



## StarForce Leak Investigator



Приложение для расследования утечек документов, защищённых в системе StarForce Content Enterprise



## Современные вызовы

В современном мире информация представляет собой наиболее ценный продукт, который можно купить, продать, обменять или даже украсть.

Несмотря на предпринимаемые действия в сфере ИТ-безопасности, существует вероятность утечек защищённых документов в результате недобросовестных или невнимательных действий сотрудников организации.

Документы могут попасть в руки посторонних лиц даже при установленных запретах на печать или пересылку – всегда остаётся вероятность, что злоумышленник сделает фотографию документа с экрана устройства, на котором тот был открыт.



## StarForce Leak Investigator

Модуль **Leak Investigator** в системе **StarForce Content Enterprise** от российской компании «Протекшен Технолоджи» позволяет определить по скомпрометированному документу (фотографии защищённого документа или скану печатной копии), на каком компьютере или мобильном устройстве данный документ был открыт в момент кражи. Это позволяет установить лиц, ответственных за утечку.

При каждом открытии или печати защищённого документа система **StarForce Content Enterprise** в журнале доступа сохраняет информацию (IP адрес, идентификатор пользователя, дата и время и пр.), позволяющую отследить, кем и когда были совершены указанные действия с документом. Идентификатор записи в журнале доступа к документам с использованием методов **стеганографии** встраивается в изображение документа, выводимое на экран или принтер. Стеганография реализована с использованием небольших сдвигов отдельных слов или других блоков текста документа.

**StarForce Leak Investigator** сравнивает скомпрометированную копию с защищённым оригиналом документа и позволяет определить закодированный идентификатор записи в журнале доступа и тем самым обнаружить источник утечки.



# Принцип работы

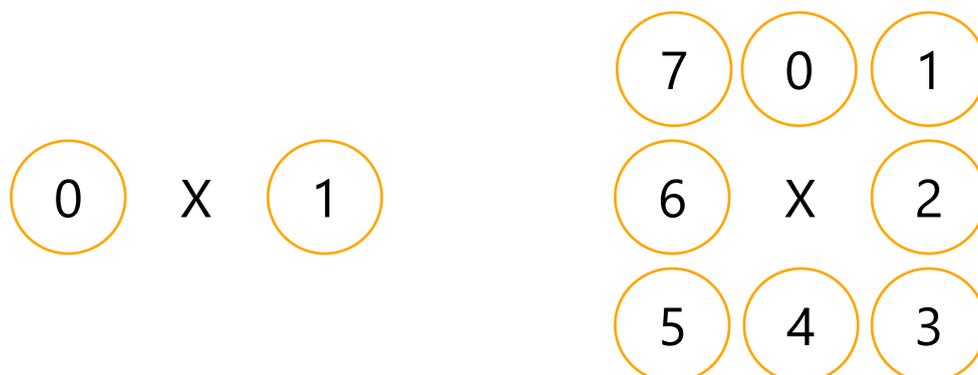
При каждом открытии документа на компьютере «читателя» на сервер отправляется запрос доступа и присваивается уникальный номер операции.

Этот номер присутствует в документе в 2-х видах:

1. Водяная метка на документе
2. Закодированный номер, реализованный с помощью метода стеганографии (микросдвигов различных участков документа)

## Процесс кодирования документа

1. Номер операции доступа к документу представляется в виде двоичного числа с 32 разрядами.
2. При защите документа на его страницах автоматически выбираются блоки текста или изображений (слова, абзацы, элементы схем и т. п.). Для каждого блока производятся сдвиги в двух или восьми направлениях.
3. Каждый сдвиг кодирует один или три разряда двоичного числа. Трёхзначное двоичное число преобразуется в восьмеричное число, которое определяет направление сдвига, (см. рисунок ниже).



## Как расследуется инцидент утечки

При открытии или печати документа новый номер операции фиксируется в журнале доступа, который доступен только администратору. Если на копии скомпрометированного документа виден номер операции доступа к документу, вы можете найти запись об активации в этом журнале.

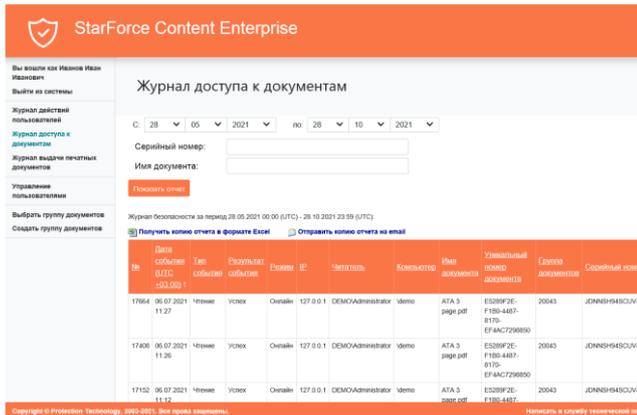
Если номер операции доступа к документу не виден (например, он замазан на фотографии экрана или документ присутствует только в частичном виде), для расследования источника утечки используется технология стеганографии. Номер операции доступа к документу определяется путем сравнения исходного защищенного (закодированного) документа и скомпрометированной копии.

Путём наложения, реализованного в программе, можно установить закодированные сдвиги, получить номер, зашифрованный в двоичном виде, по нему восстановить сам номер операции и найти соответствие ему журнале доступа к документам.

После сравнения скомпрометированного документа и его оригинала администратор получает уникальный код, по которому определяет канал утечки.



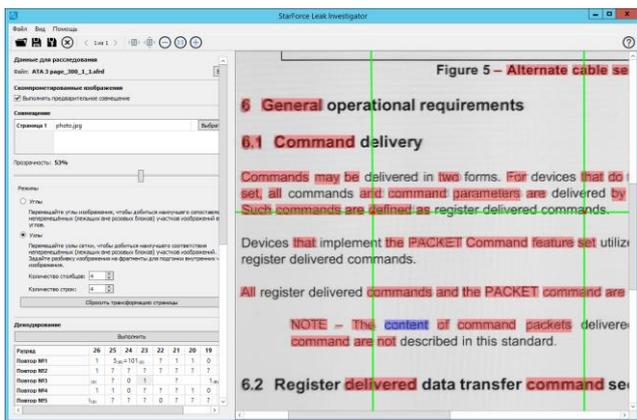
# Интерфейс администратора



Интерфейс журнала доступа к документам системы **StarForce Content Enterprise**, в котором собирается вся информация по использованию защищённых документов.

Интерфейс позволяет видеть историю использования документов, управлять правами пользователей, назначать и отзывать разрешения на один или группу документов.

Тут же находится база уникальных номеров доступа.



Интерфейс **StarForce Leak Investigator** в момент проведения расследования с целью выявления серийного номера документа с применением технологии стеганографии

Розовым цветом выделены блоки текста со сдвигами, по которым программа будет устанавливать номер операции доступа к документу.



## О компании

Компания «Протекшен Технолоджи», выпускающая с 2000 года свои продукты под брэндом Star Force, создаёт решения для защиты IT-инфраструктуры от таргетированных атак, защиты информации от незаконного копирования и распространения, а также средства обфускации кода и шифрования данных.

Под торговой маркой **StarForce** продано более **70 миллионов лицензий** по всему миру. Выбор в пользу решений ООО «Протекшен Технолоджи» сделали многие крупные российские, а также известные иностранные компании IT-индустрии в Японии, Южной Корее, Германии, Франции, Италии, США и Канаде.

### Контакты:

#### StarForce Москва – Центральный офис

127106 Россия, Москва, ул. Ботаническая дом 10Д стр.1

Телефон +7 (495) 967-14-51

Коммерческие вопросы: [sales@star-force.ru](mailto:sales@star-force.ru)

<https://www.star-force.ru>

 [facebook.com/starforcecompany](https://facebook.com/starforcecompany)

 [twitter.com/starforce\\_ru](https://twitter.com/starforce_ru)

 [youtube.com/starforce](https://youtube.com/starforce)

 [vk.com/starforcecompany](https://vk.com/starforcecompany)