В этой связи представляется возможным рассмотреть теоретико-правовые проблемы розыска лиц, пропавших без вести; совершенствование организационных основ деятельности оперативных подразделений по розыску лиц, пропавших без вести, и его тактическое обеспечение.

От эффективности розыска зависит количество обнаруженных лиц, которые становятся жертвами преступления, несовершеннолетних лиц либо лиц, которые не могут сообщить о себе из-за болезни, приведшей к потере памяти, расстройству психики, бессознательному состоянию. Это предъявляет дополнительные требования к скорости и качеству розыска, свидетельствует об актуальности рассматриваемой темы, необходимости новых разработок в данной области, актуальности рассмотрения современных оперативно-розыскных ситуаций, способов их разрешения, необходимости выработки новых подходов в деятельности по розыску лиц, пропавших без вести, научно-практических рекомендаций для сотрудников оперативных подразделений ОВД.

УДК 004.056.53

А.В. Калач

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Сегодня проблема утечек данных рассматривается на качественно новом уровне, поскольку личная и коммерческая информация представляет собой ценнейший актив, за который разворачивается нешуточная борьба.

Доктрина информационной безопасности Российской Федерации одним из национальных интересов в информационной сфере определила обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры Российской Федерации. События последнего десятилетия со всей очевидностью показывают, насколько значимой является проблема безопасности информации.

Несмотря на современный уровень развития электронно-вычислительных машин, позволивший значительно упростить множество сложных, трудоемких и рутинных математических операций, степень защищенности информации в таких устройствах значительно снизилась.

Данные мировой и российской статистики свидетельствуют о тенденции роста масштаба компьютерных злоупотреблений, приводящих к значительным финансовым потерям хозяйствующих субъектов различного уровня (рис. 1).

Рис. 1. Динамика утечки информации и объема скомпрометированных данных в мире за период 2011–2017 гг.

Из рисунка видно, что за рассматриваемый период в четыре раза вырос объем утекших данных. Представляет особый практический интерес сопоставление количества утечек информации в мире с аналогичными значениями в Российской Федерации (рис. 2).

Рис. 2. Количество утечек информации в России и мире

Рассматривая основные этапы формирования политики безопасности организации в целом, можно сделать вывод о том, что основополагающими в решении этого вопроса являются выбор и обоснование основных целей развития, т. е. информационная безопасность должна быть направлена на обеспечение динамичного развития организации и реализацию намеченной стратегии.

На рис. 3 показано, какие виды информации чаще всего похищают злоумышленники. В основном они похищают персональные данные. Это характерно и для России, и для всего мира.

Рис. 3. Распределение утечек информации по основным ее видам

Однако для России не характерен рост числа утечек коммерческой тайны и ноу-хау, тогда как в мире данный показатель увеличивается. Аналогичная закономерность наблюдается в России и в отношении сведений, составляющих государственную тайну (рис. 4).

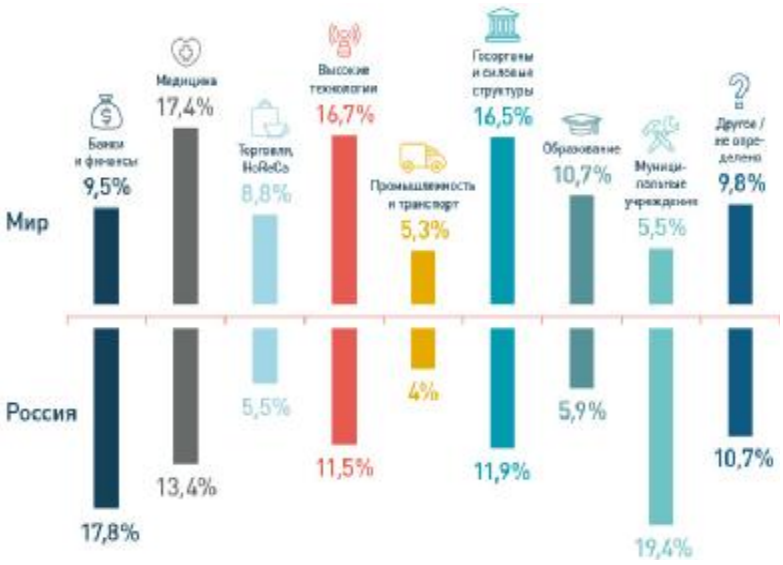

Рис. 4. Сопоставление отраслевого распределения утечек информации в России и в мире

Из рис. 4 видно, что проблема утечки информации пронизывает все сферы современной человеческой деятельности и обеспечение гарантированного уровня безопасности информации в современных условиях требует совершенствования действующих систем, средств и процессов управления информационной безопасностью организации. Не являются исключением и федеральные органы государственной власти Российской Федерации. Данный факт обусловливает необходимость непрерывной актуализации возможных каналов утечки информации.

Основной угрозой безопасности информации и нормального функционирования информационных систем являются различные каналы утечки данных. На долю чрезвычайных обстоятельств природного характера приходится не более 15 % всех потерь информации. Отсюда следует, что наибольшую опасность для информации представляют искусственные угрозы.

Следует отметить, что в динамике утечек данных наметилась тенденция к уменьшению использования «традиционных» каналов. Эти каналы практически не используются, вероятно, по причине высокой эффективности функциональных возможностей действующих защитных решений.

С позиции возможного ущерба наиболее опасными и самыми частыми являются непреднамеренные ошибки постоянных сотрудников организации. Именно такие ошибки в первую очередь создают уязвимые места для действия различных внешних угроз. Существенную угрозу при этом представляют так называемые обиженные сотрудники, работающие в данный момент на предприятии или уже уволенные. Решение этой проблемы возможно за счет своевременного и всестороннего аннулирования прав доступа этих сотрудников к информации организации.