Утечка информации, или как организации уберечь себя от мошенничества в сети

Цифровые технологии с каждым днем все больше проникают во все сферы человеческой деятельности. Поэтому перед многими руководителями достаточно острым стоит вопрос хранения и передачи данных в сети, а также обеспечения безопасности от утечки информации в цифровом поле.

Понятийный аппарат

Под утечкой информации подразумевается незаконное получение либо передача защищенных сведений (таких, как персональные данные, коммерческая, государственная тайна и пр.). Утечка информации может быть как умышленной, так и непредумышленной (случайной), что не отменяет вины лица или группы лиц, причастных к этому. Поскольку данное правонарушение является достаточно обобщенным, может касаться наиболее разных видов информации, иметь различные субъективные и объективные стороны, нет точной статьи, регулирующей его.

Но при этом факт утечки является составным элементом иных правонарушений, установленных:

- главой 13 КоАП "Административные правонарушения в области связи и информации";
- главой 28 Уголовного кодекса "Преступления в сфере компьютерной информации".

Из СМИ нам не понаслышке известно о разных примерах утечек, например, в 2020 году в сеть, утекли паспортные данные более 1,1 млн россиян, принимавших участие в голосовании по поправкам к Конституции РФ. А годом ранее общественности была представлена информация об утечке данных пользователей портала "Госуслуги".

Однако законодательство на сегодняшний день никак не регулирует способы защиты от утечки информации, поэтому как крупным организациям, так и представителям МСБ следует самостоятельно изучить наиболее возможные способы защиты от данной угрозы.

Работа с сотрудниками как способ защиты от утечки информации

Насколько банально это может показаться, но, согласно статистическим исследованиям "Лаборатории Касперского", более 60% корпоративных данных попадает не в те руки именно из-за действий самих работников компании без преднамеренного вмешательства. Причем зачастую это происходит именно из-за невнимательности либо халатности сотрудников. Так, наиболее примечательными примерами в данном случае могут быть:

- разговоры с коллегами либо третьими лицами, в ходе которых работник может неосознанно выдать конфиденциальную информацию;
- переход с корпоративной почты либо при веб-серфинге по ссылкам, содержащим "фишинговые" либо иные вредоносные программы;
- фотографии, аудио- и видеозаписи со смартфонов сотрудников, которые впоследствии могут быть взломаны либо же данные переданы третьим лицам по неосторожности;

- получение злоумышленниками доступа к конфиденциальной информации из-за слабого пароля почты либо другого корпоративного веб-инструмента работника.

Многие даже крупные компании зачастую пренебрегают обучением IT-культуре собственных работников, ограничиваясь лишь такими формальностями, как заключение соглашения о неразглашении коммерческой тайны и персональных данных. Руководству в первую очередь следует разъяснить персоналу важность кибер-безопасности, провести соответствующий обучающие тренинги самостоятельно либо с привлечением сторонних специалистов.

Например, в ноябре 2020 года произошла утечка данных программы лояльности "РЖД Бонус". Причиной тому стала халатность сотрудника, который оставил информацию в открытом доступе.

Работодателям следует установить дисциплинарную ответственность за утечку информации в ТК РФ. Напомним, ст. 192 Трудового кодекса установлено три вида дисциплинарных взысканий – замечание, увольнение, выговор, а для государственных служащих еще и предупреждение о неполном должностном соответствии (ч. 1 ст. 57 Федерального закона от 27 июля 2004 г. № 79-ФЗ "О государственной гражданской службе Российской Федерации"). При этом в локальных нормативных актах необходимо не просто указать причину применения наказания "за утечку информации", а максимально детально изъяснить все возможные факторы.

Если говорить о сотрудниках, то также достаточно распространенной причиной утечки данных являются и преднамеренные действия. Чаще всего это происходит из-за отсутствия мотивации у работников, харрасмента со стороны коллег либо руководства, а также неправомерного увольнения. Способы защиты для руководителей в данном случае схожи с описанными выше – поддержание корпоративной культуры, материальная и нематериальная мотивация сотрудников и соблюдение требований трудового законодательства.

Если же правонарушение все-таки было совершено и повлекло негативные последствия, следует обращаться в правоохранительные органы с целью привлечения виновного к административной либо уголовной ответственности.

На сегодняшний день утечка информации участилась из-за введенных в результате пандемии COVID-19 ограничительных мер. Так, многие работодатели, которые перевели сотрудников на дистанционную работу, не обеспечили должным образом сохранность конфиденциальной информации, например, не предоставив им рабочие ПК, а предоставив возможность трудиться на личных.

Как защититься от утечки информации при помощи кибербезопасности

Далеко не всегда утечка данных в организации происходит исключительно из-за действий работников, часто виной этому становится слабая защищенность именно с технической точки зрения. Способов защиты в данном случае множество, следует выделить лишь основные из них:

- использование системы контроля и управления доступом (СКУД). Подразумевается многоуровневая программная и аппаратная система, которая ограничит доступ к конфиденциальной информации третьим лицам;

- ведение корпоративных аккаунтов. Сюда входит и корпоративная почта, и аккаунты для работы в специализированных программах. Крайне важно, чтобы доступ был только у действующих сотрудников, ключи увольняющихся сотрудников необходимо удалять в момент увольнения;
- установка сложных паролей. Наряду с использованием корпоративных аккаунтов необходимо позаботиться об их достаточной защищенности. Наиболее оптимальным вариантом в данном случае является двухфакторная аутентификация (подтверждение входа с помощью СМС, одноразового кода, распознавания лица и т. д.);
- установка антивирусных программ. Современные антивирусы способны бороться с большинством известных способов кражи конфиденциальной информации;
- проведение "стресс-тестов" систем безопасности. Многие крупные компании специально нанимают сотрудников либо проводят конкурсы, в которых предлагают взломать действующую систему безопасности. Делается это для того, чтобы обнаружить возможные причины утечки информации и ликвидировать их;
- обеспечение личного пространства. При выполнении своих обязанностей сотрудники чаще всего контактируют с коллегами, клиентами и другими лицами. Поэтому крайне важно обеспечить безопасность рабочего места. Так, наиболее подвержены риску быть причиной утечки информации сотрудники, работающие в опен-спейсах;
- контроль документации (как электронной, так и бумажной). Сюда входит и работа с действующими документами, то есть использование систем шифрования, защиты от ознакомления третьими лицами, так и с недействительными, то есть использование соответствующих архивов либо удаление ненужных данных.

Вышеописанный перечень является далеко не исчерпывающим, однако при соблюдении этих требований руководителям бизнеса будет значительно проще обезопасить себя от утечки ценной информации.

/ГАРАНТ.РУ/