SEARCHINFORM

ПРАКТИЧЕСКИЙ ВЕБИНАР

ПРОАКТИВНАЯ ЗАЩИТА ОТ ШТРАФОВ ЗА УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Алексей Парфентьев

Заместитель генерального директора
по инновационной деятельности
«СёрчИнформ»

КАК ИБ-ИНЦИДЕНТЫ С ПДН МОГУТ ПОДОРВАТЬ РАБОТУ ОРГАНИЗАЦИИ?

Последствия утечек персональных данных:

- **Штраф для бизнеса:**
  - за первую утечку– 3-15 млн ₽
  - за повторную утечку– 1-3% годовой выручки (20-500 млн ₽)

  Применение новых штрафов ожидается с III-IV кв. 2025

- **Проверки Роскомнадзора, Прокуратуры, следственные действия в организации**
- **Репутационные риски**
- **Судебные разбирательства с пострадавшими**
  - сумма компенсации – до 150 000 р.

БАНКРОТСТВО?

SEARCHINFORM

ОТ ЧЕГО ЗАЩИЩАТЬСЯ?

В 2024-2025 зафиксировано **170 утечек ПДн**. **Утекло 749 млн** записей.[1,2]

БИЗНЕС

39%
компаний столкнулись
с внутренними инцидентами ИБ[3]

32%
этих инцидентов повлекли
утечку персональных данных

ГОССЕКТОР

51% организаций столкнулись
с внутренними инцидентами ИБ

52% этих инцидентов повлекли утечку
персональных данных

25% сотрудников передают данные
через мессенджеры и прочие
незащищенные каналы[4]

1/3 внутренних инцидентов произошли умышленно

1 – https://ria.ru/20250705/dannye-2027353256.html
2 – https://ria.ru/20250116/roskomnadzor-1993941562.html

3 – Исследование уровня ИБ в организациях России. 2024 год. ООО «СёрчИнформ».
4 – Исследование защиты данных в служебной коммуникации сотрудников организаций госсектора. 2024 год. ООО «СёрчИнформ»

КАКИЕ ТЕХНИЧЕСКИЕ МЕРЫ ПРИНЯТЬ?

с точки зрения требований регулятора

ФЗ «О персональных данных» от 27.07.2006 № 152-ФЗ	
Обнаружение обрабатываемых персданных	DCAP-системы
Принятие мер к ликвидации последствий инцидентов	
Обеспечение конфиденциальности персданных в процессе их обработки	DCAP-системы + DLP-системы
Обнаружение инцидентов с персональными данными для уведомления РКН	
Выявление лиц, причастных к ИБ-инцидентам	
Приказ ФСТЭК от 18.02.2013 № 21	
Реализация необходимых методов, типов и правил разграничения доступа	DCAP-системы
Поддержка и сохранение атрибутов безопасности, связанных с информацией в процессе ее хранения и обработки	
Обеспечение возможности восстановления персданных	
Анализ инцидентов, выявление причин возникновения, оценка последствий	DLP-системы
Принятие мер по устранению последствий инцидентов	
Контроль данных, вводимых в информационную систему	
Защита персональных данных при передаче по каналам связи	
Исключение возможности отрицания получения и отправки персданных	

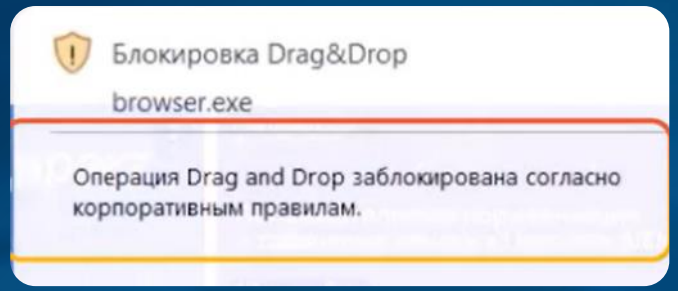
DLP\DCAP ДЛЯ ЗАЩИТЫ:
ТРАНСФОРМАЦИЯ ТРЕБОВАНИЙ В ЗАДАЧИ

ВОВЛЕЧЕНИЕ СОТРУДНИКОВ В ИБ

Защита данных без участия сотрудников невозможна

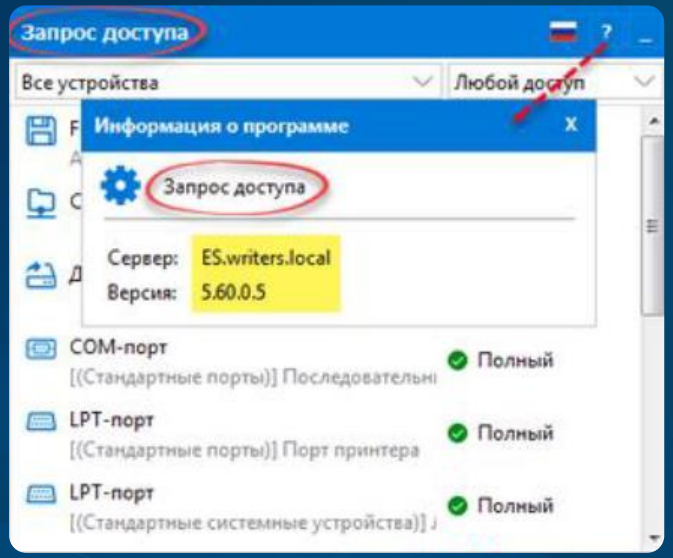
Необходимы уведомления пользователя:

- О срабатывании СЗИ
- О блокировке действий



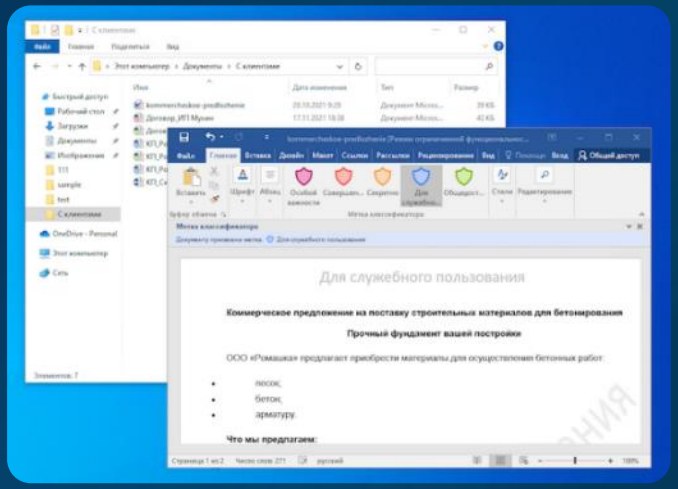
Необходимы функции:

- Коммуникации ИБ-службы и пользователя
- Исключения при необходимости



Необходима возможность пользователя:

- Помочь работе СЗИ
- Указать, что защищать



SEARCHINFORM

ДОКУМЕНТАЛЬНОЕ ОФОРМЛЕНИЕ ИБ-СРЕДСТВ

1 ПРАВО НА ЗАЩИТУ

Включить в правила внутреннего распорядка, должностные инструкции, политику обработки ПДн, положения о ИБ и комтайне в компании

- «Компания имеет право контролировать соблюдение работниками Правил/ Положения/ Политики компании любыми законными способами, в т.ч. с помощью технических средств»

3 ОЗНАКОМИТЬ ВЕСЬ ПЕРСОНАЛ ПОД РОСПИСЬ

2 ЦЕЛЬ И ПРЕДЕЛЫ ИСПОЛЬЗОВАНИЯ

Включить в приказ о вводе DLP в эксплуатацию

- Цели применения DLP:
  - Выполнение требований по защите персональных данных;
  - Защита коммерческой тайны;
  - Контроль исполнения работниками трудовых обязанностей.
- «Ответственным за эксплуатацию системы назначается [ФИО]»

ПРЕИМУЩЕСТВА ПРЕВЕНТИВНОЙ ЗАЩИТЫ

Почему это лучший способ?

- Минимизируется риск возникновения инцидента
- Инцидент ≠ утечке, если обнаружен вовремя
- Применимо к защите любой другой информации
- Объем «бумажной» работы и взаимодействия с властями минимален

Попутно выполняются и другие задачи:

- Защита коммерческой тайны
- Контроль работы и эффективности персонала
- Предотвращение угроз экономической безопасности
- Дисциплинарные взыскания и дела о нарушениях остаются на усмотрение организации

SEARCHINFORM

ПРЕИМУЩЕСТВА ПРЕВЕНТИВНОЙ ЗАЩИТЫ

А если все равно случится?

Вы увидите инцидент первыми:

- Исключается штраф за неуведомление об утечке
- Сможете сразу предотвратить последствия

У вас будут доказательства:

- Причастности инсайдера или хакера
- Добросовестности организации

У вас будут основания:

- Для снятия с бизнеса ответственности или ее смягчения (вплоть до предупреждения)
- Для возбуждения уголовного дела в отношении виновников

СПАСИБО ЗА ВНИМАНИЕ!

SEARCHINFORM

https://t.me/
searchinform

https://vk.com/
securityinform

https://rutube.ru/channel
/26067088/

Практика и аналитика

https://searchinform.ru/
practice-and-analytics/

E-mail: info@searchinform.ru
gr@searchinform.ru