ProfCheck

Самый опасный сотрудник уже подал заявление об увольнении

Это окно, между уведомлением и последним рабочим днём, самый рискованный период за весь цикл занятости. И дело не только в громких кражах. Выглядит это и так: копирование списка клиентов для личного пользования. Пересылка документов с ценами на личную почту, чтобы сохранить примеры работ. Фотографирование методик, которые сотрудник написал сам и поэтому уверен, что они принадлежат ему. А иногда и вовсе без злого умысла: облачная учётная запись, которая остаётся открытой спустя месяцы после ухода, потому что никто не знал о её существовании.

Вот как его закрыть. Шесть шагов:

1. День уведомления и есть день оповещения. Заявление об увольнении попадает к офицеру безопасности и в ИТ в тот же день. Не в конце недели и не после того, как согласуют дату ухода.

2. Немедленная карта доступов. К каким системам, базам данных и папкам у сотрудника есть доступ и что из этого особенно чувствительно с учётом места, куда он переходит.

3. Поэтапное сокращение. Всё, что не нужно для передачи дел, закрывается сейчас, а не в последний день.

4. Контроль окна. Аномальные по объёму загрузки, пересылка на личную почту, подключение съёмных носителей. В период окна это не подозрительность, это самое известное слабое место.

5. Задачи последнего дня. Закрытый список учётных записей на отключение, включая облачные системы и внешних поставщиков, не подключённых к централизованному управлению пользователями. Именно о них забывают всегда.

6. Структурированная выходная беседа. Напоминание об обязательствах по конфиденциальности и интеллектуальной собственности и открытый разговор о следующем месте работы. Не из подозрительности, а в рамках управления рисками.