Адвокатская газета
Орган Федеральной палаты адвокатов РФ

Информационная безопасность в юридических фирмах

Способы защиты от утечки данных

Фокина Дарья
Руководитель направления ЛигалТех, юрист юридической фирмы «Томашевская и партнеры»

20 июня 2025 Legal tech

Адвокатские образования и юридические фирмы, работающие с конфиденциальной информацией, нередко становятся объектом внимания киберпреступников.

Как отмечал в 2016 г. партнер Bird&Bird Саймон Шутер в интервью журналу Legal Insight, злоумышленники оценивают потенциальных жертв по трем ключевым параметрам: возможность доступа к данным, ценность информации и стоимость усилий, необходимых для ее получения.

Адвокатские образования и юрфирмы обрабатывают значительные объемы информации, включая как общедоступные данные, так и сведения ограниченного доступа. Ярким примером уязвимости можно назвать случай с Mossack Fonseca в апреле 2016 г., когда в результате масштабной кибератаки в сеть попали более 11,5 млн документов, раскрывших детали офшорных схем. Утечки конфиденциальной информации влекут не только финансовые потери, но и серьезные репутационные риски, в связи с чем обеспечение информационной безопасности становится для юридических фирм стратегическим приоритетом.

Исследование, проведенное CSI и Legal Insight в 2016 г., показало, что 48% респондентов считают безопасность ИТ-инфраструктуры и защиту информации первоочередной задачей, а 51% отметили, что вопросами кибербезопасности в компании занимается штатный ИТ-специалист.

По данным количественного анонимного опроса 2025 г., проведенного фирмой «Томашевская и партнеры» среди юридических фирм (далее – опрос), более чем у 62% из них отсутствует ответственное за информационную безопасность лицо. Поэтому первым шагом к обеспечению информбезопасности является назначение соответствующего специалиста. Также опрос выявил три наиболее популярные меры предотвращения утечек в юрфирмах:

- управление доступом (87%);
- обучение сотрудников (70%);

- политика безопасности данных (50%).

Наименее распространенными, но не менее важными мерами являются аудит информбезопасности для выявления слабых мест в системе защиты и внедрение DLP-систем, анализирующих всю входящую и исходящую информацию для отслеживания сомнительных операций и выявления утечек.

Защита от физических утечек данных также имеет значение. Основным фактором риска является человеческий фактор. Эксперты отмечают, что данные нередко считывают, фотографируя экран компьютера, планшета или смартфона. Для предотвращения таких утечек рекомендуется использовать специальные пленки, делающие монитор невидимым для камер.

Александр Свердлов в книге «Защищая юридическую фирму от хакерских атак и инсайдерских угроз» привел 14 элементов системы информационной безопасности в фирме, большую часть которых респонденты в опросе не обозначили. Указанные элементы во многом применимы также для адвокатов и адвокатских образований.

Первый элемент: управление паролями и доступом.

Многие компании заставляют сотрудников регулярно менять сложные пароли, полагая, что это повышает безопасность. Однако зачастую возникает обратный эффект – сложные пароли трудно запомнить, поэтому люди записывают их (рискуя потерять или раскрыть доступ) либо упрощают, сводя на нет всю защиту от киберугроз. Парадоксально, но пароль, который кажется сложным, например «P@ssword123» (с заглавной буквой, цифрами и состоящий более чем из 10 символов), вполне может считаться безопасным в подавляющем большинстве организаций: по статистике, его используют порядка 5% сотрудников. Это значит, что злоумышленник может угадать пароли от 5% почтовых аккаунтов!

Эффективным решением является использование корпоративного менеджера паролей. Это система, которая автоматически генерирует сложные и уникальные пароли, хранит их в защищенном месте и позволяет ИТ-администраторам получать доступ к ресурсам только через эту систему. Важно, чтобы все активы компании были учтены в менеджере паролей, а сотрудники не имели возможности самостоятельно выбирать их. Такая политика обеспечивает высокий уровень безопасности и снижает риски утечки данных. Разграничение прав доступа, техническое ограничение обработки информации и использование двухфакторной аутентификации значительно повышают уровень защиты.

Элемент второй: удаленный доступ.

Удаленный доступ к корпоративным ресурсам всегда сопряжен с риском. Чтобы его минимизировать, необходимо обеспечить шифрование всех соединений и их осуществление по защищенному туннелю; защиту ноутбуков, компьютеров и

мобильных устройств брандмауэром, их регулярное обновление и отказ от нежелательных подключений; дополнительную аутентификацию.

В 2020 г. КА «Юков и Партнеры» подчеркивала важность технических инструментов: защищенного удаленного доступа, шифрования трафика и каналов связи, принудительной блокировки гаджетов, возможности дистанционного удаления данных, проверки электронной почты на конфиденциальную информацию и запрета ее отправки. В АБ «Коблев и партнеры» отмечали, что количество атак на юридические фирмы будет расти, поскольку они являются хранителями информации о финансах клиентов, сделках, коммерческой тайне и доказательствах.

Третий элемент: политика и процедуры.

Для эффективной защиты от киберугроз представляется необходимым разработать четкие правила – политику и процедуры. Важно, чтобы эти правила были адаптированы к специфике компании и учитывали особенности ее деятельности.
Основой для формирования этих правил обычно служат:

- политика конфиденциальности: определяет, как обрабатываются и защищаются конфиденциальные данные;
- политика допустимого использования ИТ-активов: устанавливает правила использования компьютеров, сетей и других ИТ-ресурсов;
- кодекс поведения: определяет этические нормы и принципы для сотрудников в сфере информационной безопасности;
- политика защиты сети: описывает меры по защите корпоративной сети от внешних и внутренних угроз;
- политика реагирования на инциденты: определяет порядок действий в случае обнаружения кибератаки или нарушения безопасности;
- политика управления уязвимостями: описывает процесс выявления, оценки и устранения уязвимостей в ИТ-системах;
- политика защиты конечных точек: устанавливает правила защиты компьютеров, ноутбуков и мобильных устройств сотрудников;
- политика усиления безопасности: описывает меры по повышению общей безопасности ИТ-инфраструктуры;
- политика управления активами: определяет порядок учета и контроля ИТ-активов компании;
- смягчение последствий кибератак.

Чтобы понять, насколько компания уязвима к кибератакам, стоит провести моделирование угроз. Это процесс, который помогает выявить слабые места в системе безопасности. Моделирование угроз помогает обнаружить не только технические уязвимости в ПО и оборудовании, но и недостатки в бизнес-процессах, процедурах, обучении персонала и даже в физической безопасности ИТ-инфраструктуры. Суть анализа в том, чтобы выявить все возможные способы, которыми злоумышленник (или даже случайная ошибка) может навредить компании. Благодаря этому процессу можно

определить приоритетные направления для усиления защиты и эффективно распределить ресурсы.

Четвертый элемент: осведомленность о безопасности.

Обучение сотрудников – ключевой элемент защиты от киберугроз. Важно, чтобы тренинги были регулярными, понятными и доступными, а не представляли собой перечень технических терминов.

Эффективным подходом является использование практических примеров. К примеру, ИТ-отдел может разослать тестовое фишинговое письмо, имитирующее реальную угрозу. Если сотрудник переходит по ссылке, система автоматически уведомляет ИТ-департамент. После этого сотруднику отправляется сообщение о том, что это был тест и ему необходимо повторно пройти обучение по информационной безопасности. Такой подход позволяет продемонстрировать риски и закрепить полученные знания на практике. Это не просто обучение, а проверка на бдительность, которая помогает сотрудникам научиться распознавать реальные угрозы и предотвращать их.

Пятый: облачная инфраструктура безопасности.

В настоящее время большинство юридических компаний активно используют облачные сервисы для хранения данных и работы приложений, и это логично: ни одна организация, даже самая крупная, не сможет сравниться с уровнем инвестиций в безопасность компаний-гигантов. В связи с этим использование облачных провайдеров становится для многих юрфирм единственным реалистичным способом обеспечения надежной защиты от киберугроз. Эффект масштаба позволяет им эффективно противостоять огромному количеству атак, в то время как отдельная компания зачастую не обладает достаточными ресурсами.

Ключевым аспектом защиты облачных сервисов является защита административного доступа. Нельзя полагаться только на имя пользователя и пароль – необходимо внедрить дополнительные уровни защиты и строго контролировать, кто и когда получает доступ к данным.

Шестой: защита ИТ-инфраструктуры внутри юридической фирмы.

Усиление безопасности необходимо применять ко всем устройствам в сети, а не только к серверам и компьютерам сотрудников. Зачастую упускаются из виду такие, казалось бы, «безобидные» устройства, как принтеры.

Большинство ИТ-администраторов подключают принтеры к сети, используя учетные записи, чаще всего из корпоративного каталога Active Directory. При этом даже если администратор вошел на принтер со своей учетной записью и затем настроил его с более ограниченными правами доступа, на устройстве может сохраниться «отпечаток пальца», или «хеш», этой учетной записи. Если он останется действительным,

злоумышленник может получить доступ к нему и соответственно – полный контроль над ИТ-инфраструктурой компании.

Седьмой элемент: управление уязвимостями и исправлениями.

ИТ-системы – это сложная сеть взаимосвязанных компонентов. Исправление одной уязвимости может непреднамеренно нарушить работу критически важных бизнес-процессов. В связи с этим управление уязвимостями и установка обновлений – процесс, требующий системного подхода. Важно не только вовремя выявлять и устранять уязвимости, но и мотивировать ИТ-команду, контролировать эффективность ее работы и постоянно совершенствовать процесс.

Ключевые показатели эффективности (KPI) представляется целесообразным оценивать индивидуальную работу ответственных сотрудников (своевременное сканирование, уведомление и исправление уязвимостей) и общую динамику – например, уменьшение количества необработанных уязвимостей в каждой категории (критические, высокие, средние и низкие) с течением времени. Такой подход позволяет повысить уровень безопасности и минимизировать риски для компании.

Восьмой: тестирование на проникновение.

Тестирование на проникновение (или «атака-симуляция») – это способ проверить безопасность компании, смоделировав действия реального злоумышленника. Преимущество такого подхода в том, что тестировщики используют те же инструменты и тактики, что и киберпреступники, и нередко успешно проникают в систему. Полученный отчет позволяет выявить и устранить уязвимости в защите. При этом важно учитывать, что тестирование на проникновение – это не исчерпывающий анализ безопасности.

Тестировщик, как правило, останавливается на первом найденном способе проникновения в систему, не тратя время на поиск других уязвимостей. Он сообщает о найденной точке входа, поскольку она позволила ему достичь цели – получить доступ к сети компании. Это означает, что в системе могут существовать и другие – не выявленные – уязвимости, которые могут быть использованы в недобросовестных целях.

Девятый: безопасность конечных точек.

Несмотря на то, что администратор может чувствовать себя «хозяином» на своем компьютере, он должен соблюдать те же строгие правила информационной безопасности, что и любой другой сотрудник компании.

Для повышения безопасности рекомендуется создать два профиля пользователя для каждого администратора:

- обычный пользователь: для повседневной работы (чтение электронной почты, совместная работа и редактирование документов);

- административный пользователь (для выполнения задач, требующих повышенных привилегий).

Администратору целесообразно использовать функцию «Выполнить как» (Run as), или sudo, чтобы повысить свои привилегии только тогда, когда это необходимо для выполнения административных задач. Это помогает ограничить потенциальный ущерб в случае компрометации учетной записи.

Десятый элемент: мониторинг безопасности.

Для обеспечения безопасности необходимо регулярно контролировать активность всей ИТ-инфраструктуры компании. Это включает мониторинг сетевых устройств (компьютеры, серверы и маршрутизаторы), а также анализ интернет-трафика. Регулярный мониторинг позволяет своевременно выявлять и реагировать на любые подозрительные действия или потенциальные угрозы.

Одиннадцатый: предотвращение, выявление и ответ на инциденты.

Предотвращение инцидентов информационной безопасности включает ряд мер – в частности, запрет самостоятельной установки ПО сотрудниками, обязательную двухфакторную аутентификацию для удаленного доступа к корпоративным ресурсам и шифрование всех устройств – от ноутбуков до мобильных телефонов.

Внедрение системы мониторинга безопасности может привести к резкому увеличению количества оповещений, в том числе о реальных инцидентах. Многие компании удивляет объем активности, которую они начинают фиксировать в сети, когда получают полную картину происходящего.

Задача специалистов по информационной безопасности – оперативно выявлять взломы – как внутренние, так и внешние – и изолировать злоумышленников до того, как они смогут нанести компании серьезный ущерб.

Двенадцатый элемент: безопасность электронной почты и коммуникации.

Двухфакторная аутентификация значительно повышает безопасность, но не гарантирует полную защиту электронной почты. Для конфиденциальности важной переписки рекомендуется применять шифрование, чтобы доступ к сообщениям имели только авторизованные получатели. Кроме того, стоит использовать защищенные мессенджеры вместо общедоступных, чтобы обеспечить конфиденциальность переписки.

Тринадцатый: безопасность веб-сервисов.

Существует множество способов, которыми злоумышленники могут атаковать веб-сайт, поэтому важно уделить внимание защите от всех возможных уязвимостей.

Начать можно с использования надежных паролей, сгенерированных менеджером паролей, для всех учетных записей, где требуется пароль. Это касается удаленного доступа к веб-серверу, базам данных, панелям управления сайтом, учетных записей пользователей, которые могут редактировать контент, и, что особенно важно, – системы резервного копирования. Защита последней важна не менее чем защита веб-сервера, поскольку хакеры зачастую выбирают самый легкий путь – взлом резервной копии, чтобы получить доступ к данным.

Таким образом, усиление информационной безопасности – не просто необходимость, но и разумная предосторожность.