НЕЛИЧНОЕ пространство

Информационная безопасность как элемент корпоративной культуры

Эльвира Колмыкова, HR-консультант RCC Group

В вопросе информационной безопасности обычно выделяют три направления, которые, как правило, курируются тремя разделенными корпоративными функциями.

1) Собственно информационная безопасность — защита от вирусов, нецелевых кибератак и т.п. — функция ИТ-службы.
2) Защита от внешнего целевого проникновения с целью похищения информации компании — курируют ИТ совместно со службами экономической безопасности.
3) Контроль за использованием работниками корпоративных ресурсов в личных целях, распределение авторских и смежных прав — работа ИТ, службы персонала и юридического департамента.

Третье направление, собственно, и относится к корпоративной культуре. Многолетний опыт реализации проектов в области управления персоналом на российских промышленных предприятиях химического и добывающего сектора позволил составить представление о наиболее часто встречающихся проблемах в области информационной безопасности со стороны действий персонала.

«Правильные» или «неправильные» модели обращения с информацией поддерживаются программно-аппаратными решениями, такими как камеры наблюдения или защита от копирования, но в случае с собственными сотрудниками на первый план выходит нормативно-правовая среда, наличие или отсутствие на предприятии комплекса документов, подписываемых сотрудниками, и главное — тщательно внедряемая и поддерживаемая корпоративная культура, формирующая правильное использование сотрудниками ресурсов компании.

Требования, за выполнение которых сотрудник несет полную, в том числе финансовую и юридическую ответственность, должны быть предъявлены сотруднику в письменном виде, прочтены и подписаны каждым специалистом.

Две политики

Применительно к информации, оборот которой осуществляется на предприятии, необходимо выделить две разнонаправленных задачи.

С одной стороны, компания не заинтересована, чтобы коммерческая тайна, детали процессов, существующих до прихода сотрудника и независимо от него, выходили за пределы территории, с другой стороны — чтобы права на созданные сотрудником или связанные

с им вновь полученные данные сохранялись за компанией.

Свод правил, относящихся к первой категории, рекомендуется озаглавить «Политика информационной безопасности предприятия». Политика описывает все, что необходимо компании для соблюдения требований в области обеспечения коммерческой, технологической тайны, данных о системе взаимодействия и управляющих структурах предприятия.

Раньше результаты деятельности сотрудника, которые могут быть отображены на различных информационных носителях и права на которые заинтересована закрепить за собой компания, также описывались политикой информационной безопасности.

Но после выхода закона о защите персональных данных рекомендуется иметь отдельную политику касательно этих прав, поскольку направленность документов в каком-то смысле противоположная. Данный документ можно назвать «Политика в области интеллектуальной собственности, авторских и смежных прав».

Наряду с политиками для сотрудников, описывающими ограничения, крайне желательно иметь внутреннюю управленческую политику, направленную на премирование сотрудников за создание новых продуктов или за эффект от использования в интересах компании созданных информационных носителей (особенно если создание информационных носителей не входит в круг обязанностей конкретного сотрудника).

В трудовом договоре обязательно должен присутствовать пункт, согласно которому работник обязуется знать, понимать и выполнять обе политики.

Самоконтроль

Существует проработанный комплекс технических решений, который со стороны «железа», компьютерных рабочих станций и сетей, контролирует оборот всех данных и позволяет анализировать действия сотрудников. (Это предмет отдельного рассмотрения.)

Но специалисты должны быть уведомлены о применении средств технического контроля.

В результате фактический контроль за использованием ресурсов в личных целях или несанкционированным доступом оказывается, как правило, номинальным — люди, будучи проинформированы о том, что все их действия фиксируются, ограничивают себя сами.

Разглашению не подлежит!

О регламентах

Комментирует руководитель отдела ИТ крупной производственной компании:
«На нашем предприятии разработан документ «Правила информационной безопасности», с которыми сотрудник знакомится и которые подписывает при трудоустройстве, как и со всеми прочими ЛНА.
Формулировки стандартные — работник, в целях осуществления своих должностных обязанностей (трудовой функции) использует... не имеет права использовать в целях, не связанных с выполнением должностных обязанностей...
В случае выявленных отклонений, например, при работе в интернете, действуем по процедуре.

1) Запрос в ИТ. Ставим перед службой вопросы: кому принадлежит такая-то запись, мог ли ей воспользоваться посторонний, какие сайты посещались в указанный промежуток времени. ИТ дает ответы, прилагает список сайтов.
2) На основании списка сайтов от ИТ делаем запрос к руководителю сотрудника, который дает заключение, может ли быть связано посещение указанных сайтов с выполнением сотрудником должностных обязанностей.
3) После ответа руководителя делаем запрос сотруднику на предоставление объяснений.
4) Пишется служебная записка от руководителя на наложение взыскания в форме замечания.
5) Накладывается замечание и сотрудник лишается премии (такая возможность прописана в Положении о заработной плате). Уволить за нарушение инфобезопасности сложно, но при систематических нарушениях и если это повлекло заметное снижение производительности или другой ущерб бизнесу, возможно и необходимо.

Надо понимать, что просмотр протоколов — дело хлопотное и небыстрое, затраты на которое растут в геометрической прогрессии при росте числа работников.

Поэтому рекомендуется иметь на предприятии программу с пользовательским интерфейсом, которая сама формирует статистику навигации и трафика, позволит не только руководителю просмотреть отчеты об использовании ресурсов, но и самим пользователям ознакомиться со своими «похождениями» — как по пространству внутренних серверов, так и в интернете.

В нашей практике, после внедрении этого механизма за счет самоконтроля непроизводственный интернет-трафик снизился в 16 раз, что значительно, иногда в разы, увеличило производительность по профильным для сотрудников направлениям.

С появлением мобильных телефонов, а особенно смартфонов, ситуация заметно усложнилась — люди отвлекаются от работы и без использования корпоративных ресурсов, и трансляция данных во внешний мир возможна также без использования защищенного сервера.

Здесь основная роль отводится прописанным и подписанным сторонами правилам, невыполнение которых может быть зафиксировано уже неаппаратными методами и также может повлечь финансовые и репутационные риски для сотрудника.

Завершенный процесс

Итак, первый шаг для предприятия — это формирование четкого понимания и позиции по каждому вопросу в сфере информационной безопасности.

Шаг второй — описывание позиции во внутренних регламентах через политики, правила и ограничения.

Третий — внедрение выработанных подходов в корпоративную политику компании.

Некоторые компании пропускают третий шаг — возможно, самый важный: руководителям кажется, что если инструкции разработаны, прочитаны и подписаны сотрудником, то он автоматически будет их выполнять. Но так не происходит.

Сотрудников нужно обучать регламентам, формировать ответственное отношение к корпоративным ресурсам (информационным в том числе), и конечно — контролировать.

В корпорациях отношение к информационной безопасности и использованию ресурсов компании являются частью корпоративной культуры, которую тщательно разрабатывают, продвигают, популяризируют, прививают новичкам, обязательно — мониторят.

При таком подходе сотрудники сами, без насильственного контроля, действуют по выработанным правилам, и компания достигает экономии на обслуживании сложных и затратных систем контроля, привлекая их только в настораживающих случаях, отслеживая только серьезные нарушения и работая с прецедентами.

Кстати, такой подход иногда применяют для реализации трудных кадровых решений, например, когда необходимо произвести сложное или потенциально конфликтное увольнение и минимизировать «торг» со стороны работника. Если на регламентах по информационной безопасности стоит подпись работника, а на актах о нарушении политик и процедур — визы ответственных лиц, то процедуры расставания с некомпетентным и потенциально конфликтным сотрудником реализуются значительно быстрее и дешевле для компании.

Компании с развитой корпоративной культурой такие кейсы используют для поддержания культуры: в одних случаях ситуацию обсуждают в узком кругу, а в других — мифологизируют и используют в качестве примера неодобряемого корпоративного поведения.

Важно понимать, что, как бы ни была «оцифрована» и автоматизирована производственная деятельность, компания работает с людьми, с сознанием людей. А значит, ключевой инструмент — это слово, произнесенное и записанное. ■

Персональные данные. Согласно требованиям закона о персональных данных, после увольнения сотрудника необходимо уничтожить все данные о нем, в том числе данные в корпоративных информационных системах. В то же время, каждый гражданин вправе выразить согласие на распространение или использование персональных данных в определенных целях. Таким образом, для выполнения буквы закона и соблюдения корпоративной безопасности необходимо получить письменное согласие сотрудника на хранение его персональных данных, в целях соблюдения политики безопасности, в закрытой ИТ-системе предприятия в том числе после увольнения.

Соцсети. Неожиданным риском для компании может обернуться слишком вольное поведение работников в соцсетях, в том числе – выкладывание в общий доступ фотографий с мероприятий, имеющих элементы частных отношений.

Сотрудница одной из фармкомпаний выложила на своей страничке в популярной соцсети несколько фотографий с выездного корпоратива. Жена одного из сотрудников узнала на фотографиях своего супруга и посчитала, что он изображен в щекотливой ситуации, в неприглядном свете. Сначала она попросила компанию убрать эти снимки, а затем все равно обратилась в суд с иском против компании. Компания иск проиграла.

Использование корпоративных изображений. Неподписание существующих политик может привести к значительным издержкам для компании. В 2017 году ООО «Группа Полипластик» предоставила отраслевому изданию The Chemical Journal фотографии своей промышленной площадки, в частности – труб большого диаметра, для демонстрации размеров которых внутри трубы в полный рост стоял человек. Этим человеком оказалась Чабанец Анастасия Алексеевна, сотрудник компании, которая получала зарплату, находилась в командировке на заводе и в рамках служебного задания, сформулированного и согласованного устно – позировала штатному фотографу компании. Проработав в компании 9 месяцев и уволившись, сотрудница нашла опубликованное фото, подала судебный иск против издания, потребовав компенсацию нанесенного ей морального вреда. Издание привлекло в качестве основного ответчика компанию, а суд определил взыскать компенсацию и опубликовать сообщение о нарушении прав Чабанец А.А. в связи с неправомерным использованием изображения (имя истца публикуется в соответствии с решением суда).

Выход в СМИ. Находясь на конференциях, других отраслевых или массовых мероприятиях, сотрудники известных компаний дают комментарии средствам массовой информации, считая, что они помогают улучшить имидж компании. Но допускают порой ошибки – сообщая ошибочные сведения или сведения, относящиеся к коммерческой тайне компании. Кроме того, компания может считать, что круг данных вопросов относится к компетенции руководства и рядовыми сотрудниками обсуждаться не должен.

Поэтому компания определяет перечень сотрудников, которые уполномочены взаимодействовать со СМИ и делать публичные заявления. Остальные сотрудники могут это делать только после письменного согласования тем и деталей послания. Такое положение восприниматься порой как ограничение свободы, но защищает компанию от репутационных рисков.

Присвоение результатов интеллектуального труда. Являясь сотрудником лаборатории завода и внедряя технологический процесс на одной из установок совместно с другими сотрудниками, специалист копировал на смартфон всю входящую документацию, переписку с поставщиками и транзакции. После успешного пуска установки он произвел поиск вакансий на предприятиях смежного профиля и во время собеседования предложил новой компании свои знания в области модернизации установок определенного типа. После трудоустройства специалист передал новому работодателю всю имеющуюся у него документацию.

Ассоциация делового сотрудничества в области передовых комплексных технологий «АСПЕКТ»

ASSOCIATION
ASPECT
FOR ADVANCED TECHNOLOGIES

Ассоциация «АСПЕКТ» – 20 лет на рынке коммерциализации инновационных технологий.

Сферы основных интересов:
* реализация перспективных наукоемких проектов,
* содействие в организации наукоемких производств,
* развитие международного научно-технического сотрудничества.

Для проведения комплексных исследований и опытно-конструкторских работ «АСПЕКТ» располагает собственной уникальной научно-производственной базой.

К услугам партнеров отлично оснащенный экспертно-аналитический центр «Нанотехнологии в нефте- и газохимии».

В «АСПЕКТЕ» разрабатываются эффективные и экономичные процессы конверсии биомассы в моторные топлива, которые масштабируются до крупных высокорентабельных производств.

«АСПЕКТ» производит уникальные металлокерамические мембраны, обладающие гибкостью и сохраняющие все преимущества неорганических мембран.

Ассоциация «АСПЕКТ» готова к сотрудничеству и партнерству.

www.aspect.ru ■ 7 (495) 434 80 91 ■ 7 (495) 936 88 45 ■ aspect@aspect.ru