УДК 34.096

В.С. Якимёнок
(Белорусский государственный экономический университет)

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ ОХРАНЫ КОММЕРЧЕСКОЙ ТАЙНЫ

В свете быстрого развития цифровых технологий и распространения информационных угроз становится все более важным обеспечение охраны коммерческой тайны. В настоящей статье проанализированы актуальные методы и подходы к защите коммерческой тайны с использованием информационных технологий, включая применение AI-моделей и систем класса DLP (Data Leakage Prevention). Кроме того, предлагаются рекомендации по оптимизации использования информационных технологий для обеспечения безопасности коммерческой тайны.

В настоящее время наблюдаются тенденции к цифровизации экономического пространства, что приводит к возрастанию количества неправомерного распространения информации, составляющей коммерческую тайну. В современном мире информационных технологий охрана коммерческой тайны становится все сложнее из-за возрастающей угрозы киберпреступности и несанкционированного доступа к данным. Существующие на сегодняшний день меры не способны в полной мере гарантировать безопасность коммерческой тайны от неправомерных посягательств. Учитывая тот факт, что информация сегодня – это товар, имеющий определенную стоимость, необходима разработка принципиально новых мер охраны коммерческой тайны, закрепленных на законодательном уровне.

Случаи коммерческого шпионажа известны белорусскому законодательству уже давно, однако не наблюдается тенденций к снижению количества преступлений по данному составу. Как сказал адвокат Владимир Парахневич в своем интервью pravo.by: «Чтобы информация охранялась с точки зрения закона и можно было привлечь за ее раскрытие к ответственности, должна быть обеспечена не только «бумажная», но и реальная защита этих сведений. Даже если база данных клиентов представляет коммерческую ценность, но собственник не принял надлежащих мер по ее защите, требовать наказания для виновных бесполезно» [1].

Актуальность данного исследования вызвана необходимостью выявления более эффективных способов охраны коммерческой тайны, которые помогут организациям укрепить свою позицию на рынке и сохранить конкурентное преимущество в условиях современного информационного общества.

В своем интервью начальник 6-го управления (по Брестской области) Главного управления по борьбе с организованной преступностью и коррупцией Александр Лаврукович рассказал о практике возбуждения уголовных дел по составу коммерческого шпионажа (ст. 254 Уголовного кодекса Республики Беларусь): «Такие ситуации имели место и в Минске, и в областных центрах. Но принимались решения об отказе в возбуждении уголовного дела, поскольку на предприятиях не соблюдался режим коммерческой тайны. Этот вопрос лежит в плоскости правовой неграмотности» [1].

Из вышесказанного можно сделать вывод, что прежде чем говорить о дополнительных и новых способах охраны коммерческой тайны, владельцам коммерческой тайны необходимо в первую очередь установить надлежащим образом правовой режим коммерческой тайны, который включает закрытый перечень мер, определенный законодательством Республики Беларусь. И после того, как правовой режим «формально» будет установлен, позаботиться о реальной охране коммерческой тайны. Поскольку владельцы коммерческой тайны вспоминают о необходимости соблюдения режима после понесения финансовых потерь, а успех в привлечении к ответственности лиц, посягнувших на коммерческую тайну, зависит во многом от того, какие меры были предприняты владельцами до этого.

В зависимости от способа защиты информации, составляющей коммерческую тайну, существуют две процедуры защиты информации: процедуры ограничения доступа (AR – access restriction) и процедуры обращения с информацией (HP – handling procedures). Первая процедура включает меры, фактически ограничивающие доступ к сведениям, а вторая – юридические [2].

AR охватывает меры физического ограничения доступа в отдельные помещения, использования конфиденциальных документов, их копирования, что в принципе исключает возможность завладения информацией. Использование информационных технологий относится к процедурам ограничения доступа.

Интерес для нас представляет опыт использования информационных технологий в сфере охраны коммерческой тайны в ПАО Сбербанк, так как эксперты кибербезопасности банка учитывают актуальные тенденции как в информационном, так и технологическом пространстве. Специалистами Сбербанка были реализованы инициативы, связанные с применением AI моделей для автоматического поиска и выявления информации ограниченного доступа, а также её защитой от утечек на основе систем класса DLP (Data Leakage Prevention).

Специалисты Сбербанка отметили, что проблема, с которой сталкиваются организации в построении режима коммерческой тайны, заключается в определении сведений, которые включается в Перечень сведений, составляющих коммерческую тайну организации, и будут подлежать охране. Незнание того, какая информация действительно имеет ценность, еще более затрудняет ее выявление на отправляемых письмах, сообщениях, в файловых ресурсах и на съемных носителях [3].

В Сбербанке для решения названной проблемы была разработана AI модель, которая может работать в качестве ядра сервиса выявления сведений, составляющих коммерческую тайну в составе различных бизнес-систем и систем безопасности, в том числе систем защиты от утечек информации. Кроме того, AI модель совместно с агентом используется в качестве ассистента, помогающего работнику принять верное решение об отнесении информации, содержащейся в документе, к сведениям, составляющим коммерческую тайну.

В функционал AI модели входит:

1. Автоматическое выявление сведений, составляющих коммерческую тайну в файлах, сохраняемых в файловых хранилищах или передаваемых по каналам связи;

2. Автоматическая маркировка документов грифом «Коммерческая тайна» и их защита от несанкционированного доступа;

3. Учет и контроль распространения документа, содержащего сведения, составляющие коммерческую тайну, и контроль соблюдения работниками требований режима коммерческой тайны;

4. Контроль и предотвращение нарушений при хранении и передаче сведений, составляющих коммерческую тайну [3].

Для того, чтобы AI модель заработала, необходимо, в первую очередь, обучить ее обработке документов с целью выявления содержащих сведения, составляющие коммерческую тайну. Для этого специалисты Сбербанка разработали методику разметки документов. Разметка выполняется, как правило, аналитиками (исследователями) данных в рамках подготовки данных для обучения AI модели – нужно «сообщить» ей, какие именно элементы текста точно содержат сведения, составляющие коммерческую тайну, а какие точно не содержат.

Данный подход не лишен недостатков и нуждается в дальнейшей доработке, а применение AI модели требует значительных трудозатрат. Внедрение подобной системы не означает, что работники организации смогут расслабиться и возложить на нее ответственность за сохранность режима коммерческой тайны, так как необходимо регулярно дообучать и валидировать AI модель, консультировать работников, подготавливать и утверждать новые редакции документов режима коммерческой тайны.

Однако несмотря на некоторые недостатки и трудности во внедрении вышеописанной модели, по мнению специалистов Сбербанка, AI модель способна значительно повысить эффективность защиты режима коммерческой тайны, кратно снизить трудозатраты на его поддержание в актуальном состоянии, значительно снизить субъективизм и человеческий фактор в процессе сбора информации, составляющей коммерческую тайну, повысить прозрачность процесса сбора информации и обеспечить более высокий уровень её защищенности.

Возникает вопрос, как соответствующие меры по охране коммерческой тайне закрепить на законодательном уровне.

В ч. 2 ст. 8 Закона Республики Беларусь «О коммерческой тайне» от 05.01.2013 № 16-З (далее – Закон) закреплен перечень мер, составляющих режим коммерческой тайны. В соответствии с ч. 3 ст. 8 Закона наряду с мерами, указанными в части второй настоящей статьи, владелец коммерческой тайны вправе применять не запрещенные законодательством технические средства и методы защиты информации, а также другие меры, не противоречащие законодательству [4].

Подход законодателя заключается в определении закрытого перечня мер, необходимых для установления режима коммерческой тайны и в предоставлении владельцам коммерческой тайны возможности использовать

иные технические средства и методы защиты информации, не противоречащие законодательству.

Данный подход нам видится целесообразным ввиду постоянного изменения информационных технологий. Использование AI модели может быть не актуальным в будущем и субъекты хозяйствования столкнутся с тем, что существующие программные продукты, средства защиты и ИТ-системы не будут соответствовать современным тенденциям.

Принимая во внимание подход законодателя, мы предлагаем организациям, планирующим внедрить AI модель, внести в уже существующие локальные нормативные правовые акты (далее – ЛНПА) – положения о коммерческой тайне или инструкциии по работе со сведениями, составляющими коммерческую тайну, или издать новые ЛНП, в которых будут закреплены правоотношения, возникающие в ходе внедрения AI модели, а именно: правила обращения со сведениями, составляющими коммерческую тайну; перечень должностей работников, ответственных за разметку документов и ответственных за актуализацию перечня сведений, составляющих коммерческую тайну; технические меры по обеспечению безопасности коммерческой тайны, организационные меры по охране коммерческой тайны (обучение сотрудников в области информационной безопасности).

Субъектам хозяйствования необходимо помнить, что информационные отношения в сфере охраны коммерческой тайны требуют комплексного подхода и постоянного мониторинга, организации должны придерживаться строгих политик и процедур, регулярного обучения своих сотрудников и использования современных технических средств защиты. Только таким образом можно обеспечить надежную охрану коммерческой тайны и сохранить конкурентное преимущество на рынке.

Таким образом, в настоящее время ставится под вопрос об эффективности существующих способов охраны коммерческой тайны, поскольку появляются новые виды киберпреступности. Специалисты Сбербанка предлагают существующую проблему решить с помощью разработанной ими AI модели, которая способна снизить субъективизм и человеческий фактор в процессе сбора информации, составляющей коммерческую тайну.

С учетом положений действующего законодательства нам представляется целесообразным закрепить правоотношения, возникающие при внедрении AI моделей, с помощью ЛНПА, определяющего меры по охране коммерческой тайны в организации.

Список использованной литературы:

1. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2018/january/27272/– Дата доступа: 09.11.2023.

2. Лясович, Д. М. Оптимизация режима коммерческой тайны для охраны объектов интеллектуальной собственности в сфере информационных технологий / Д. М. Лясович // Охрана и защита прав и законных интересов в современном праве: сборник статей по

результатам международной научно-практической конференции. – Симферополь, 2022. – С. 338–349.

3. Гарбузов, Г. Использование технологий искусственного интеллекта в построении режима коммерческой тайны на предприятии / Г. Гарбузов, А. Теренин, Н. Бабак // Кибрарий [Электронный ресурс]. – 2022. – Режим доступа: http://www.sberbank.ru/ru/person/kibrary/articles/tehnologiy_iskusstvennogo_intellekta_v_postroenii_rezhima_kommercheskoy_tayny. – Дата доступа: 09.11.2023.

4. О коммерческой тайне [Электронный ресурс]: Закон Респ. Беларусь, 5 января 2013 г., № 16-З : в ред. Закона Респ. Беларусь от 17.07.2018 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Дата доступа: 09.11.2023.