Судебная практика в информационной безопасности

Каждый специалист знает, что одной из главных проблем в информационной безопасности является обоснование необходимости любых защитных мероприятий. Как бы красочно вы ни описывали возможные угрозы, уязвимости, нарушителей и виды атак, руководство всегда будет интересовать — случалось ли уже что-то подобное в других организациях? Здесь на помощь специалисту приходит обзор судебной практики. Казалось бы, что сложного — выбрать несколько дел по нужной тематике и предоставить их начальству. Однако не все так просто.

КСЕНИЯ ШУДРОВА,
руководитель Красноярского отделения RISC, блогер

Все течет, все меняется

Законодательство в сфере информационной безопасности изменяется очень быстро, поэтому иметь подборку «лучших практик на все времена» не получится. К слову, мне приходилось писать статью на подобную тему пять лет назад, и приведенные в ней примеры уже никуда не годятся. Естественно, никто не заставляет вас искать судебные решения за текущий месяц — практика одно-двухлетней давности вполне подойдет. Если, конечно, за это время не произошло кардинальных изменений. Например, 1 июля были повышены штрафы в области персональных данных[1].

Ключевые статьи

Для эффективного поиска судебных решений полезно знать основные статьи законодательства, касающиеся нарушений в области информационной безопасности. В качестве шпаргалки мною был составлен следующий список (что-то вам не пригодится, ну а где-то его придется дополнить):

1. Уголовный кодекс Российской Федерации
   - Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.
   - Статья 159.6. Мошенничество в сфере компьютерной информации.
   - Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.
   - Статья 185.6. Неправомерное использование инсайдерской информации.
   - Статья 272. Неправомерный доступ к компьютерной информации.
   - Статья 273. Создание, использование и распространение вредоносных компьютерных программ.
   - Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
   - Статья 283. Разглашение государственной тайны.
   - Статья 283.1. Незаконное получение сведений, составляющих государственную тайну.
   - Статья 284. Утрата документов, содержащих государственную тайну.
   - Статья 310. Разглашение данных предварительного расследования.
2. Гражданский кодекс Российской Федерации
   - Часть 2. Статья 727. Конфиденциальность полученной сторонами информации.
   - Часть 2. Статья 771. Конфиденциальность сведений, составляющих предмет договора.
3. Кодекс Российской Федерации об административных правонарушениях
   - Статья 5.53. Незаконные действия по получению и (или) распространению ин-

Законодательство в сфере информационной безопасности изменяется очень быстро, поэтому иметь подборку «лучших практик на все времена» не получится

[1] Изменилась статья 13.11 КоАП.

Поиск решений на этих ресурсах удобнее всего осуществлять по номеру статьи и временному периоду

формации, составляющей кредитную историю.

- Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных.
- Статья 13.12. Нарушение правил защиты информации.
- Статья 13.13. Незаконная деятельность в области защиты информации.
- Статья 13.27.1. Нарушение требования о размещении на территории Российской Федерации технических средств информационных систем.
- Статья 13.33. Нарушение обязанностей, предусмотренных законодательством Российской Федерации в области электронной подписи.
- Статья 13.34. Неисполнение оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети Интернет, обязанности по ограничению или возобновлению доступа к информации, доступ к которой должен быть ограничен или возобновлен на основании сведений, полученных от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций.
- Статья 14.30. Нарушение установленного порядка сбора, хранения, защиты и обработки сведений, составляющих кредитную историю.
- Статья 15.21. Неправомерное использование инсайдерской информации.
- Статья 17.13. Разглашение сведений о мерах безопасности.
- Статья 20.23. Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации.
- Статья 20.24. Незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности.

Поиски иголки

Судебные решения можно найти на специализированных сайтах и порталах[2]. Поиск решений на этих ресурсах удобнее всего осуществлять по номеру статьи и временному периоду. По некоторым популярным статьям можно найти готовые подборки[3]. По персональным данным подборка судебных решений есть на портале Роскомнадзора[4]. Также интересные судебные решения публикуют на тематических отраслевых сайтах, например, по банковскому сектору[5]. Не следует забывать и о новостных агрегаторах по информационной безопасности. Основная трудность поиска подходящих судебных решений состоит в том, что судебная практика по информационной безопасности еще довольно скромная и разрозненная, поэтому делать выводы и обобщения очень сложно.

Отрицательный результат — тоже результат

Не нужно стремиться найти только выигранные дела. Много полезной информации можно почерпнуть из неудачного опыта других предприятий. Например, в судебном решении, касающемся уральского банка[6], были отмечены на-

[2] Например, http://sudact.ru, https://rospravosudie.com
[3] Например, здесь: http://sudact.ru/practice/personalnye-dannye
[4] https://pd.rkn.gov.ru/law/p139
[5] Судебная практика по ДБО: https://www.vedomosti.ru/finance/articles/2017/03/28/682955-ukradennie-internet-dengi
[6] https://rospravosudie.com

рушения, выявленные Роскомнадзором в ходе проверки:

- Отсутствуют документы, подтверждающие ознакомление и обучение сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства и документами, определяющими политику оператора в отношении обработки персональных данных, а также локальными актами по вопросам обработки персональных данных без использования средств автоматизации.
- Не определены процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных.
- Не обеспечено наличие документов, определяющих место хранения персональных данных и перечень лиц, имеющих к ним доступ.
- Согласие клиентов на обработку не содержит перечня персональных данных, фактически обрабатываемых оператором.
- Безосновательно обрабатываются данные близких родственников работников.
- Анкета соискателя содержит пункт, требующий указывать сведения о судимости, причем не только субъекта персональных данных, но и его родственников.
- Не определен порядок уничтожения персональных данных, а также материальных носителей информации, их содержащих.

Таким образом, лишь в этом судебном решении можно выделить семь типичных ошибок операторов персональных данных. Проанализировав еще несколько решений на данную тему, вы легко определите примерный перечень необходимых мероприятий.

Но не только в области персональных данных полезно изучать чужой негативный опыт. В сфере защиты коммерческой тайны очень важно обращать внимание на дела, в которых режим коммерческой тайны был признан организованным некорректно. В частности, в одном из судебных решений в качестве аргумента были указаны разнящиеся определения «коммерческая тайна» в должностной инструкции и стандарте компании[7], из-за чего организация не смогла отстоять свои интересы в суде. Это еще раз доказывает: мелочей в информационной безопасности не бывает.

Тебя посодют, а ты не воруй!

Судебные решения могут пригодиться не только для убеждения руководства, но и для устрашения сотрудников. На долгие годы моим самым любимым делом в области информационной безопасности остается суд над женщиной, которая пробралась в пекарню, где раньше работала, чтобы украсть рецепт хлеба для своего нового бизнеса. Работодатель сполна получил компенсацию, поскольку все было организовано правильно.

Важность соблюдения формальных правил при организации режима коммерческой тайны[8] подтверждается и последними судебными решениями. Так, Коломенским городским судом было рассмотрено ходатайство о восстановлении на работу сотрудника завода, нарушившего режим коммерческой тайны. Допуск персонала осуществлялся исключительно в соответствии с регламентами завода по работе со служебной и коммерческой тайной. Дополнительно были утверждены «Положение о коммерческой тайне», устанавливающее режим коммерческой тайны, и «Перечень сведений, отнесенных к категории “коммерческая тайна”». Все документы на момент возникновения спора между

[7] https://rospravosudie.com
[8] http://sudact.ru

Не нужно стремиться найти только выигранные дела. Много полезной информации можно почерпнуть из неудачного опыта других предприятий

сотрудником и работодателем были действующими. С вышеуказанными локальными нормативно-правовыми актами истец ознакомлен, что было подтверждено «Списком для ознакомления с локальными нормативными актами».

Сотруднику был ограничен доступ к служебной и коммерческой тайне, однако на его рабочем месте были найдены чертежи с грифом «КТ». Факт дисциплинарного проступка был подтвержден актом внутренней проверки и материалами фотосъемки. Работник не смог представить доказательства, что изъятые чертежи находились у него в связи с полученным производственным заданием.

С учетом фактических обстоятельств дела суд пришел к выводу о законности увольнения, поскольку на работника ранее было наложено дисциплинарное взыскание в виде выговора за неоднократные действия по неправомерному копированию конфиденциальной информации на материальный носитель, а также вынос чертежей за территорию завода и передачу их представителям сторонних организаций. Таким образом, уже имея дисциплинарное взыскание, работник не сделал должного вывода и не исполнил доведенное до его сведения распоряжение о запрете доступа к коммерческой тайне, за что и был справедливо уволен.

Клиент всегда прав. Или не всегда?

Судебные решения нужны для понимания вероятных проблем, которые могут возникнуть при взаимодействии с клиентами. Отдельные случаи иллюстрируют негативный для организации ход развития событий. Начальник отдела по работе с проблемными активами отделения крупного банка был подвергнут административному наказанию в виде штрафа в размере 500 рублей за то, что его подчиненный выяснял местонахождение задолжника у его работодателя. Суд посчитал такие действия распространением информациио наличии задолженности по кредитным обязательствам перед банком, а также осуществлением недопустимого сбора информации[9].

К счастью, суд не всегда встает на сторону клиента, поэтому полезно знать, когда предприятие может рассчитывать на выигрыш дела. К примеру, в екатеринбургском банке[10] клиенткой был заключен договор потребительского кредита. Впоследствии банк поменял форму собственности с закрытого акционерного общества на акционерное общество. Данное обстоятельство привело к тому, что клиентка стала отказываться платить по кредиту, мотивируя свои действия тем, что заключала она договор с ЗАО. Суд признал, что наличие кредитной карты и осуществление по ней операций доказывают наличие фактических договорных отношений, и иск банка о взыскании задолженности удовлетворил.

Иногда предприятию в судебных разбирательствах помогает время. Так, клиентка уже новосибирского отделения другого банка[11] обратилась в прокуратуру по вопросу нарушения ее прав на защиту персональных данных. Из материалов проверки следует, что ее персональные данные были сообщены банку заемщиком в качестве контактного лица. Суд установил, что имеет место нарушение установленного порядка обработки персональных данных, в том числе их раскрытие неопределенному кругу лиц без согласия субъекта персональных данных. Данное правонарушение не является длящимся, и временем его совершения считается дата принятия соответствующих данных от заемщика. Согласно ч. 1 ст. 4.5 КоАП РФ срок давности привлечения к административной ответственности за совершение правонарушения, предусмотренного ст. 13.11 КоАП РФ, составляет три месяца. А поскольку срок давности истек, то наказания не последовало.

Тема судебной практики настолько обширна, что рассмотреть все нюансы в одной статье просто невозможно. При определенной сноровке удается находить решения на любой случай и успешно применять полученную информацию на совещаниях с руководством, а также при обучении сотрудников. Для достижения лучшего результата следует обращать внимание не только на выигранные организациями дела, кроме того, предпочтительно выбирать примеры, имеющие давность не более двух лет. И помните: хороший специалист по ИБ всегда найдет в море судебной практики то, что поддержит его позицию.

[9] https://rospravosudie.com

[10] https://rospravosudie.com
[11] https://rospravosudie.com