Т.А. Курзенева

ПРИМЕНЕНИЕ КОНКУРЕНТНОЙ РАЗВЕДКИ В ЦЕЛЯХ ЗАЩИТЫ ИНФОРМАЦИИ

(Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ)

В настоящее время общество находится в той стадии развития, когда каждый из нас получает, обрабатывает, хранит огромное количество информации. В быстром темпе жизни, который присущ современному человеку, с большой долей вероятности можно упустить какую-либо информацию, задачу из виду. Особенно это актуально для людей, ведущих свой бизнес, развивающих собственными силами компании, реализующими новейшие технологии в различных сферах жизни.

Для упрощения подобной ситуации многие используют возможности ИТ-технологий, накапливать и обрабатывать необходимую информацию, напоминать о важных встречах и т.д., а также существенно проще управлять делами не в одиночку. Для этого нанимается персонал, который обучается, информируется о делах компании, о ее новейших разработках и планах на дальнейшее будущее. Но вот именно в этот момент, когда, казалось бы, решена проблема потери информации вследствие забывчивости одного человека и не способности человеческого мозга обрабатывать слишком большие объемы информации в единицу времени, возникает новая проблема – проблема доверия. Достаточно ли мы защищаем информационную структуру компании от несанкционированного доступа и хищении информации? Можно ли доверять столь ценную информацию только что нанятым сотрудникам?

Начнем последовательно разбираться в возникших проблемах. Вопрос защиты информационной структуры компании давно является одним из самых актуальных в сфере информационной безопасности. Существует множество законодательных актов, обязывающих и рекомендующих защищать определённые виды информации конкретными способами. Разработано большое количество комплексов и систем защиты информации, способных обезопасить компанию в зависимости от модели угроз. Используя предложения рынка информационной безопасности можно закрыть возможные уязвимости информационной структуры компании.

Можно сделать вывод, что в таком случае не стоит опасаться на безопасность компании. Однако есть один интересный закон – закон Мерфи. Согласно данному закону, интерпретируемому в область информационной безопасности Алексеем Лукацким в декабре 2003 года, доказано, что «Если 4 дыры устранены, то всегда найдется пятая» и «Любая программа содержит дыры», как следствие «Даже системы защиты содержат дыры».

Конечно, можно бесконечно закрывать уязвимости в информационной структуре, настраивать средства защиты информации, устанавливать патчи и

т.п. Но, когда специалисты службы информации уже приняли все возможные на данные момент меры по защите информационной структуры, а атаки и утечка информации продолжается стоит вспомнить про второй вопрос, возникший в начале рассуждения. Можно ли доверять коммерчески ценную информацию только что нанятым сотрудникам?

В данной ситуации необходимо понимать, что по статистике большую часть злоумышленников составляют так называемые внутренние злоумышленники. Такие злоумышленники в компании могут появиться по различным причинам: кто-то специально внедряется в доверенный круг лиц с целью хищения информации, кто-то совершает действия, которые могут нанести ущерб компании, по не знанию, не имея мотивации. Если со вторым типом внутренних злоумышленников можно бороться простейшим обучением сотрудников правилам и нормам работы со средствами защиты, то вычисление и нейтрализация первого типа дается гораздо сложнее.

Поскольку необходимость в персонале имеющим доступ к определенным частям коммерчески значимой информации никуда не пропадет, необходимо найти способ проверки доверия к данным сотрудникам. Одним с подходящих - Конкурентная разведка.

У большинства людей Конкурентная разведка ассоциируется либо со шпионажем (промышленным, военным, агент 007), либо со сбором информации о конкурентах с целью опережения. Второе представление является правильным, однако не полноценным. Конкурентная разведка на данный момент может служить не только в качестве инструмента продвижения бизнеса, но и в целях защиты информации. С ее помощью руководитель может изучать не только конкурентов, клиентов, но и работников, претендующих на должности с определенным уровнем доступа. Таким образом, одной из целей конкурентной разведки является защита информации. Выяснив, что инструменты конкурентной разведки позволяют проанализировать личность и мотивацию человека, желающего занять должность в компании, нужно понять, как именно «проверять» будущего сотрудника.

В американской интерпретации конкурентная разведка - Competitive Intelligence – это особый вид информационно-аналитической работы, позволяющий собирать обширнейшую информацию о юридических и физических лицах без применения специфических методов оперативно-розыскной деятельности, являющихся исключительной прерогативой государственных правоохранительных органов и спецслужб. Согласно данному определению можно сделать вывод, что способы сбора и анализа информации, применяемые при «проверке» кандидата на работу, являются простейшими и доступными. Например, для составления досье на физическое лицо, достаточно использовать единые государственные базы данных: ЕГРЮЛ, судебных дел, о банкротстве и многие другие. Для полноты картины проводят анализ социальных сетей, форумов, СМИ, а также применяют дополнительные команды различных поисковых машин, с помощью которых в большой выдаче поиска можно отфильтровать и

найти файлы фиксированного расширения (чаще всего информация находится в xls и pdf), конкретные словосочетания.

Все получается замечательно, проверяем кандидата на работу, убеждаемся в его целях и мотивах, но возникает вопрос о законности подобной «проверки». Не нарушаем ли мы законы Российской Федерации и какие они?

В России конкурентная разведка появилась значительно позже, чем в Европе и Америке. Российское законодательство еще не содержит норм, направленных на регулирование именно конкурентной разведки. В связи с этим данное направление деятельности подчиняется общим нормам и законам, связанным со сбором и анализом информации: федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О коммерческой тайне», «О средствах массовой информации», «О частной детективной и охранной деятельности», «Об авторском нраве и смежных правах», «О бюро кредитных историй», «О государственной тайне», Уголовный кодекс (Гл. 19, Ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», Гл. 21, Ст. 163 «Вымогательство», Гл. 22, Ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», Гл. 23, Ст. 204. «Коммерческий подкуп»). Именно они описывают нарушения и незаконные способы получения информации. При этом открытые информационные источники часто предоставляют достаточно широкие возможности для работы в данном направлении.

Защищать коммерчески значимую информацию компании можно и нужно. Данная защита не должна ограничиваться исключительно техническими средствами защиты, обновлениями программного обеспечения и физической защитой. Необходимо защищать информацию и на организационном уровне, включая обучение персонала и его проверку при приеме на работу. С последней задачей легко справиться с помощью методов конкурентной разведки. Применив комплексный подход к защите информации, можно не бояться потери ценной для компании и бизнеса информации.

Литература

1. А.В. Лукацкий Законы Мерфи для информационной безопасности [Статья]. - 2003 г.

2. Е.В. Ющук Конкурентная разведка: маркетинг рисков и возможностей [Книга]. - Екатеринбург : Издательство "Вершина", 2006.

3. Конкурентная разведка [Электронный источник]. - http://www.grandars.ru/college/ekonomika-firmy/konkurentnaya-razvedka.html .

4. Конкурентная разведка [Электронный источник]. - https://searchinform.ru/resheniya/biznes-zadachi/konkurentnaya-razvedka/.