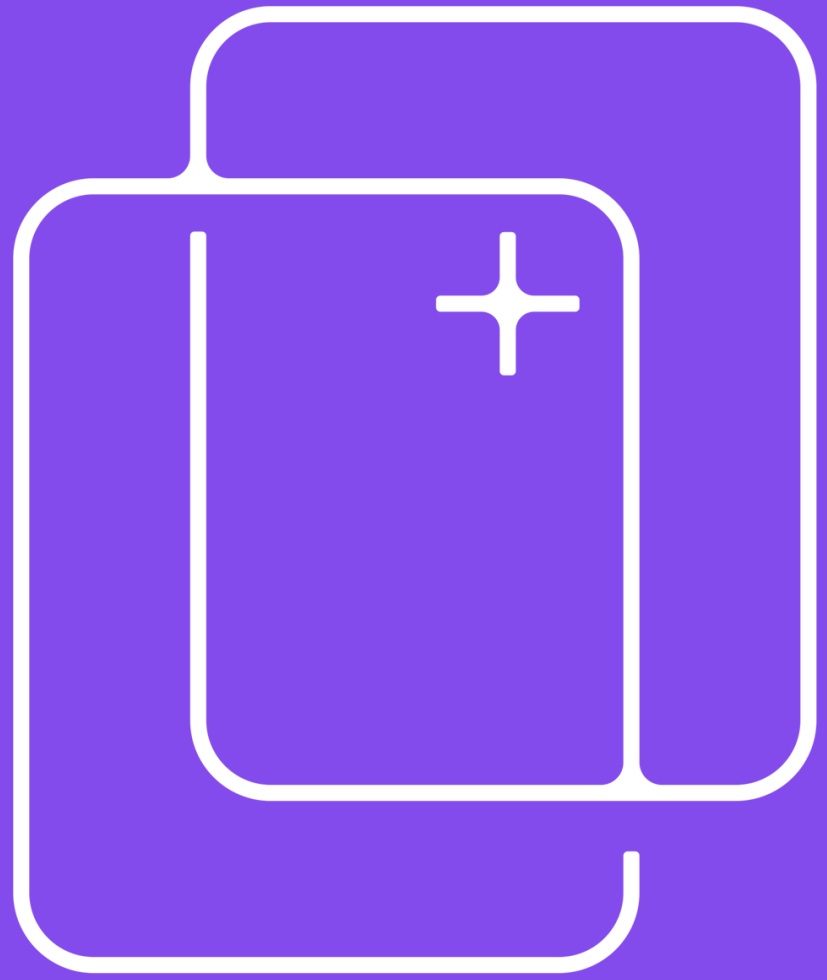
Мониторинг и управление инцидентами



Алексей Некрасов
Старший специалист отдела внедрения

Контур Эгида

kontur.ru/aegis

Задумайтесь, сколько стоит час простоя вашего бизнеса? А теперь представьте что хакерская атака, или случайная ошибка сотрудника останавливают работу на сутки, а то и неделю...

Но всё ещё большое количество компаний откосятся к информационной безопасности по принципу «авось не коснется».

Правило фисташки:
всегда проще добраться до тех, кто раскрыт больше.

Методы и «улов» злоумышленников

Рисунок 14. Методы атак (доля успешных атак)

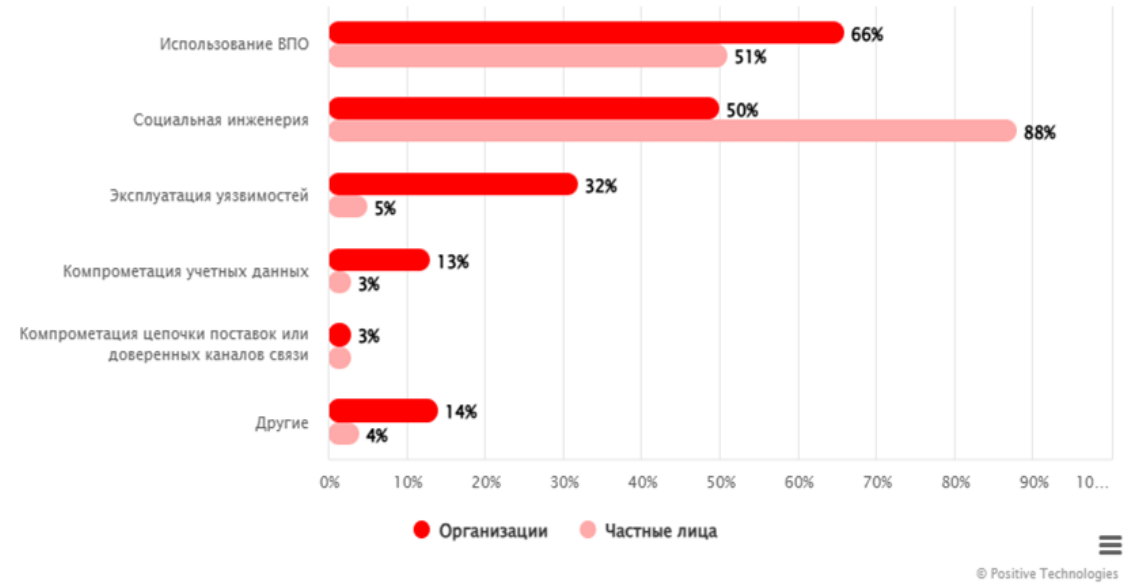
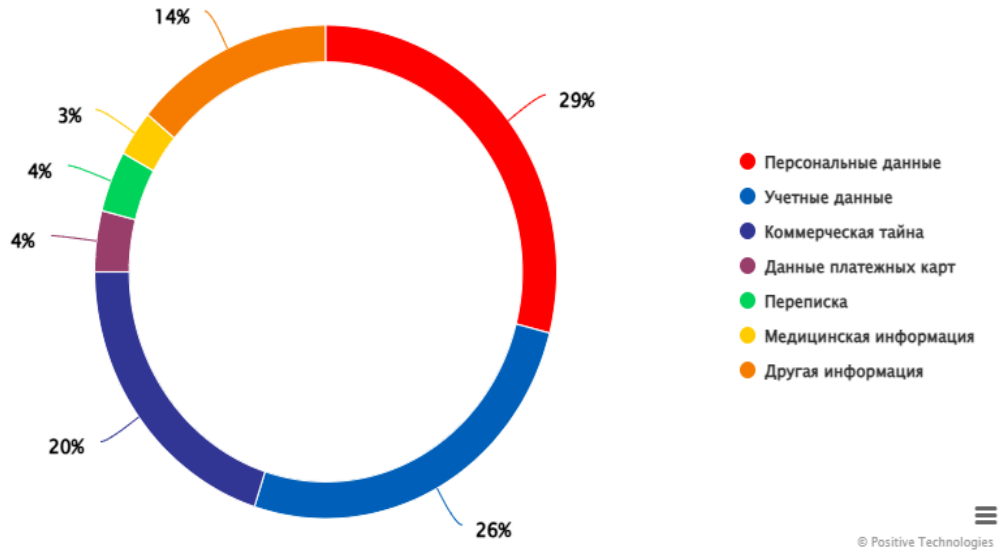


Рисунок 9. Украденные данные (доля успешных атак на организации)



Как сделать ИБ частью бизнеса без боли

Почему это важно не только для компании

На примере личной безопасности сотрудника решите задачи организации.

ИБ как процесс, а не «зеленая кнопка»

Технологии и решения меняются, как и атаки, поэтому вы тоже должны адаптироваться под эти изменения.

Автоматизация, а не рутина

Проводите аудиты, выявляйте слабые места, повышайте уровень осознанности сотрудников, оповещайте об актуальных опасностях.

С чего стоит начать, даже если бюджет или экспертиза ограничены

Закройте первичные потребности которые стоят в организации – Антивирус, требования регуляторов

Начните с фундамента – организуйте инфраструктуру так, чтобы ей было удобно управлять

Тестируйте и используйте решения, которые могут решать максимум ваших задач, а также могут интегрироваться с другими решениями

Возможности IRM, которые предоставляет Контур.Staffcop

Расследования

Инцидентов внутренней информационной безопасности
Причин неэффективной работы

Выявление

Коррупционных схем и мошенничества внутри компании
Нелояльных сотрудников, работающих на конкурентов

Уведомления

Оповещение на почту или Telegram по инцидентам, которые вас интересуют

Блокировка

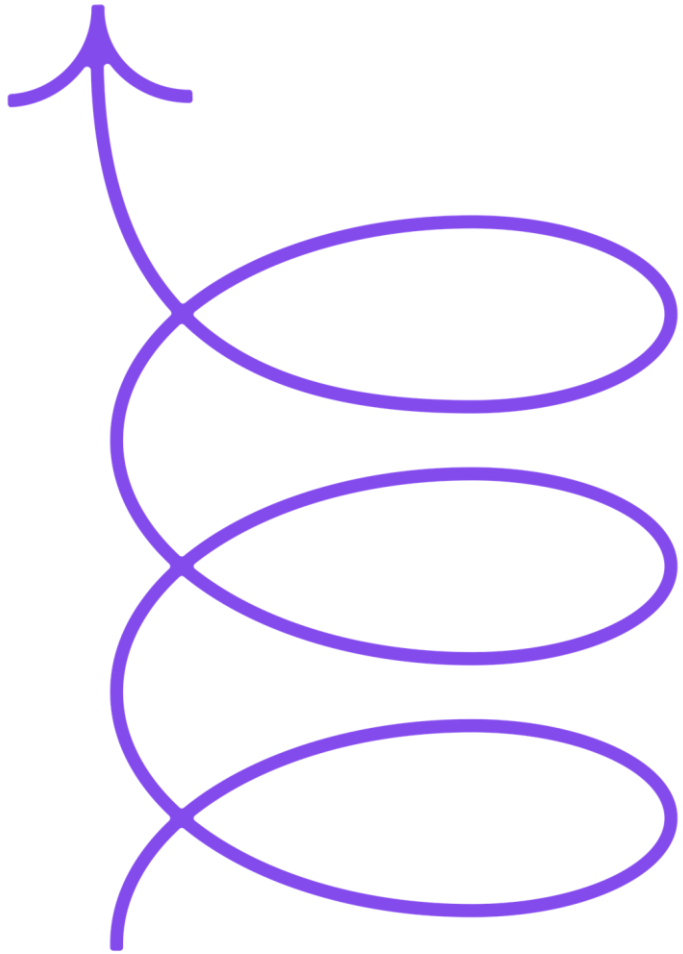
Копирования съемные носители
Доступа к нерегламентированным ресурсам
Пересылки конфиденциальной информации

Кейс

Компания использует только классическую DLP.
Последние месяцы в интернете и СМИ регулярно всплывают документы с грифом «коммерческая тайна».
Отследить источник невозможно — в логах шлюза нет нужной детализации.

ИБ-служба в тупике.

Выявление нарушений на этапе тестирования



Итог:
Закуплен Staffcop на весь парк ПК. Утечки прекращаются — ИБ-служба получает полный контроль над действиями пользователей. DLP остается только на шлюзе.

Жду ваших вопросов!

ИБ – это не про паранойю, а про уверенность в завтрашнем дне. Начинайте с малого и масштабируйте по мере роста.

Алексей Некрасов

Старший специалист отдела внедрения

Контур Эгида

kontur.ru/aegis