Предисловие

Современный этап развития общества характеризуется существенным возрастанием понимания роли и актуальности проблем обеспечения безопасности во всех сферах жизнедеятельности. Особенно показателен этот процесс для сферы информационной безопасности, которая за последнее десятилетие вышла из области компетенции сугубо специальных служб и превратилась в мощный сегмент рыночной индустрии современных информационно-телекоммуникационных технологий.

При мощном прогрессе области технической защиты информации общепризнано, что безопасность функционирования сложных организационно-технических систем определяется, прежде всего, так называемым человеческим фактором, в качестве одной из характеристик которого выступает уровень профессиональной подготовки работников. Проведенные теоретико-методологические исследования проблем информационной безопасности позволили сделать вывод, что задача создания системы планомерной подготовки, переподготовки и повышения квалификации кадров играет не менее важную роль наряду с технологическими и техническими аспектами защиты чувствительной (критичной) информации. Актуальность такой задачи не подлежит сомнению в связи с возрастающими требованиями к эффективности, надежности и безопасности сложных комплексов, функционирующих на основе использования сложных современных технологий.

Именно поэтому в Доктрине информационной безопасности Российской Федерации развитие системы обучения кадров, используемых в области обеспечения информационной безопасности, отнесено к числу первоочередных мероприятий по реализации государственной политики в рассматриваемой сфере.

Проблема повышения кадрового потенциала является важнейшей и для государственной системы технической защиты информации. Так, в соответствии с постановлениями Правительства Российской Федерации необходимыми требованиями и условиями осуществления лицензируемых видов деятельности в области технической защиты конфиденциальной информации является наличие у специалистов организации-лицензиата либо соответствующего высшего профессионального образования, либо свидетельства о специальной

переподготовке по вопросам защиты информации. Такие требования введены в связи с наличием определенного дефицита квалифицированных кадров по обеспечению безопасности современных информационных технологий.

Органы государственной власти, в частности Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, как компетентные органы всегда уделяли особое внимание и поддерживали усилия ученых, преподавателей и специалистов по разработке нормативного и методического обеспечения процессов обучения кадров в области технической защиты информации в рамках государственной системы высшего, дополнительного и среднего специального образования. Не секрет, что в настоящее время остро ощущается также дефицит в специализированной литературе для подготовки кадров разных образовательных уровней. Особенно остро это ощущается в различных учебных центрах, занимающихся повышением квалификации специалистов в области технической защиты информации. Имеющаяся в наличии литература пока не охватывает все аспекты рассматриваемой проблемы, а обсуждаемые вопросы часто не имеют достаточной глубины проработки.

В предлагаемом вниманию читателей специализированном учебном пособии автор, используя существующую литературу, свой опыт работы и методические разработки в данной области, последовательно и в необходимом объеме постарался изложить вопросы, касающиеся организации и осуществления работ по защите от утечки информации по техническим каналам.

Введение

Приступая к решению любого вопроса, мы, прежде всего, интересуемся тем, что же нам известно по данному вопросу, то есть собираем необходимые данные или информацию. Однако то, что нам представляется важной информацией, другими, не интересующимися данным вопросом, может восприниматься как никчемный и заурядный шум, поэтому представляется необходимым и актуальным разобраться в том, что же означает термин «информация» и как его трактуют руководящие документы.

В Большой советской энциклопедии этот термин трактуется следующим образом: «Информация (от лат. informatio — разъяснение, изложение) — сведения, передаваемые одними людьми другим людям устным, письменным или каким-либо другим способом (например, с помощью условных сигналов, с использованием технических средств и т. д.), а также сам процесс передачи или получения этих сведений» БСЭ, издание III, том 10, страница 353.

ФЗ № 149 «Об информации, информационных технологиях и защите информации», принятый Государственной Думой 27 июля 2006 года, таким образом трактует это понятие: информация — сведения (сообщения, данные) независимо от формы их представления.

Расширим и уточним, применительно к нашей тематике, понятие информации. Для удобства изложения разделим всю информацию на две основных категории:

- информация вербальная;
- информация невербальная.

Вербальная информация — это различные сведения, выраженные средствами языка (письменно или устно).

Невербальная информация не передает какого-то конкретного содержания, но косвенно указывает, подтверждает или опровергает тот или иной факт. Это перемещения, встречи с кем-то, посещаемые места, поведение при этом и т. д. (например, тайная встреча с представителем конкурирующей фирмы).

Данные категории информации можно условно подразделить на два вида: первый — это (используя американскую терминологию) «мягкая» информация, второй — «твердая» информация.

«Мягкая» информация — это информация, носителем которой является поле (акустическое или электромагнитное). Такая информация живет буквально мгновения; однажды произведенная (озвученная), она исчезает и повторно воспроизведена быть не может. Говоря простым языком, «мягкая» информация — это сведения, которые содержатся в произнесенных вами (по телефону или в личной беседе) словах, или ваши текущие действия.

«Твердая» информация — это информация, записанная на каком-то материальном носителе (бумаге, магнитном носителе, флешкарте и т. п.). Такая информация, если ее специально не стирать, может существовать до тех пор, пока существует сам носитель. К ней можно отнести различные документы, магнитные, кино- и видеозаписи и т. п.

Кроме того, информацию можно условно подразделить на:

- общую, или тотальную, которая позволяет получить общее обзорное представление об интересующей проблеме и участниках (индивидах и организациях) решающих данную проблему;
- текущую, или оперативную, позволяющую постоянно ориентироваться в курсе изменяющихся событий;
- конкретную, т. е. информацию, позволяющую ответить на определенные вопросы и заполнить выявленные пробелы в имеющихся данных;
- косвенную, которая, будучи состыкованной с имеющимися данными по решаемой проблеме только опосредованно, позволяет подтвердить или опровергнуть некие предположения;
- оценочную, позволяющую разобраться и оценить события и дать прогноз относительно их развития в будущем. Это оптимально обработанные данные.

При этом следует конкретно различать и не путать: факты (данные), мнения (личностные предположения) и собственно информацию (аналитически обработанные данные).

Своевременно полученная и достоверная информация обычно позволяет:

- ориентироваться в ситуации;
- четко планировать свои действия;
- отслеживать результативность проводимых акций;
- уклоняться от неожиданностей;
- манипулировать отдельными людьми и группировками.

При этом для получения необходимой информации широко используются её физические свойства. Следовательно, знание особенностей функционирования информации различного вида позволит успешно организовать защиту от её утечки по различным каналам. Что

же мы подразумеваем под утечкой информации? Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Понятие «утечка» широко распространено. Говорят об утечке воды, газа, материальных ценностей со склада, информации и т. д. Утечка информации возможна при ее разглашении людьми, утери ими носителей с информацией, переносе информации с помощью любого вида носителя.

Рассматривая вопрос об особенностях утечки информации, необходимо отметить, что:

- утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю (злоумышленнику), в отличие, например, от утечки воды или газа;
- при утечке информации происходит ее тиражирование, которое не изменяет характеристики носителя информации (не уменьшается количество листов документа, не сокращается число пикселей изображения, не меняются размеры, цвет и другие характерные признаки продукциии и т. д.);
- цена информации при ее утечке уменьшается за счет тиражирования;
- факт утечки информации, как правило, обнаруживается спустя некоторое время, по последствиям, когда меры по обеспечению ее безопасности могут оказаться неэффективными.

Следовательно, под утечкой информации следует понимать не процесс распространения носителя информации за пределы определенной области пространства вообще, а частный случай распространения, когда она попадает к злоумышленнику.

Замечание о несанкционированности получателя имеет принципиальное значение. Если получатель информации санкционирован, то речь идет не об утечке, а о передаче информации по так называемому функциональному каналу связи, специально создаваемому для обеспечения коммуникаций в человеческом обществе.

Современный деловой человек не может отмахиваться от проблем доступа к закрытой информации и от вопросов скрытия своей информации. Естественно, не рекомендуется использовать криминальные пути достижения своих целей — заниматься шпионажем для шантажа и вторжения в личную жизнь граждан. Но обязательно необходимо представлять, как это могут сделать другие по отношению к вам.

Обладание одной и той же информацией различными пользователями может привести к абсолютно противоположным результатам. При этом информацию принято считать ценной лишь тогда, когда ее

можно использовать, причем полезность информации сильно зависит от ее полноты, точности и своевременности.

По мнению западных специалистов, утечка 20 % коммерческой информации в шестидесяти случаях из ста приводит к банкротству фирмы. Информация — второй, после времени, по ценности товар. Кто владеет информацией, тот добивается наибольших результатов.

Для уменьшения угроз экономической деятельности фирмы необходимо получение информации о внешней и внутренней среде, а это включает в себя, помимо прочего, информацию о конкурентах, информацию о сотрудниках. Поэтому вполне естественно, что уменьшение данных угроз для одних влечет за собой увеличение угроз экономической деятельности для других.

Получение даже незначительной информации о конкуренте может сэкономить фирме огромные средства, что является достаточно сильным стимулом для нарушения законов, регулирующих отношения в области информации. Сложнее приходится добросовестному субъекту данных отношений, так как он ограничен в своих действиях Законом.

Поэтому знание того, каким путем важная для него информация ограниченного пользования может попасть к конкурентам, позволит собственнику информации организовать ее успешную защиту, а изучение законодательства Вашего государства позволит Вам, не нарушая законов, регламентирующих деятельность в области информационной безопасности, осуществить защиту информации ограниченного пользования, которая циркулирует на Вашем предприятии.