

Предотвращение утечек информации – ВОЗМОЖНО ЛИ ЭТО?



Андрей Эли
info@andrei-eli.ru

> 110 млн

уникальных записей
персональных данных

- ФИО
- Email
- Телефон
- Пароль
- Паспортные данные
- Место жительства
- Медицинские данные
- и др...

РАСТЕТ СРЕДНЯЯ СТОИМОСТЬ «ПРОБИВА»

+58%

Мобильные операторы

2021 – 17 000 рублей

2022 – 27 000 рублей

- 2%

Банки

2021 – 26 000 рублей

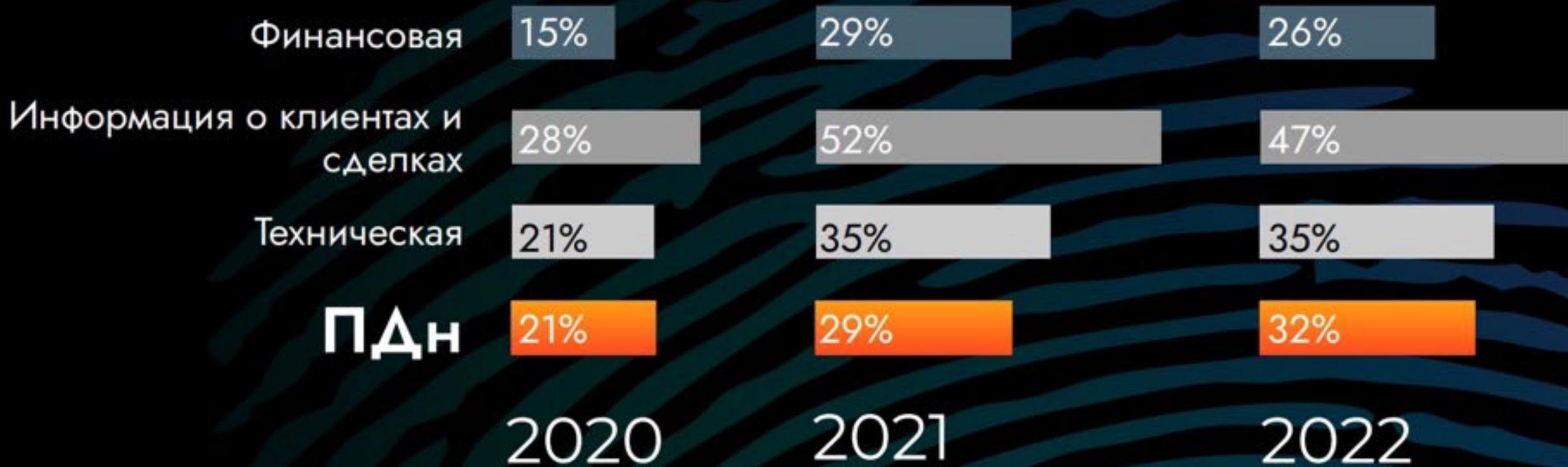
2022 – 25 500 рублей

+25%

Государственные органы

2021 – 2 000 рублей

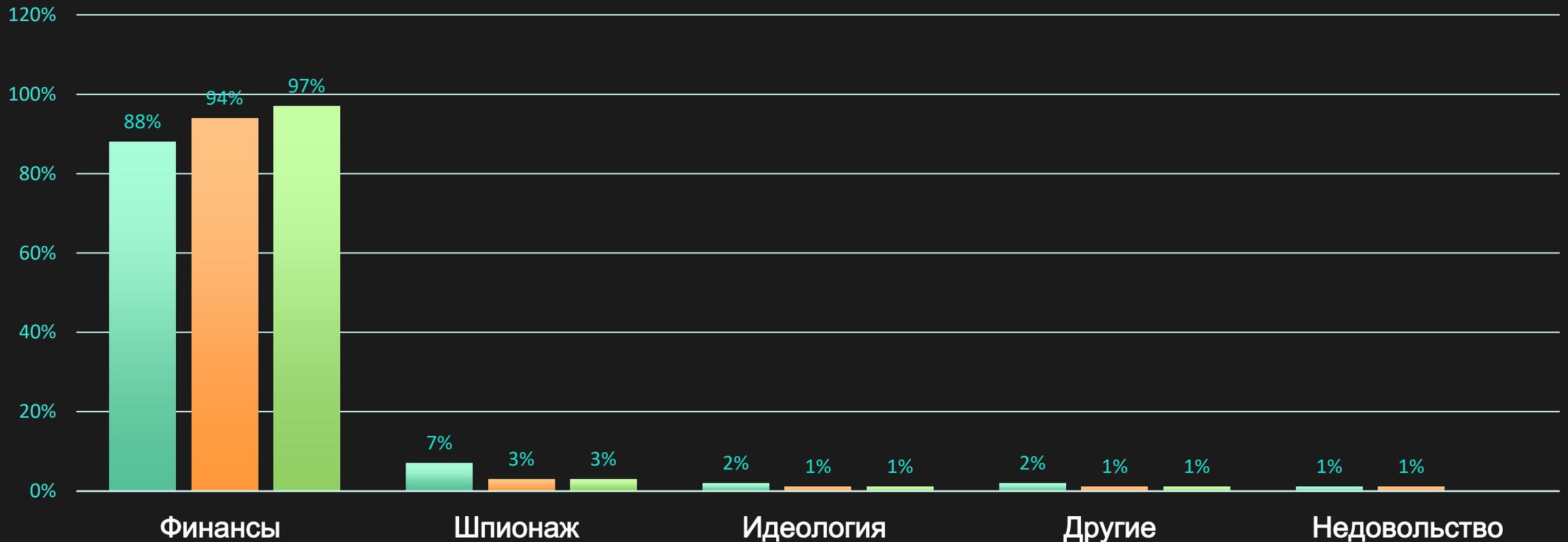
2022 – 2 500 рублей



Мотивация внешних злоумышленников

Мотивация

■ 2021 ■ 2022 ■ Финансовый сектор 2022





Поправки в 152 ФЗ – головная боль?

Уведомлять оператора о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) ПД, повлекшей нарушение прав субъектов ПД (ч. 3 ст. 6 Закона о ПД в новой ред.).

Оператор обязан принимать меры, не обходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, не обходимых и достаточных для обеспечения выполнения обязанностей,

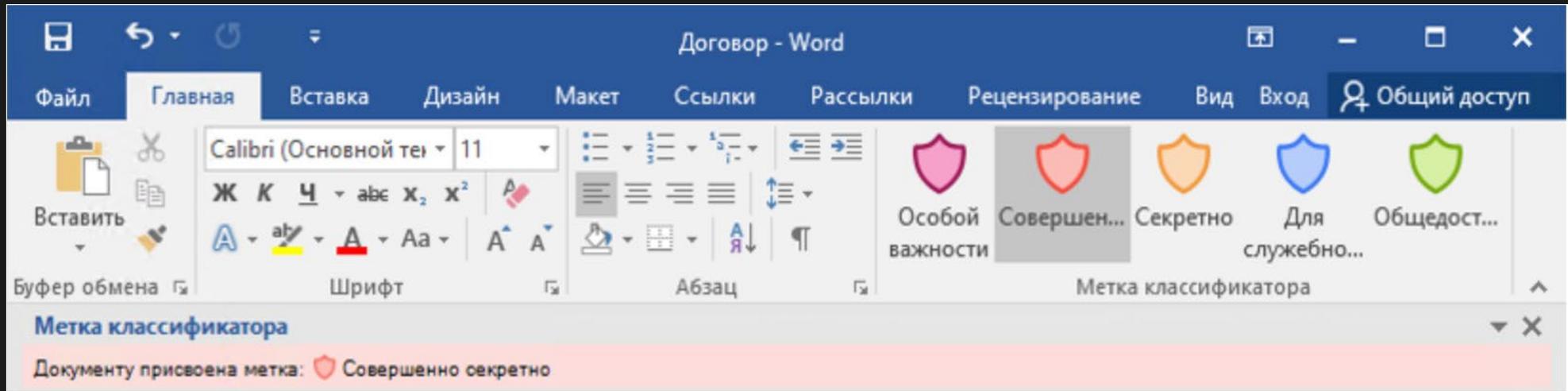
предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.

Введение оборотного штрафа. Штраф в размере от 1% до 3% годовой выручки за повторную утечку персональных данных

Контекстный анализ – какие решения принято использовать?

- DLP: предотвращение утечек информации.
- DСАР: категорирование информационных массивов организации – файловых хранилищ, аудит прав доступа к файлам, а также регистрация обращений к ним пользователей.
- Маркирование информации (метки конфиденциальности): простановка «видимых» и «невидимых» грифов конфиденциальности.

Метки конфиденциальности



Метки конфиденциальности

The image shows a screenshot of the Microsoft Azure Information Protection (AIP) interface. The main window is titled "Microsoft Azure Information Protection" and contains several configuration fields:

- Чувствительность** (Sensitivity): Строго конфиденциально (Strictly confidential)
- Выбор разрешений** (Select permissions): Выбор разрешения (Select permission)
- Выбор пользователей, групп или организаций** (Select users, groups, or organizations): Пример: John@contoso.com (Example: John@contoso.com)
- Завершение срока действия доступа** (Expiration of access): Никогда (щелкните, чтобы...)

At the bottom of the main window is a "Применить" (Apply) button. Overlaid on top of this window is a smaller dialog box, also titled "Microsoft Azure Information Protection", with the following content:

Требуется обоснование (Justification required)

Ваша организация требует обосновать изменение этой метки классификации. (Your organization requires justification for changing this classification label.)

- Предыдущая метка больше не применяется (Previous label no longer applies)
- Предыдущая метка была неверной (Previous label was incorrect)
- Другое (поясните) (Other (explain))

Below the radio buttons is a large text input field for providing justification. At the bottom of the dialog box are "Изменить" (Change) and "Отмена" (Cancel) buttons.

Коммерческая тайна
ООО «Рога и копыта»
г. Москва, ул. Ленина 1

Мессенджеры и социальные сети – стоит ли разрешать?

Плюсы

- + Открытость бизнеса (ближе к клиенту)
- + Большой охват получаемой информации
- + Меньше рисков ухода информации в «серую» зону

Минусы

- Увеличение рисков утечки конфиденциальной информации
- Увеличение нагрузки на оператора/ИТ
- Увеличение попыток обхода ограничений ИБ
- Запрет использования при передаче ПДн



Виды блокировок, что возможно?

Контентная блокировка

- Съёмные носители
- Печать
- Отправка в облака и файлообменники
- Отправка по электронной почте
- Отправка в отдельно взятые приложения (radmin, telegram и др.)
- Интеграция с корпоративным мессенджером по API
- Интеграция с системой обмена файлами

Белые списки

- Тоже что и контентные
- Интернет-ресурсы
- Программное обеспечение (версионность, издатель, подпись и др.)
- Сетевые диски (smb, nfs, webdav и др.)



Карантин – средство осведомления и «дополнительная ответственность»

Добрый день, коллега! Ваше письмо #133830 было заблокировано политикой информационной безопасности. Если вы считаете то произошла ошибка, то перейдите по ссылке: [Разблокировать сообщение](#)

Дата отправки: 2022-04-05 11:31:07 +03:00

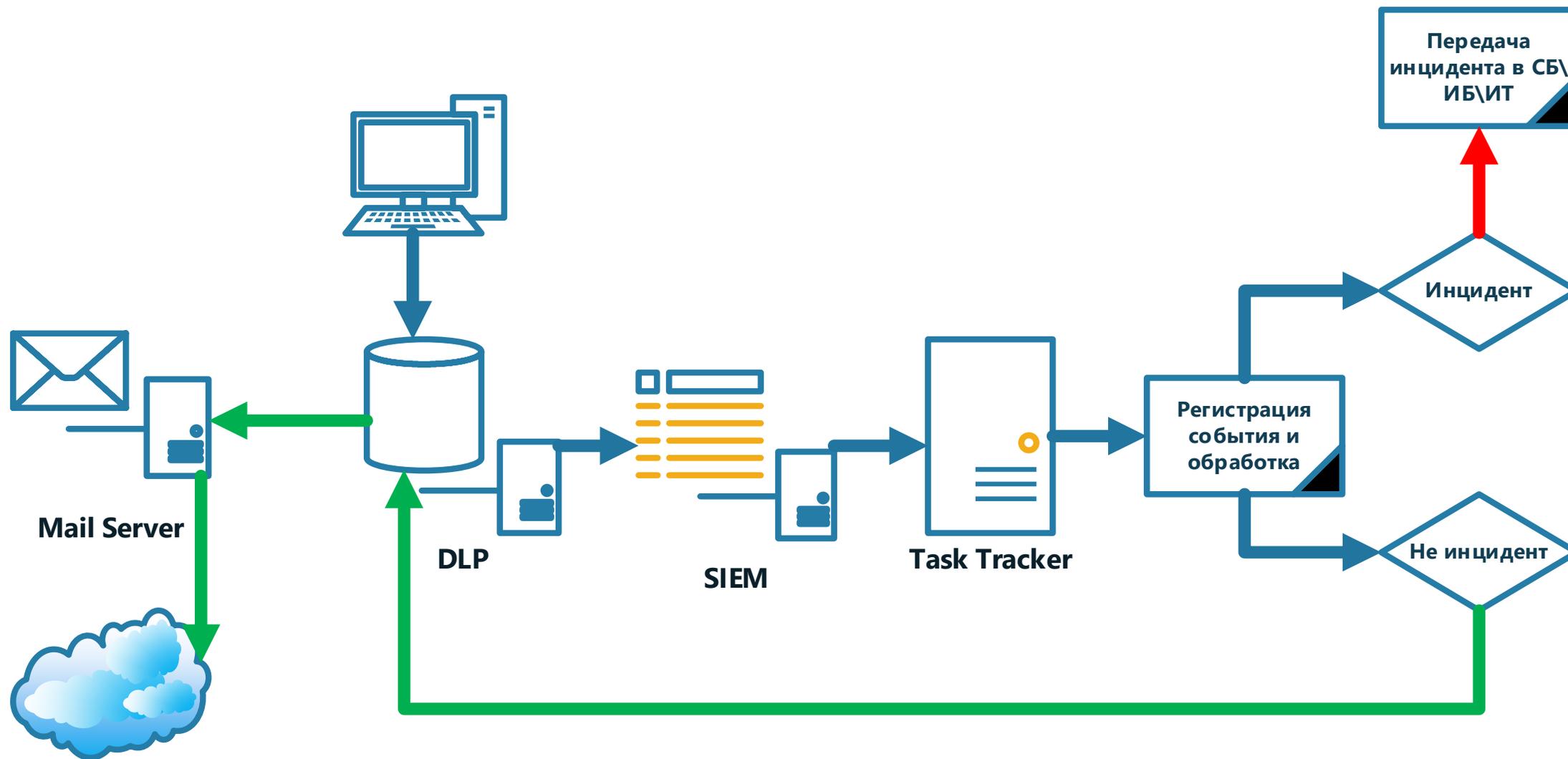
От кого: <.ru>

Кому: <@gmail.com>

Тема письма: FW: продление

Данное уведомление сформировано автоматически и не требует ответа

Регистрация инцидентов и назначение задач на ответственных



[Спасибо!]



Андрей Эли
info@andrei-eli.ru
tg: @andreyр

