые по протоколам HTTP/HTTPS

КРЭТ
АЭРОПРИБОР-ВОСХОД

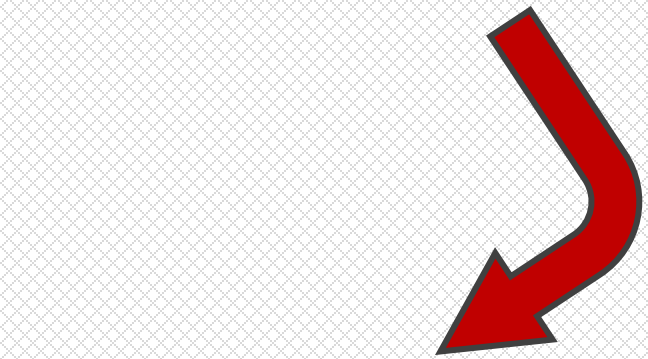
Политики безопасности

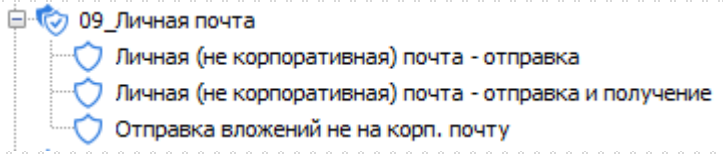
В течении нескольких недель производился анализ трафика на предмет изучения информации, циркулирующей в локальной сети.

Были сформированы и откорректированы в процессе эксплуатации 27 групп политик безопасности, закрывающие основные инциденты информационной безопасности.



Для примера, группа «Личная почта» позволяет просматривать активность пользователей на момент пересылки файлов на не корпоративную почту.

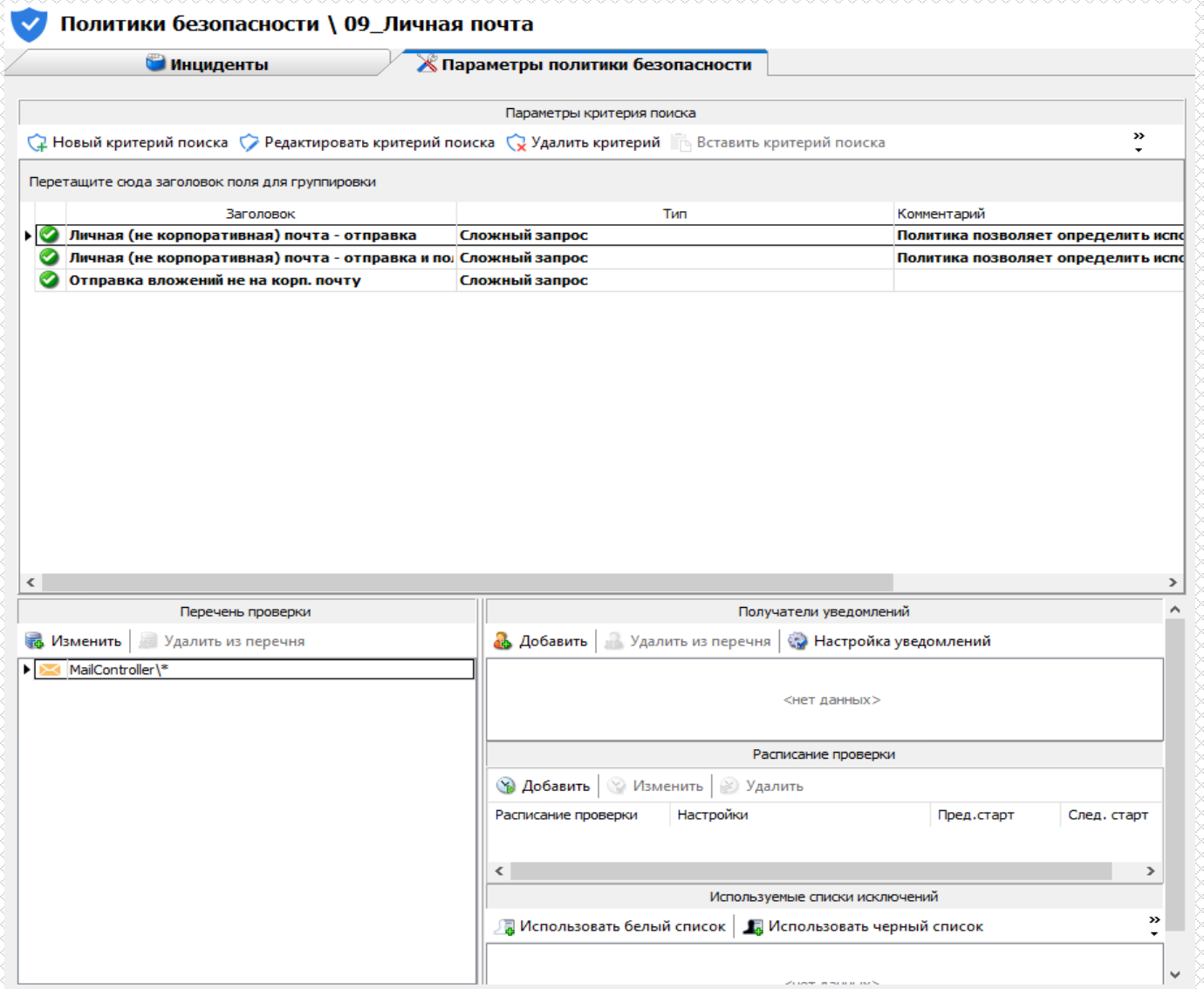




КРЭТ
АЭРОПРИБОР-ВОСХОД

Политика безопасности «Личная почта»

В данном разделе возможна корректировка политики безопасности в целом или отдельно конкретных критерий для поиска под собственные нужды.

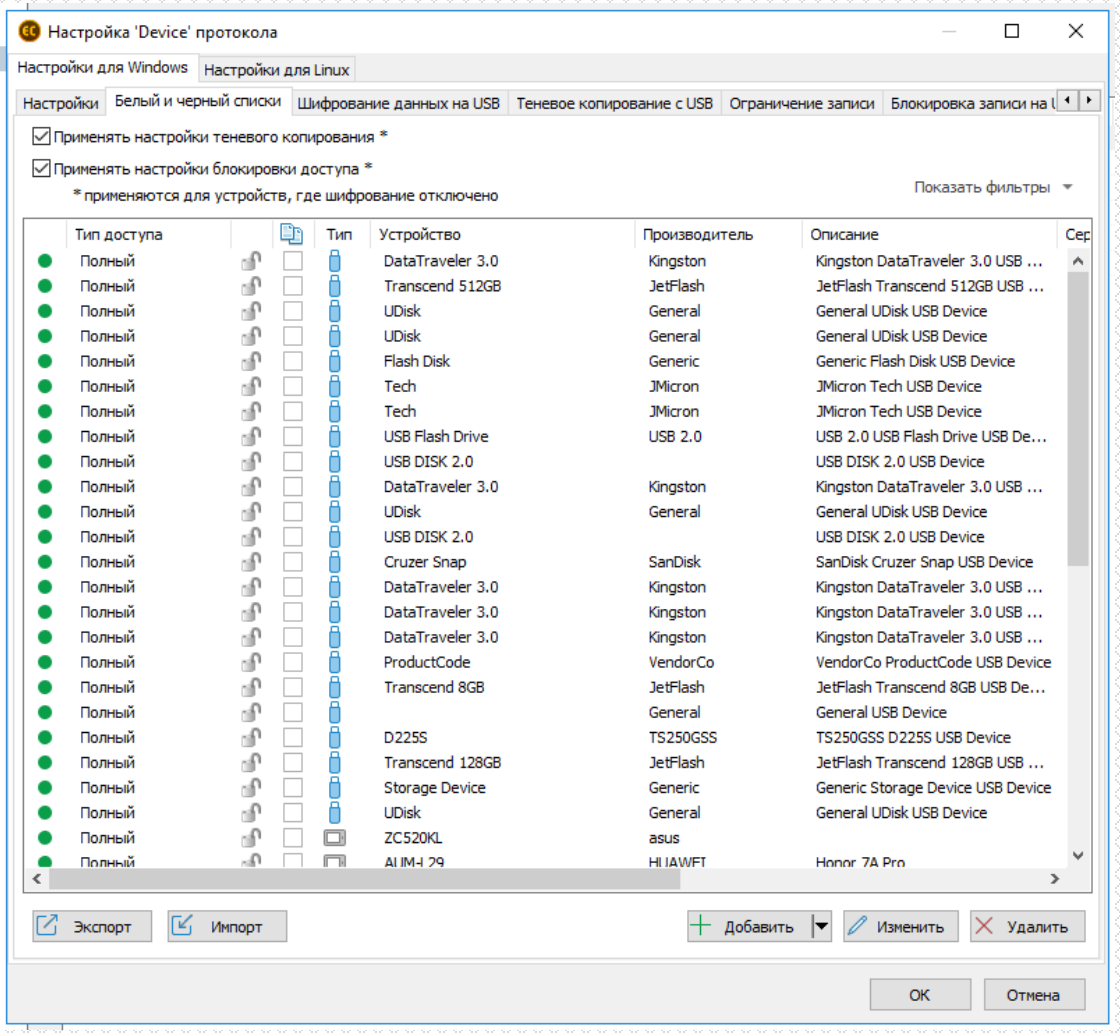


КРЭТ
АЭРОПРИБОР-ВОСХОД

Внешние машинные носители информации

Благодаря КИБ «СерчИнформ» Была проведена процедура внедрения контроля внешних устройств, на основе его использования были внесены изменения в регламент учета и контроля ВМНИ.

В настоящее время возможна эксплуатация только зарегистрированных устройств, а доступ к эксплуатации других устройств, полученных «извне», будет блокироваться.

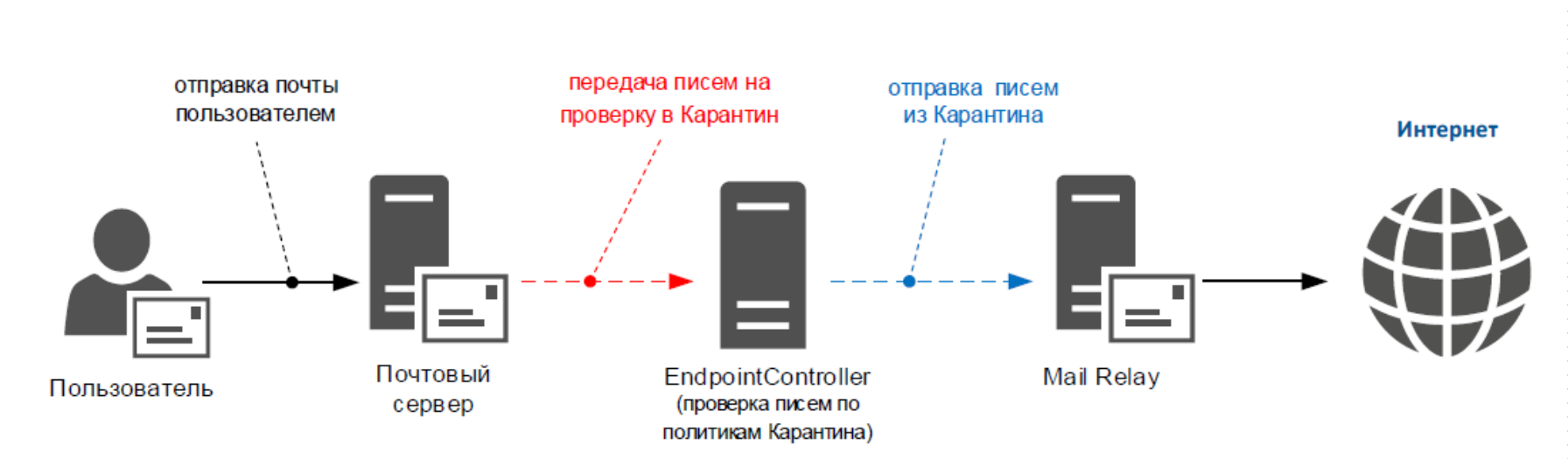


КРЭТ
АЭРОПРИБОР-ВОСХОД

Блокировка почты на уровне почтового сервера

Во взаимодействии информационной инфраструктуры организации организована интеграция системы КИБ с электронной почтой предприятия.

Блокировка отправляемых пользователями писем на уровне почтового сервера реализуется путем настройки на почтовом сервере промежуточного узла отправки исходящей из него почты. В роли промежуточного узла выступает сервер КИБ, где осуществляется последующая проверка писем по политикам безопасности карантина.



КРЭТ
АЭРОПРИБОР-ВОСХОД

Результаты проекта

- Повышение уровня информационной безопасности предприятия за счёт контроля и анализа всех информационных потоков в компании
- Снижение рисков финансовых потерь, репутационного ущерба и юридических последствий, связанных с утечкой конфиденциальной информации
- Обеспечение соответствия требованиям законодательства и внутренних политик безопасности
- Повышение доверия клиентов и партнёров к предприятию благодаря надёжной защите конфиденциальных данных
- Улучшение качества управления рисками информационной безопасности на предприятии

КРЭТ
АЭРОПРИБОР-ВОСХОД

ТАГИЛЬ ВАДИМ ОЛЕГОВИЧ

Заместитель директора по информационным технологиям и информационной безопасности

АО «АП Восход», 105318, Москва, ул. Ткацкая, д.19.
Тел. +7 (495) 363-23-00 доб. 1907
tagilvo@aeropribor.ru