ANALYTICUM+
IT COMPANY

АУДИТ **ИНФОРМАЦИОННОЙ** БЕЗОПАСНОСТИ

Выявим уязвимости в системе безопасности
и спасем от финансовых и репутационных потерь

АЛЬБЕРТ ЗИЯЗИТДИНОВ

Эксперт в области автоматизации бизнеса

16+ ЛЕТ В IT-СФЕРЕ

7+ ЛЕТ В УПРАВЛЕНИИ БИЗНЕСОМ

400+ ЭКСПЕРТНЫХ КОНСУЛЬТАЦИЙ

100+ КОМПАНИЙ НА ПОСТОЯННОМ СОПРОВОЖДЕНИИ

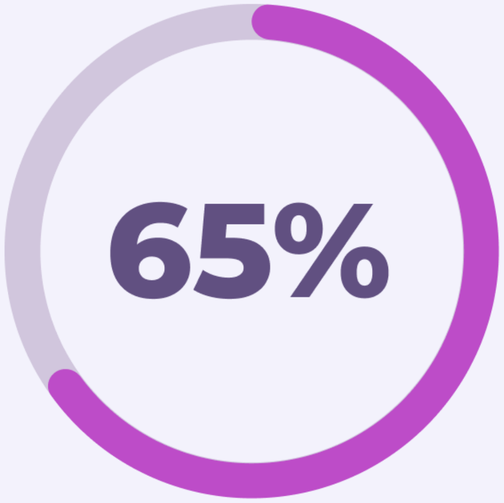
60% КЛИЕНТОВ - ПРОМЫШЛЕННЫЕ КОМПАНИИ

50+ ВНЕДРЕНИЙ КОМПЛЕКСНЫХ РЕШЕНИЙ

ДАННЫЕ КОМПАНИИ - ВАЖНЕЙШЕЙ РЕСУРС

База клиентов и поставщиков, кадровые документы, договоры и данные 1С - все это ценная информация, которую необходимо защищать.

Ежегодно в России растет количество случаев утечки данных, как из-за взломов, так и по вине сотрудников.



утечек связано с преднамеренными или случайными действиями персонала компании

290 тыс.

Инцидентов безопасности за 1 полугодие 2023

по данным Ростелеком солар.

20 млн руб. в год.

Теряет в среднем российская компания из-за кибератак

по данным Ростелеком солар.

5 СЦЕНАРИЕВ ПОТЕРИ ДАННЫХ

1

МАССОВАЯ АТАКА

Одновременная атака множества компаний с целью шифрования данных и получения денежного вознаграждения.

2

ЗАКАЗНАЯ АТАКА

Атака, направленная на конкретную компанию для нанесения финансового и репутационного ущерба.

3

ВНУТРЕННЯЯ УМЫШЛЕННАЯ УТЕЧКА

Сотрудники намеренно похищают, искажают информацию или передают ее третьим лицам.

4

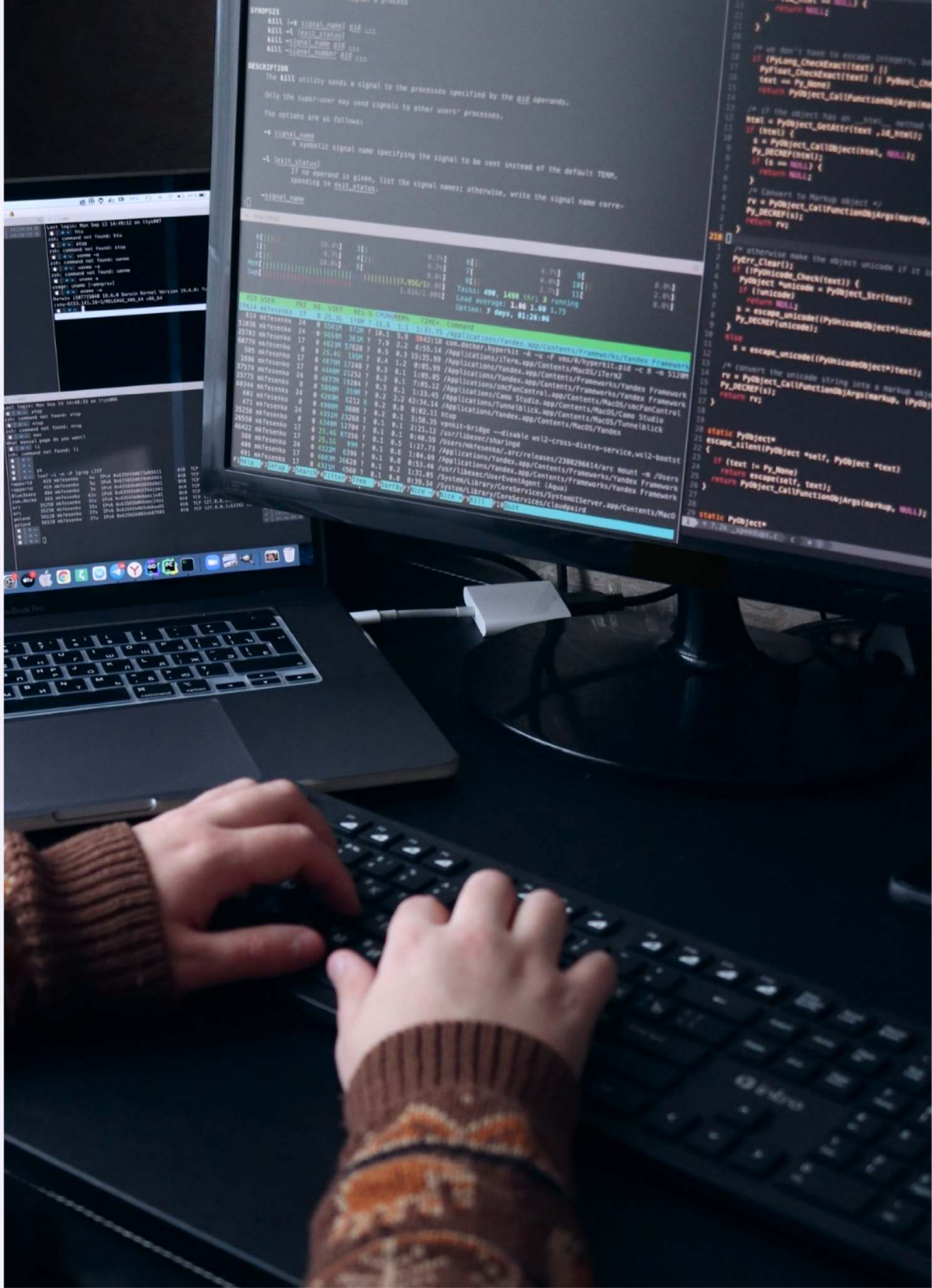
ВНУТРЕННЯЯ НЕПРЕДНАМЕРЕННАЯ УТЕЧКА

Сотрудники по незнанию или неосторожности дают доступ к данным.

5

ПОЛОМКА ОБОРУДОВАНИЯ

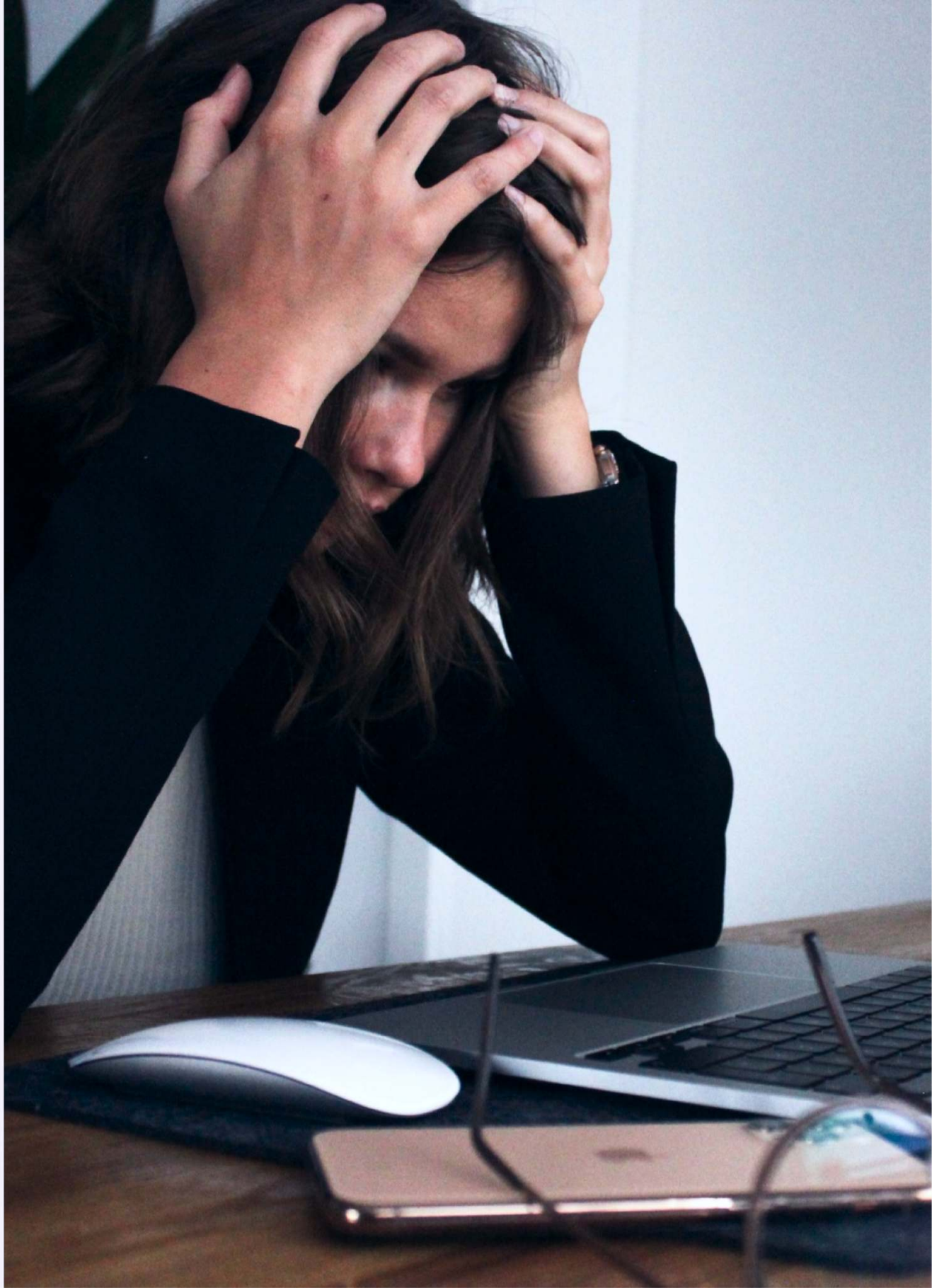
Потеря информации в следствие уничтожения ее физического носителя.



ПОСЛЕДСТВИЯ ДЛЯ КОМПАНИИ

1. ФИНАНСОВЫЕ ЗАТРАТЫ НА ВЫКУП ДАННЫХ ИЛИ ДЕШИФРАТОРА
2. ШТРАФ ОТ ГОСУДАРСТВА ПРИ УТЕЧКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
3. РЕПУТАЦИОННЫЕ РИСКИ, ВКЛЮЧАЯ ПОТЕРЮ КЛИЕНТОВ
4. ПРИОСТАНОВКА ДЕЯТЕЛЬНОСТИ (ПОТЕРЯ ДЕНЕГ И РЕПУТАЦИИ)

МОЖНО ПРЕДОТВРАТИТЬ



АУДИТ БЕЗОПАСТНОСТИ ОТ АНАЛИТИКУМ ПЛЮС

Эксперт проведет оценку состояния информационной безопасности вашей компании и предложит перечень рекомендаций для повышения уровня защищённости. Совместно с вашими специалистами сформирует план развития ИБ.

АНАЛИЗ ТЕКУЩЕЙ СИТУАЦИИ ЭКСПЕРТОМ

Включает в себя диалог с ответственными лицами, оценку оборудования, сетевой инфраструктуры, идентификацию критических активов и уязвимостей, а также оценку рисков.

ТЕСТИРОВАНИЕ СИСТЕМ

Включает в себя пентест (тестирование безопасности на проникновение), сканирование уязвимостей и анализ журналов безопасности. Результаты тестирования позволяют выявить слабые места в системе.

РАЗРАБОТКА ПЛАНА ДЕЙСТВИЙ ДЛЯ УСТРАНЕНИЯ ПРОБЛЕМ

В зависимости от выявленных на 1 и 2 шаге угроз, может включать в себя приобретение ПО и систем мониторинга, установку обновлений, усиление политики паролей, обучение сотрудников отдела безопасности и другие меры.

РАЗРАБОТКА СТРАТЕГИИ БЕЗОПАСНОСТИ*

На основе собранных данных наши специалисты помогут разработать стратегию безопасности компании. Это совокупность действий, направленных на повышение уровня защиты в долгосрочной перспективе.

*Дополнительная услуга

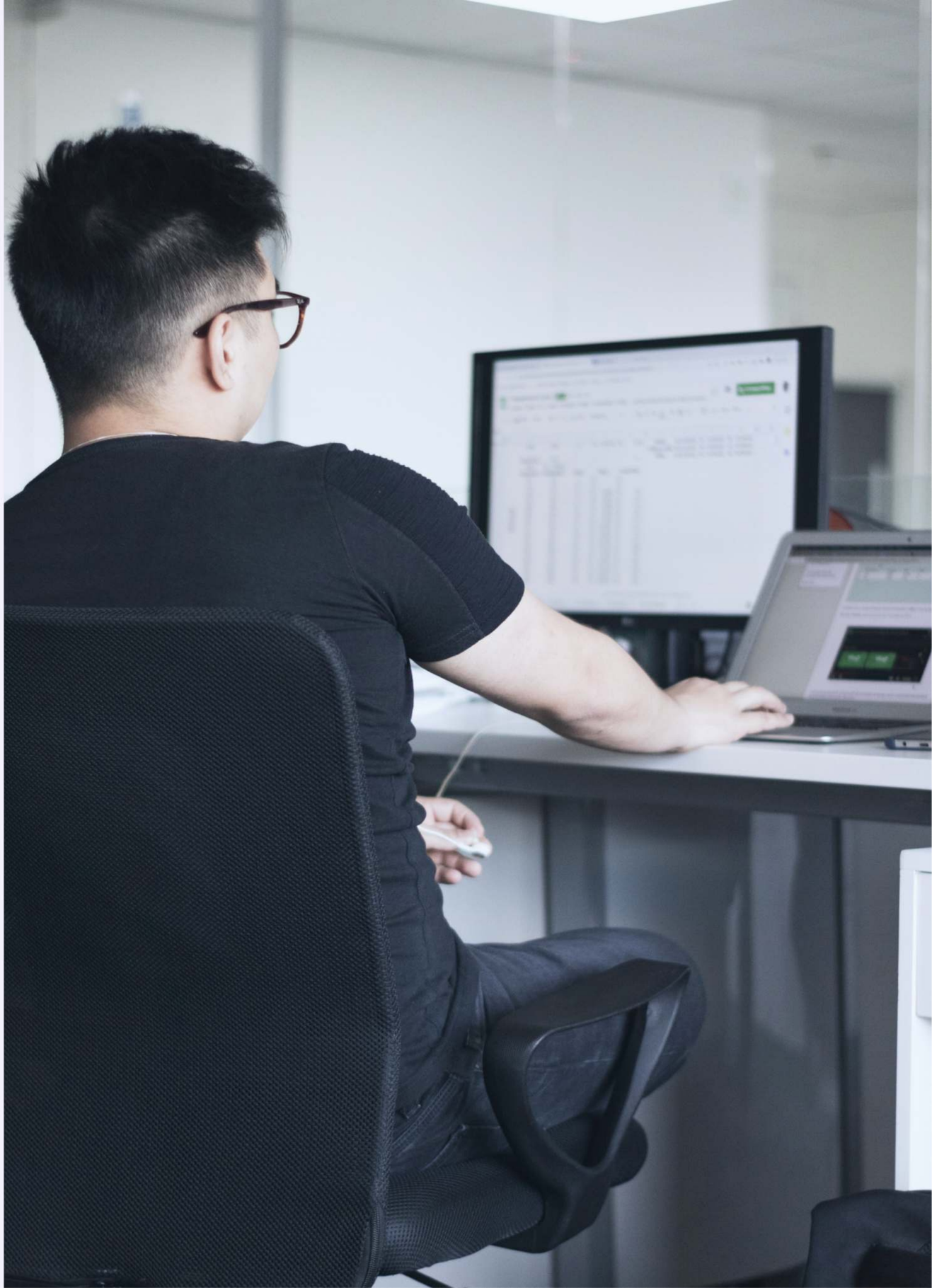
В ПРОЦЕССЕ АУДИТА МЫ ПРОВЕРИМ 2 СОСТАВЛЯЮЩИЕ ИНФРАСТРУКТУРЫ: ИНФОРМАЦИОННУЮ И ТЕХНИЧЕСКУЮ

АНАЛИЗ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ:

1. КАК С ИНФОРМАЦИЕЙ РАБОТАЕТ ПЕРСОНАЛ
2. КТО И КАК УПРАВЛЯЕТ ДОСТУПОМ К ИНФОРМАЦИИ
3. КАК ОБЕСПЕЧИВАЕТСЯ ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ
4. КТО СЛЕДИТ ЗА ИНЦИДЕНТАМИ В СФЕРЕ ИБ
5. КАК ПРОХОДИТ АРХИВАЦИЯ, ВОССТАНОВЛЕНИЕ, ДУБЛИРОВАНИЕ ДАННЫХ
6. КАК КОНТРОЛИРУЕТСЯ ДОСТУП К СЕТИ ВНУТРИ КОМПАНИИ И ИЗВНЕ
7. ПОЛУЧАЮТ ЛИ ДОСТУП К ИНФОРМАЦИИ СТОРОННИЕ ЛЮДИ
8. КАК ПОДКЛЮЧАЮТСЯ К СИСТЕМЕ МОБИЛЬНЫЕ УСТРОЙСТВА И ФЛЕШКИ

АНАЛИЗ ТЕХНИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ:

1. КОМПЬЮТЕРЫ И СЕТЕВОЕ ОБОРУДОВАНИЕ
2. БАЗЫ ДАННЫХ И АНТИВИРУСЫ
3. ОПЕРАЦИОННЫЕ СИСТЕМЫ НА СЕРВЕРАХ И ПК
4. ВСЕ ПРОГРАММЫ И ПРИЛОЖЕНИЯ, КОТОРЫЕ ИСПОЛЬЗУЮТ В КОМПАНИИ
5. ФИЗИЧЕСКИЕ ХРАНИЛИЩА: СЕРВЕРНЫЕ И АРХИВНЫЕ КОМНАТЫ, СЕЙФОВОЕ ОБОРУДОВАНИЕ, ВИДЕОКАМЕРЫ, ОХРАННЫЕ И ПРОТИВОПОЖАРНЫЕ СИСТЕМЫ



ПОЛЬЗА АУДИТА

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ

Выявить потенциальные уязвимости и слабые места в системе, которые могут быть использованы злоумышленниками для атак. Это позволит предпринять шаги по их устранению до того, как произойдет инцидент.

ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

Контролировать доступ к конфиденциальным данным и убедиться в том, для защиты информации используются правильные политики и механизмы шифрования.

ОЦЕНКА СООТВЕТСТВИЯ БИЗНЕС-ПРОЦЕССАМ

Убедиться, что данные компании защищены на каждом этапе бизнес-процесса и система соответствует стандартам безопасности

СОДЕЙСТВИЕ В ПРИНЯТИИ СТРАТЕГИЧЕСКИХ РЕШЕНИЙ

Оценить текущее положение и предложить обоснованные решения по инвестициям в безопасность и улучшению процессов.

МОНИТОРИНГ АКТИВНОСТИ И ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ

Быстро реагировать на инциденты и пресекать их до того, как они приведут к утечке данных или иным угрозам.

ЗАЩИТА РЕПУТАЦИИ И КЛИЕНТСКОГО ДОВЕРИЯ

Утечка данных или другие инциденты в области информационной безопасности могут серьезно повредить репутацию организации.

ПРЕИМУЩЕСТВА АУДИТА ИБ ОТ АНАЛИТИКУМ ПЛЮС

НЕПРЕДВЗЯТОЕ ОТНОШЕНИЕ И ПРОФЕССИОНАЛИЗМ

Объективная оценка ситуации, подбор оптимальных технологий

ПРАКТИЧЕСКИЙ ОПЫТ ОБЕСПЕЧЕНИЯ ИБ КЛИЕНТОВ

Экспертиза работы с компаниями различного размера и сферы деятельности

ЭКОНОМИЯ РЕСУРСОВ КОМПАНИИ

Возможность составить четкий план работ по ИБ и просчитать IT-бюджет

БАЗОВАЯ ЦЕНА 20 000 РУБ.

Зависит от размера IT-инфраструктуры и бизнес-процессов компании

НАШИ ПАРТНЕРЫ

ANALYTICUM+
IT COMPANY

УЗНАЙТЕ, **ЧТО УГРОЖАЕТ** БЕЗОПАСНОСТИ ДАННЫХ КОМПАНИИ

СВЯЖИТЕСЬ С НАМИ

Чтобы узнать подробности
и начать сотрудничество

8 351 939-38-10

8 908 055-45-37

info@analyticum.pro

analyticum.pro