

Проактивный контур защиты данных: пропустить нельзя блокировать



Александр Янчук
Заместитель генерального
директора по СЗФО

SEARCHINF@RM
INFORMATION SECURITY



Блокировки

при передаче информации по сети,
на конечной рабочей станции, или
с использованием почтового
сервера заказчика

Контекстные
(по атрибутам)

Контентные
(по содержимому)

Клиенты с блокировками



Планируемые штрафы

Первая утечка ПДн:

- 1 000 – 10 000 субъектов ПДн, штраф **3-5 млн**
- 10 000 – 100 000 субъектов ПДн, штраф **5-10 млн**
- от 100 000 субъектов ПДн, штраф **10-15 млн**

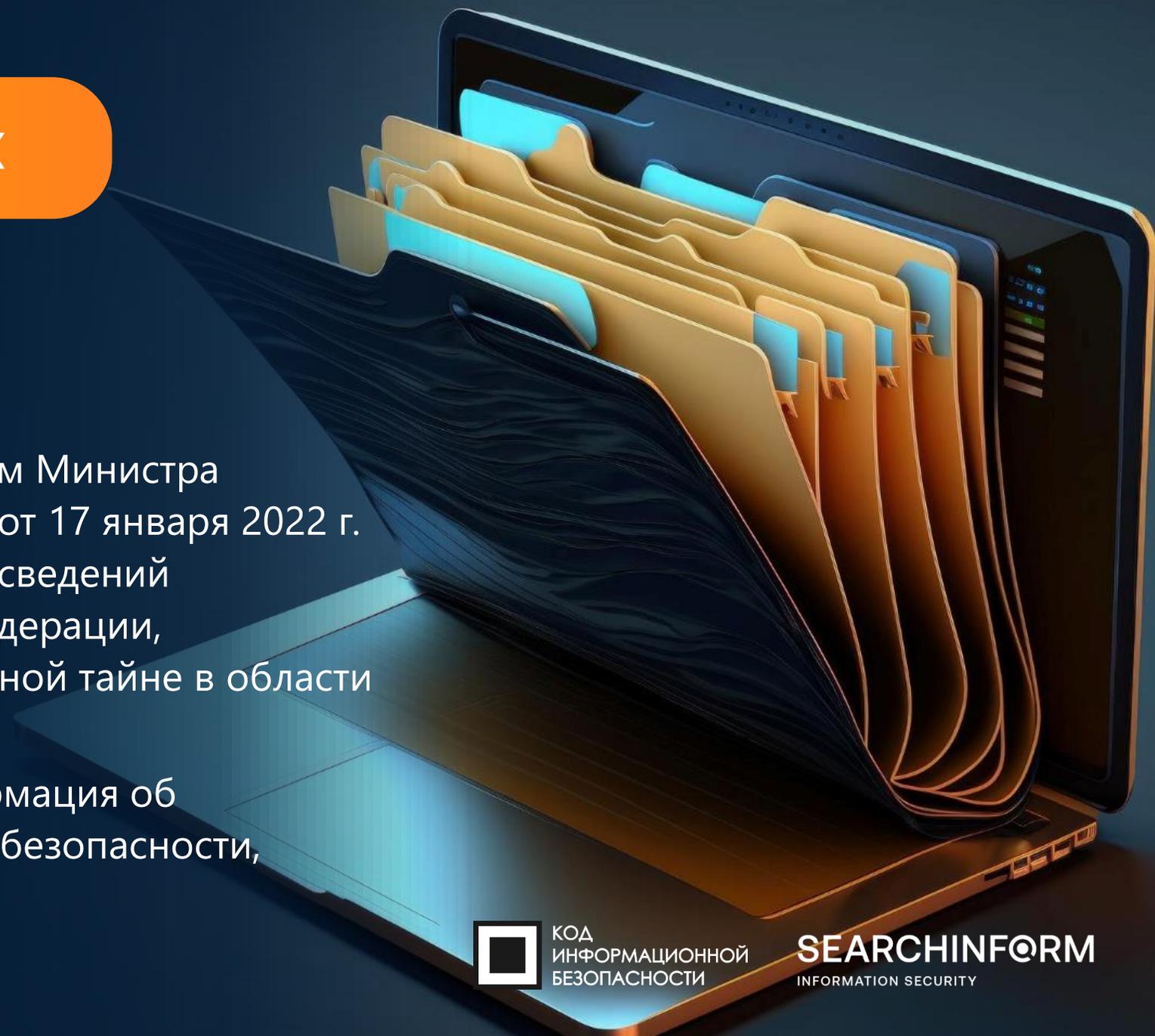
Повторно:

- оборотные штрафы от 0,1 до 3% выручки за календарный год или за часть текущего года, но не менее **15 млн** и не более **500 млн**



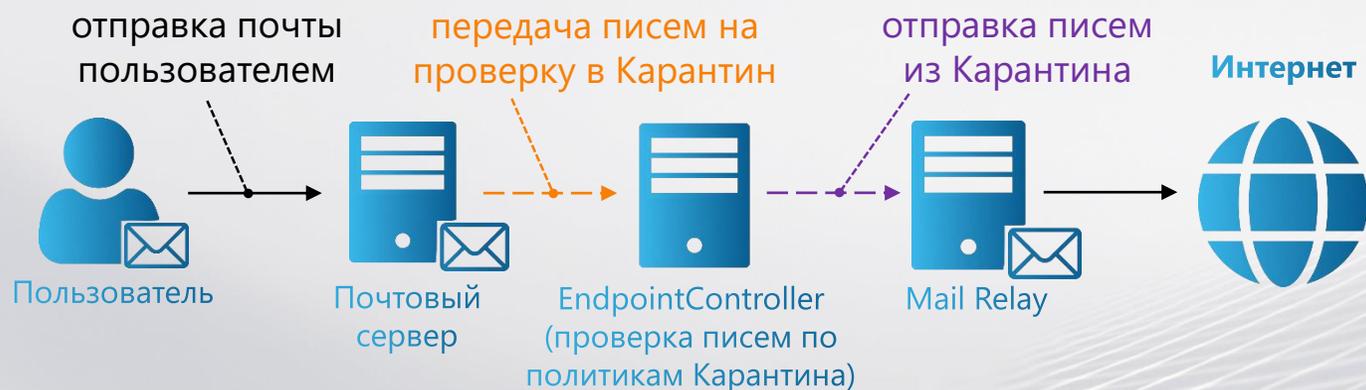
Контроль данных

- Финансовые документы.
- Персональные данные.
- Учетные записи.
- ДСП в соответствии с Приказом Министра обороны Российской Федерации от 17 января 2022 г. № 22 «Об утверждении Перечня сведений Вооруженных Сил Российской Федерации, подлежащих отнесению к служебной тайне в области обороны»
- Внутренние документы: информация об архитектуре сети, о политиках безопасности, регламенте работы, зарплатах.
- Коммерческая тайна и др.

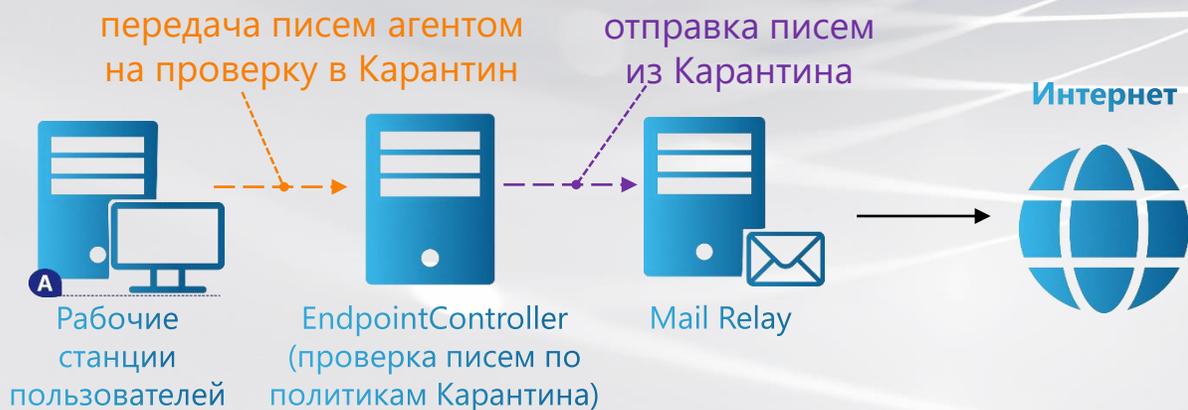


Контентные блокировки в DLP

Блокировка почты через интеграцию с почтовым сервером



Блокировка на агенте



Блокировка трафика «в разрыв» (ICAP)



Взаимодействие с ИТ

- Рекомендации от вендора по настройкам блокировок
- План-график активации блокировок
- Регламент взаимодействия ИБ и ИТ в случае выявления проблем, согласованность действий.



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

SEARCHINFORM
INFORMATION SECURITY

Блокировки запускаются поэтапно, отдельно по каждому модулю

MailController

1

Внутренняя корпоративная почта

2

Внешняя некорпоративная почта

1. Сначала тестовая группа до 10 АРМ.
2. После успешной опытной эксплуатации в течение минимум 1 недели, добавляем +50 АРМ.
3. После успешной опытной эксплуатации в течение минимум 1 недели, добавляем +100 АРМ.
4. После успешной опытной эксплуатации в течение минимум 1 недели, добавляем +200 АРМ и т.д.

Возможности GUI на агенте

SEARCHINFORM
INFORMATION SECURITY

- Предупреждения о блокировках доступа.
- Запрос доступа и взаимодействие с ИБ

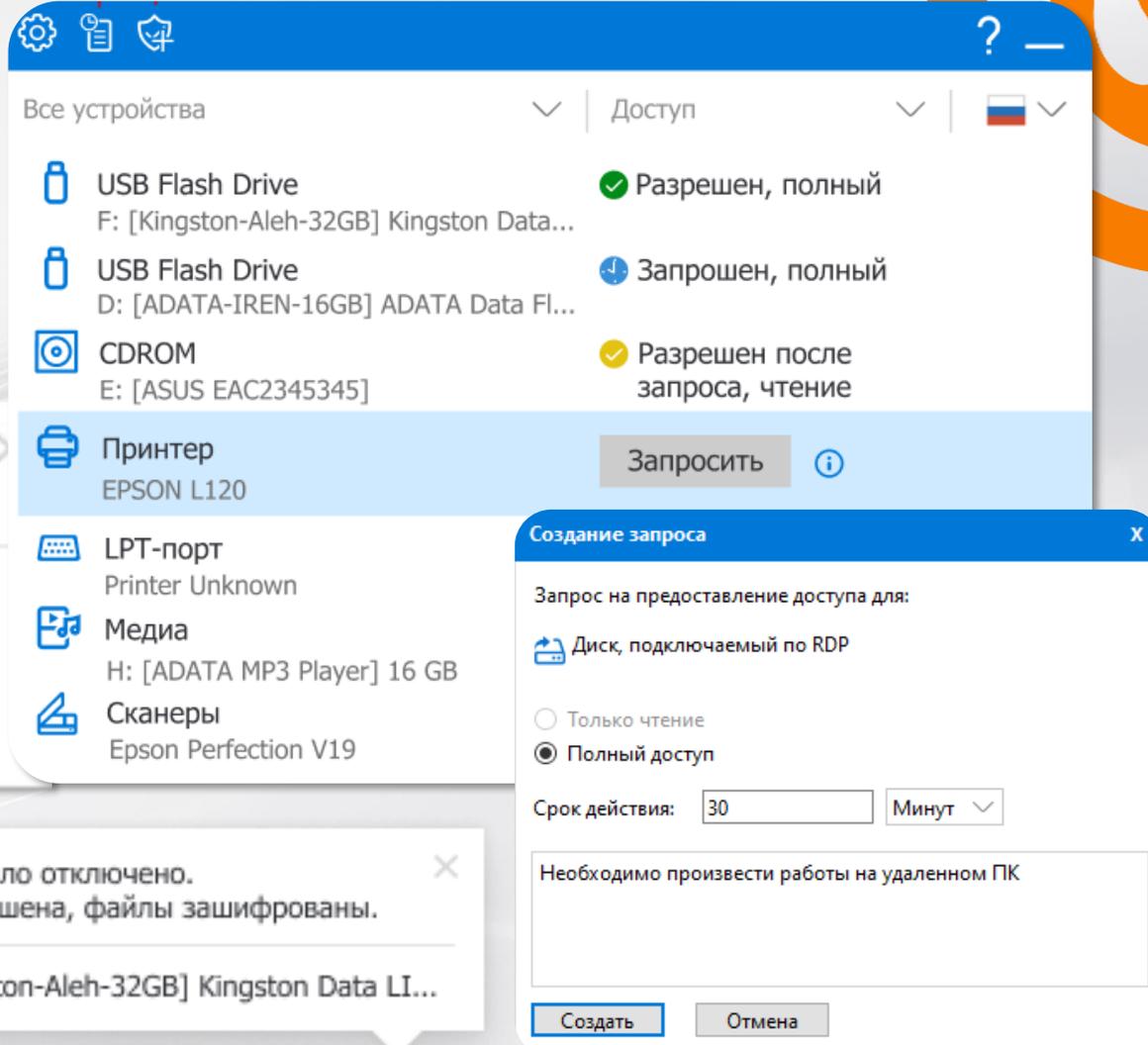
 Печать на принтере заблокирована согласно корпоративным правилам.

Принтер: HP 1100P
Процесс: Notepad.exe
Пользователь: n.konovalov

 USB-устройство было отключено.
Проверка не завершена, файлы зашифрованы.

Устройство: H: [Kingston-Aleh-32GB] Kingston Data LI...

 КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



The screenshot shows the Windows Device Manager window with the 'All devices' tab selected. The 'Printer' section is expanded, showing an Epson L120 printer. A 'Request' button is visible next to the printer. In the foreground, a 'Create request' dialog box is open, showing a request for access to a disk connected via RDP. The request type is set to 'Full control', and the duration is 30 minutes. The dialog also includes a text area for a message and 'Create' and 'Cancel' buttons.

Все устройства | Доступ | 

- USB Flash Drive F: [Kingston-Aleh-32GB] Kingston Data... Разрешен, полный
- USB Flash Drive D: [ADATA-IREN-16GB] ADATA Data Fl... Запрошен, полный
- CDROM E: [ASUS EAC2345345] Разрешен после запроса, чтение
- Принтер EPSON L120** 
- LPT-порт Printer Unknown
- Медиа H: [ADATA MP3 Player] 16 GB
- Сканеры Epson Perfection V19

Создание запроса 

Запрос на предоставление доступа для:

-  Диск, подключаемый по RDP
- Только чтение
- Полный доступ

Срок действия:

Необходимо произвести работы на удаленном ПК

Блокировки с OCR

Блокировки по контенту изображений:

- Печати изображений.
- Записи изображений на USB.
- Передачи изображений в мессенджерах.
- Передачи изображений в web.

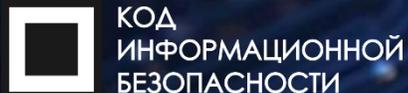
SEARCHINFORM
INFORMATION SECURITY

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



Блокировки 2.0 Эволюция

Ещё лучше блокировки в DLP работают в связке с DCAP. DCAP может метить файлы, а DLP контролировать их перемещение.



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

SEARCHINFORM
INFORMATION SECURITY



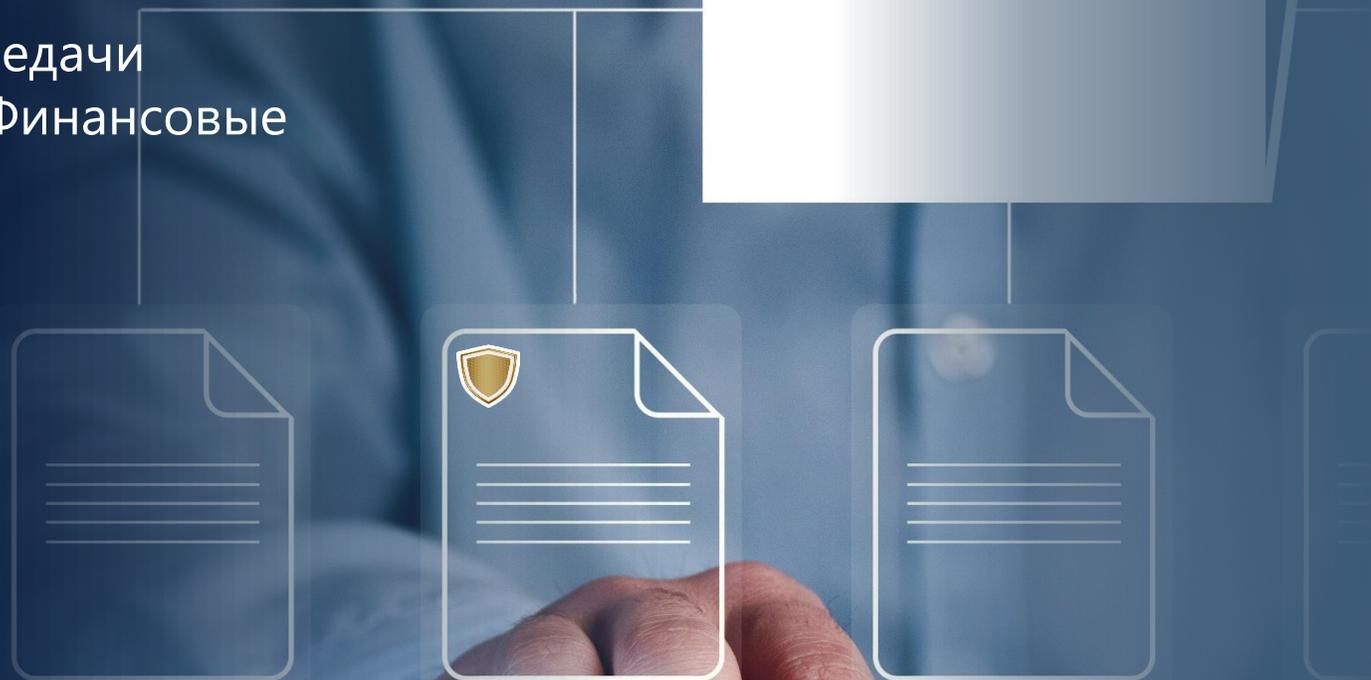
DLP+DCAP

Блокировки нежелательных действий с файлами и папками

В FileAuditor реализованы блокировки передачи документов: на документ ставится метка «Финансовые документы», «Коммерческая тайна» и т.д.

После этого можно:

- запретить отправку файла с меткой;
- предотвратить загрузку в облако;
- заблокировать отправку в мессенджере документа.



Метки сохраняются при копировании, изменении, пересохранении и переносе файла на USB.

Запреты можно задать для всех или отдельных пользователей/ПК, а также настроить исключения. О файлах, попавших под блокировку, ИБ-специалисты будут узнавать из оповещений на email.

Спасибо за внимание!

Вопросы?



[https://t.me/
searchinform](https://t.me/searchinform)



[https://vk.com/sec
urityinform](https://vk.com/securityinform)



[https://www.youtube.
com/user/SearchInform](https://www.youtube.com/user/SearchInform)

Практика и аналитика



[https://searchinform.ru/
practice-and-analytics/](https://searchinform.ru/practice-and-analytics/)

SEARCHINFORM
INFORMATION SECURITY