

ПРИЩУР ЧЕТКОЙ СТРУКТУРЫ

УТЕЧКА ДАННЫХ СПОСОБНА НАНЕСТИ ЗНАЧИТЕЛЬНЫЙ УРОН КОМПАНИИ И ПОДОРВАТЬ ДОВЕРИЕ К БРЕНДАМ. ПОЭТОМУ НАНИМАТЕЛИ УСИЛИВАЮТ КОНТРОЛЬ ЗА ДЕЯТЕЛЬНОСТЬЮ СВОИХ СОТРУДНИКОВ. КАКАЯ СЛЕЖКА НЕОБХОДИМА, ЗАКОННА И ЭФФЕКТИВНА, РАЗБИРАЛСЯ КОРРЕСПОНДЕНТ ВГ РОМАН РУСАКОВ.

Корпоративные данные — один из самых ценных активов компании. Утечка информации ведет к прямым финансовым потерям. Актуальнее всего это для предприятий, занимающихся производством уникальной продукции, а также для фирм, чей основной доход связан с обработкой больших объемов данных.

Защищают бизнес от противоправных действий сотрудников федеральный закон «О коммерческой тайне» и отдельные нормы Трудового кодекса. Вместе с тем, полагает директор центра компетенций «Гарда Технологии» Роман Жуков, они дают руководителям правовые основания контролировать корпоративные ресурсы и ограничивать сотрудникам возможности использовать свои трудовые ресурсы ненадлежащим образом. «Мониторинг обстановки для защиты активов — вынужденная практика. Люди работают на компьютерах предприятия и создают продукцию в интересах собственников, хотя некоторые до сих пор считают, что это не так, что присвоить себе интеллектуальную собственность, базу клиентов, заниматься майнингом криптовалют или просто бездельничать, играть в игры и сидеть в соцсетях на работе — это норма. Работодатель платит зарплату, полностью финансирует средства производства и вправе рассчитывать на ответный добросовестный труд», — полагает господин Жуков. По его словам, когда дело доходит до реальных расследований, угрозы дисциплинарной или иной ответственности, сотрудники пытаются «сыграть» на тайне переписки и личной жизни, в ответ обвиняя компанию в чтении личных писем. Это слабая позиция, уверен директор компании «Гарда Технологии». «Работодатель закрепляет во внутрикорпоративной нормативной документации очевидные вроде бы вещи: компьютеры должны использоваться исключительно в производственных целях, в связи с чем любые личные коммуникации — это уже нарушение со стороны работника. Поверьте, компаниям нет дела до "скелетов в чужих шкафах", они стремятся уберечь себя от мошенничества. Кроме того, мониторинг деятельности сотрудников полезен не только компании, но и самим работникам», — утверждает Роман Жуков. Часто противоправные действия совершаются не по злему умыслу, говорит он, а просто по незнанию или халатности. «И главное, что отличает мониторинг от паранойи контролировать все и всех, это современные технологии машинного анализа, без необходимости устраивать слежку со стороны службы безопасности, — подчеркивает эксперт. — Применяются Big Data и

Machine Learning, они позволяют автоматически выявлять сложные и хитроумные мошеннические схемы, еще до причинения реального ущерба».

Ирина Доброхотова, председатель совета директоров компании «Бест-Новострой», с коллегой солидарна: «Почта с корпоративным аккаунтом — на то и корпоративная, она не является личной, и переписка в ней не является личной перепиской. Поэтому компания имеет право такую почту просматривать и анализировать. Нередко это делается вовсе не с целью шпионажа за расходом времени сотрудников, а с целью предотвратить различные утечки информации, в том числе непроизвольные». Иногда сотрудники пересылают по почте важные документы (договоры, акты) или информацию о финансовых операциях, уточняет госпожа Доброхотова. В задачи службы безопасности входит предотвращать такие утечки, а кроме того, постоянно напоминать, какие файлы можно пересылать и открывать в рабочих почтовых ящиках. «Поэтому в компаниях, которые следят за информационной чистотой, проверка рабочей почты — очень важный момент. Особенно сегодня, когда многие бизнес-процессы переходят на цифровизацию», — поясняет она.

ТОНКАЯ ГРАНЬ По мнению генерального директора Бюро корпоративного консалтинга и безопасности Алексея Долженкова, проверка корпоративной почты и телефона, расследования, проверка компетентности и профессиональной пригодности сотрудника проводиться могут, но следует учитывать важное исключение. «"Шпионить" за сотрудником можно в той мере, пока не нарушаются его личные права на неприкосновенность частной жизни и личности. То есть проводить обыск или осмотр сотрудника после работы, вскрывать его личные ящики, проверять личную почту сотрудников — запрещено. Если у работодателя есть подозрение в нарушении работником законов, он должен сообщить об этом в органы внутренних дел», — говорит господин Долженков.

Практика по корпоративной почте — на стороне работодателя: суды исходят из того, что служебная почта — мера технического обеспечения работника, поэтому она должна использоваться в рабочих целях. Были даже случаи увольнений за невыполнение трудовой функции и использование рабочей почты в личных целях, рассказывает Алексей Долженков. Опротестовать эти случаи в суде с учетом соблюдения процедуры увольнения у работников не получилось.



1. МАКСИМ ШАФИРОВ,
генеральный директор JetBrains

2. АНДРЕЙ ТЕРЕХОВ,
президент ЗАО «Ланит-Терком»

3. АЛЕКСАНДР ЕГОРОВ,
генеральный директор ООО «Рексофт»;

АНДРЕЙ ФЕДОРОВ,
председатель совета директоров ГК Digital Design

В ГОЛОСОВАНИИ ТАКЖЕ УЧАСТВОВАЛИ

СЕРГЕЙ БАКЛАН,
генеральный директор АО «Аркадия»

ПАВЕЛ ВАСИЛЬЕВ,
генеральный директор компании «АстроСофт»

ИГОРЬ ГОРЬКОВ,
генеральный директор компании Nexign

ДМИТРИЙ ДЫРМОВСКИЙ,
генеральный директор ГК «Центр речевых технологий»

ПАВЕЛ ЕГОРОВ,
генеральный директор Санкт-Петербургского центра разработок Dell EMC

АРТЕМ МИХАЙЛОВ,
генеральный директор ООО «Е-Легион»

ВЛАДИМИР ПОНОМАРЕВ,
директор по развитию бизнеса АО «Вяртсиля Цифровые Технологии»

АНДРЕЙ РОГОЗОВ,
управляющий директор «ВКонтакте»

МАКСИМ САМСОНОВ,
первый заместитель генерального директора GS Labs

АЛЕКСЕЙ СЕМЕНОВ,
председатель правления ГК «Геоскан»

СВЕТЛАНА СОКОЛОВА,
генеральный директор ООО «Промт»

АЛЕКСЕЙ ФИЛИМОНОВ,
исполнительный директор компании DataArt

ДЕНИС ШЕВЧЕНКО,
генеральный директор компании «Би Питрон»