sst-03.qxd 01.08.2007 22:42 Page 68

Анатолий ДАВЫДОВ,
начальник Департамента безопасности, группа компаний «РЕСО»

ПРОБЛЕМЫ СОХРАНЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ В УДАЛЕННОМ ФИЛИАЛЕ

В головном офисе утечку информации можно пресечь довольно быстро и эффективно. В удаленных филиалах ситуация усложняется.

Вопросы сохранения коммерческой тайны в каждой страховой компании решаются по-разному. Связано это с тем, что, во-первых, у всех свое видение проблемы, во-вторых, у каждого свои возможности.

У страхового общества «РЕСО-Гарантия» – 82 филиала, практически во всех субъектах федерации. Почти в половине филиалов есть службы безопасности, одной из задач которых является обеспечение сохранения коммерческой тайны.

Наличие или отсутствие службы безопасности в филиале во многом зависит от общей обстановки в регионе. Есть сложные области, которые можно отнести к проблемным. Есть, наоборот, спокойные. Поэтому служба безопасности вводится избирательно. При необходимости – создаем на местах, нет необходимости – время от времени отправляем туда сотрудников.

sst-03.qxd 01.08.2007 22:42 Page 69

За разглашение коммерческой тайны не судят

Отмечу, что не только в страховании, но и в других сферах бизнеса, говорить о привлечении к уголовной ответственности за разглашение коммерческой тайны очень сложно. Сотрудник несет наказание за конкретный состав преступления. Например, если в результате его действий похищены деньги – рассматривается дело о хищении. Если производились незаконные действия, искажающие конкретные даты, формулировки, суммы – это служебный подлог.

Случаев, когда человека судили бы за нарушение информационной безопасности, я назвать не могу. Поэтому, прежде всего, речь пойдет о мерах административного характера.

Люди и машины

Понятие общей информационной безопасности делится на две составляющие:

• техническое оснащение

• организационные и контрольные мероприятия.

В «РЕСО-Гарантия» техническими вопросами занимается управление информационной технологии. В ряду задач, которые стоят перед этим управлением, назову следующие:

• отсекать незарегистрированных пользователей

• оповещать о проникновении в систему

• не допускать скачивание информации на какой-либо носитель.

Решение перечисленных задач достигается как с помощью программного обеспечения, так и с помощью специальных устройств.

Как и в любой уважающей себя компании, у нас существуют уровни доступа – разные для всех сотрудников. Кроме того, в информационных системах мы работаем в режиме online. То есть практически с каждым из филиалов установлена прямая связь, и все изменения в базе можно отслеживать, не выезжая в командировки. Что касается разработки свода правил по соблюдению коммерческой тайны и контроля за их выполнением, они возложены на службу безопасности.

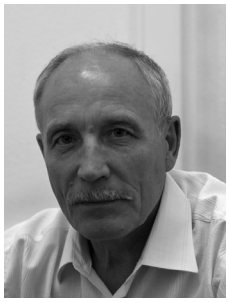
sst-03.qxd 01.08.2007 22:42 Page 70

Так как работа с базой осуществляется в режиме online, важную роль в обеспечении информационной безопасности играет надежность наших системных администраторов. Они подбираются директорами филиалов, но прежде чем вступить в должность, должны пройти проверку в службе безопасности. Проверяются их профессиональные знания и предыдущий опыт работы. Например, встречаются ситуации, когда администратор работает по совместительству в нескольких компаниях. Не исключено, что среди них есть и страховые. Тогда появляется возможность воспользоваться служебным положением в корыстных целях, что нельзя не упускать из вида.

Защита информации при увольнении сотрудников

Если из филиала уходит сотрудник, перед увольнением с ним проводят собеседование и напоминают положение о коммерческой тайне. После увольнения необходимо

Дополнение по теме



Владимир ВОЛКОВ,
старший специалист службы экономической безопасности, ООО «АльфаСтрахование»

СИСТЕМА БЕЗОПАСНОСТИ В ФИЛИАЛАХ

Сохранить коммерческую тайну в филиале сложно именно из-за его удаленности. Мы не можем непосредственно воздействовать на филиалы и не можем позволить себе содержать сотрудников, которые специально занимались бы вопросами экономической безопасности. Отсюда вытекают проблемы применения технических средств защиты и кадровой политики.

Возможны два взаимосвязанных пути решения этих проблем:

– выезд в филиалы сотрудников службы экономической безопасности;

– обучение руководителей филиалов.

Кто несет ответственность

Практически все вопросы, связанные с экономической безопасностью, решаются руководством филиала. Правда, возможен другой вариант. Наряду с филиалами в структуру нашей компании включены дирекции, которые курируют определен-

sst-03.qxd 01.08.2007 22:42 Page 71

в срочном порядке сменить пароли и коды доступа к информационной системе.

К сожалению, иногда в филиалах поступают по принципу русского «авось». Кто-то думает – обойдется, кто-то, что есть дела важнее, и не выполняет это требование в полном объеме.

Маловероятно, что кто-то будет скачивать информацию, когда заявление об уходе уже подано.

Если при увольнении сотрудник решил скачать какую-то информацию, вряд ли он будет заниматься этим в последний рабочий день. Скорее всего, он предпримет какие-то меры заранее.

Какие последствия могут быть у такого хищения? Чтобы ответить на этот вопрос, необходимо понимать специфику страхования. Часть клиентов могут уйти вместе с агентом, но в большинстве случаев все зависит от условий страхования. Чтобы переманить страхователя, недостаточно просто располагать сведениями о нем. Поэтому большую опасность представляет хищение показателей компании – общих и по отдельным страховым продуктам.

ные регионы. Соответственно, региональные филиалы подчинены им. В крупных дирекциях есть сотрудники службы безопасности. Управление может идти и через них, но непосредственно в самом филиале вся ответственность за сохранение коммерческой тайны лежит на руководителе.

Однако, за сохранение коммерческой тайны в целом, как показывает практика, должна отвечать служба экономической безопасности.

Когда организуются новые филиалы и дирекции, перед нашими сотрудниками стоит задача определить:

- *круг информации, составляющей коммерческую тайну*
- *круг работников, которые будут владеть доступом к этой информации*
- *ситуации, когда эта информация может раскрываться внутри компании либо в договорных отношениях.*

Естественно, круг лиц, владеющих коммерческой тайной, и сам перечень информации в филиалах значительно уже, чем в головном офисе.

Какого рода коммерческие тайны доступны сотрудникам и руководству филиала?

- *Сведения о страхователях, страховых агентах, брокерах (о взаимоотношениях с ними, их финансовом положении, проводимых операциях и их объемах; условиях действующих и заключаемых договоров)*
- *данные о размере полученной страховой премии, комиссии и оплаченных убытках*
- *информация о планах по продвижению и разработке страховых продуктов*

sst-03.qxd 01.08.2007 22:42 Page 72

Злоупотребления имеют свойство накапливаться

Когда сотрудник вносит какие-то изменения в базу, обнаружить их достаточно трудно. Ведь к каждому человеку контролера не приставишь. Аналитические выкладки помогают обратить внимание на какие-то неувязки, «дыры» в базе, но они требуют времени. В центральных офисах, где службы безопасности мощнее, процесс проходит более оперативно. В удаленных филиалах – порой затягивается.

Отвечает ли руководитель за сохранение коммерческой тайны в своем филиале? Несомненно. Но ведь это не единственная возложенная на него обязанность. Часто, в силу разных причин (неподготовленность, занятость, отсутствие заинтересованности), директор решает этот вопрос эпизодически, что называется, от случая к случаю. Во-первых, руководитель может просто не обратить внимание на нарушение, хотя бы в силу того, что у него масса других обязанностей. Во-вторых, выявив в филиале какие-то злоупотребления, он может решить, что лучше «не

• сведения о разработках компании и ее подразделений, которые могут быть отнесены к «ноу-хау».

Ответственность за всю информацию, составляющую коммерческую тайну, несет руководитель. Он – с учетом наших рекомендаций – сам, на месте, определяет к какой информации каких сотрудников допустить.

Если компания разрабатывает какие-то новые технологии, мы, конечно, предоставляем данные филиалам, но дозировано – в целях сохранения коммерческой тайны.

Способы и методы

Для сохранения коммерческой тайны наиболее эффективны превентивные меры. Подбор сотрудников должен быть тщательным – особенно при назначении на должность руководителя. Опыт его предыдущей работы изучается самым подробным образом. Зная человека, мы можем с большой вероятностью сказать, каких сотрудников он будет подбирать.

Отправляясь в филиалы, сотрудники службы экономической безопасности проверяют организацию работы, разрабатывают рекомендации и обучают сотрудников. Как функционирует то или иное подразделение, можно выяснить по предоставляемым отчетам. Если денежные средства идут, жалобы не поступают, от правоохранительных органов нет никаких запросов, значит, все нормально. Поэтому один из методов контроля – ежедневный мониторинг поступающей из филиалов информации. По итогам можем спрогнозировать ситуацию в филиале.

sst-03.qxd 01.08.2007 22:42 Page 73

выносить сор из избы» и попытается исправить проблему своими силами. Получится у него или нет, это уже другой вопрос. Поэтому нашей службе необходимо постоянно проявлять бдительность.

Предположим, аналитика выявила, что в таких-то филиалах есть проблемы. Сопоставив факты, определяем, что, допустим, в одном не все неблагополучно со страхованием автотранспорта по таким-то категориям, по таким-то маркам машин и т.д. Начинаем выяснять, почему. Получается, оказывает влияние близость государственной границы. Тогда задаем себе вопрос: а в компаниях-конкурентах – та же ситуация? Такая же тенденция по региону? Нет, у нас показатели хуже. Значит, неблагополучная обстановка в самом филиале. Приблизительно зная направление работы, едем на место событий. Зачастую становится известно о лицах, действия которых не контролировались в определенный период времени. Проводится расследование, по результатам незамедлительно

Как и за что наказывать

Меры пресечения и наказания предусмотрены законодательством. Конечно, существуют специфичные способы, но подчеркну, что все они тоже в рамках закона.

Приведу несколько примеров нежелательных ситуаций и способов их решения.

Когда брокер или агент переходят в другую компанию, у них, естественно, остаются сведения о клиентской базе. Несколько человек, которые работали у нас и потом перешли к конкурентам, в какой-то мере стали использовать эту информацию. Как быть? Применять ли меры пресечения? Сведения о страхователях составляют коммерческую тайну. Мы вмешивались и предупреждали о возможном привлечении к ответственности – минимум, административной.

Еще один случай – сотрудник пытался использовать данные компании при подготовке дипломной работы. Дипломная работа, возможно, получилась бы интересной на примере конкретных цифр – но ведь на всеобщее обозрение попала бы рабочая информация. Мы также провели беседу, и сотрудник отказался от своих намерений. Применять тут меры наказания? Ущерб не нанесен, получается, наказывать не за что.

Необходимо постоянно отслеживать данные о страховом портфеле («болевая точка» в филиалах) и о суммах денежного оборота. Эта информация и представляет собой основную коммерческую тайну, сохранность которой может быть затруднена удаленностью региональных филиалов. А что касается мер, повторюсь, большинство из них – превентивного характера. Как говорится, стараемся не допускать, чтобы потом не наказывать.

sst-03.qxd 01.08.2007 22:42 Page 74

принимаются меры – вплоть до увольнения и передачи дела в прокуратуру.

Оповещать или замалчивать?

Даже если отвлечься от темы страхования и обратиться к опыту других крупных компаний, где хорошо отлажена служба безопасности, все равно можно привести примеры, так или иначе связанные с утечкой информации. Мы не скрываем, что такие случаи есть и у нас.

Когда выявляется подобная ситуация, мы оповещаем как агентов и сотрудников, так и страхователей. Но здесь надо учесть: определить, является ли кто-то преступником, может только суд. Поэтому, как правило, мы сообщаем о самом факте – без обозначения фамилий и, возможно, даже не называя конкретный филиал. Оповещаем через наш журнал, газету, через Интернет-сайт и информационные стенды.

Когда мы ставим людей в известность о выявленных злоупотреблениях, мы тем самым доносим до них:

- что нам известно о данном способе мошенничества
- что такие случаи не проходят безнаказанно.

Также мы показываем, что компания не скрывает недочеты и работает над их исправлением.

Например, сейчас в Санкт-Петербурге расследуется дело с привлечением нескольких наших сотрудников. Были использованы лазейки, позволившие совершить незаконные выплаты на сумму свыше двух миллионов рублей. Заведено уголовное дело.

Надо учитывать, что одному человеку, чтобы совершить мошенничество на подобную сумму, понадобилось бы много времени – оставаться после работы, чтобы никто не видел, какие изменения вносились в базу и т.д. Группе удалось выполнить все махинации за относительно короткий период.

Вместо послесловия

Способы мошенничества давно описаны в соответствующей литературе. Со временем они совершенствуются, но при надлежащей работе все рано или поздно выявляются. Методы пресечения индивидуальны в каждом конкретном случае.