Ю.А. Белевская

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проведен анализ организации обеспечения информационной безопасности, который определяется через содержание защиты информации, предполагает уточнение особенностей решения задач информационной безопасности и дальнейшего совершенствования методов защиты.

Организация обеспечения информационной безопасности как важнейшего института информационного права предполагает уточнение содержания задач обеспечения информационной безопасности, методов и средств их решения.

Методы и средства обеспечения информационной безопасности предлагается выбирать в рамках создания такой системы защиты информации, которая гарантировала бы признание и защиту основных прав и свобод граждан; формирование и развитие правового государства, политической, экономической, социальной стабильности общества; сохранение национальных ценностей и традиций.

Такая система должна обеспечивать защиту информации, включающую сведения, составляющие государственную, коммерческую, служебную и иные охраняемые законом тайны, с учетом особенностей защищаемой информации в области регламентации, организации и осуществления защиты. В рамках этого многообразия видов защищаемой информации, по мнению автора, можно выделить следующие наиболее общие признаки защиты любого вида охраняемой информации [1]:

- защиту информации организует и проводит собственник или владелец информации или уполномоченные им на то лица (юридические или физические);

- организация эффективной защиты информации позволяет собственнику защитить свои права на владение и распоряжение информацией, стремиться оградить ее от незаконного владения и использования в ущерб его интересам;

- защита информации осуществляется путем проведения комплекса мер по ограничению доступа к защищаемой информации и созданию условий, исключающих или существенно затрудняющих несанкционированный, незаконный доступ к защищенной информации и её носителям.

Для исключения доступа к защищаемой информации посторонних лиц собственник информации, осуществляющий ее защиту, в том числе ее засекречивание, устанавливает определенный режим, правила ее защиты, определяет формы и методы защиты. Таким образом, защита информации представляет собой надлежащее обеспечение обращения защищаемой ин-

формации в специальной, ограниченной режимными мерами сфере.

С учетом содержания этого определения, а также других определений понятия защиты информации [2, 3, 4] и выделенных в них основных целей защиты информации, включающих предупреждение уничтожения или искажения информации; предупреждение несанкционированного получения и размножения информации, можно выделить ***основную задачу защиты информации*** в государстве – это ***сохранение секретности*** защищаемой информации.

В системе комплексной защиты информации решение этой задачи осуществляется относительно уровней защиты и дестабилизирующих факторов. А формирование относительно полного множества задач по этим группам осуществляется на основе анализа объективных возможностей реализации поставленных целей защиты, обеспечивающих требуемую степень информационной безопасности. Задачи можно разделить на две основные группы:

1) своевременное и полное обеспечение специалистов органов государственной власти конфиденциальной информацией;

2) ограждение засекреченной информации от несанкционированного доступа к ней других субъектов.

При обеспечении секретной информацией действуют ограничения, предусматривающие наличие допуска к информации соответствующей степени секретности и разрешения на доступ к конкретной информации. Анализ действующей практики и нормативных правовых актов, определяющих порядок доступа специалиста к соответствующей информации, позволил выделить ряд противоречий. С одной стороны, максимальное ограничение доступа к засекреченной информации уменьшает вероятность утечки этой информации, с другой – при обеспечении специалиста засекреченной информацией возможности доступа к ней ограничиваются его служебным положением и решаемой в настоящее время проблемой.

Вторая группа задач [5] является общей для всех органов государственной власти и включает:

1) защиту информационного суверенитета страны и расширение возможности государства по укреплению своего могущества за счет формирования и управления развитием своего информационного потенциала;

2) создание условий эффективного использования информационных ресурсов общества и государства;

3) обеспечение безопасности защищаемой информации: предотвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации;

4) сохранение конфиденциальности информации в соответствии с установленными правилами ее защиты, в том числе предупреждения утеч-

ки и несанкционированного доступа к ее носителям, предотвращение ее копирования, модификации и др.;

5) сохранение полноты, достоверности, целостности информации и ее массивов и программ обработки, установленных собственником информации или уполномоченными им лицами;

6) обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальной персональной информации, в том числе накапливаемой в банках данных;

7) недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности, принадлежащей государству, предприятиям и фирмам, частным лицам.

Для решения рассмотренных задач защиты информации можно выделить следующие методы: скрытие, ранжирование, дезинформация, дробление, страхование, морально-нравственные, учет, кодирование, шифрование.

Скрытие - это максимальное ограничение числа лиц, допускаемых к секретам, которое достигается следующим образом:

- путем засекречивания информации, то есть отнесения ее к секретной или конфиденциальной информации; ограничения в связи с этим доступа к этой информации в зависимости от ее важности для собственника;

- устранения или ослабления технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них.

Ранжирование как метод защиты информации включает деление засекречиваемой информации по степени секретности, регламентацию допуска и разграничение доступа к защищаемой информации.

Дезинформация – один из методов защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности, положения дел в организации и т. д. Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующие соперника объекты, и др.

Дробление (расчленение) информации на части с таким условием, что знание какой-то одной части информации не позволяет восстановить всю картину, всю технологию в целом. Применяется достаточно широко при производстве военной техники.

Страхование как метод защиты информации пока еще только получило признание. Нетрудно предположить, что страховые методы защиты информации будут применяться прежде всего для защиты коммерческих

секретов от промышленного шпионажа. Особенно, надо полагать, страховые методы будут эффективны в независимом секторе экономики, где административные методы и формы управления а более всего контроля, плохо применимы.

При страховании информации должно быть проведено аудиторское обследование и дано заключение о сведениях, которые предприятие будет защищать как коммерческую тайну, и о надежности средств защиты.

Целью применения указанных методов является, с одной стороны, обеспечение конституционных прав граждан – защита информации о частной жизни лица, с другой – защита информации, циркулирующей в органах государственной власти и не подлежащей распространению.

Морально-нравственные методы защиты информации можно отнести к группе тех методов, которые, исходя из выражения, что "тайну хранят не замки, а люди", играют очень важную роль в защите информации. Именно человек, сотрудник, допущенный к секретам и накапливающий в своей памяти колоссальные объемы секретной информации, нередко становится источником утечки этой информации или по его вине соперник получает возможность несанкционированного доступа к носителям защищаемой информации.

Морально-нравственные методы защиты информации предполагают воспитание сотрудника, допущенного к секретам; проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично); обучение сотрудника правилам и методам защиты информации; привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Проведенный анализ организации обеспечения информационной безопасности, который определяется через содержание защиты информации, предполагает уточнение особенностей решения задач информационной безопасности и дальнейшего совершенствования методов защиты.

Литература

1. Шиверский А.А. Защита информации: проблемы теории и практики. -М.: Юристъ, 1996. - 112 с.

2. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. -М.: МИФИ, 1995. - 96 с.

3. Фисун А.П., Касилов А.Н., Мешков А.Г. Информатика и информационная безопасность: Учебное пособие. -Орел: ОГУ, 1999. - 282 с.

4. Шураков В.В. Обеспечение сохранности информации в системах обработки данных. -М.: Финансы и статистика, 1985. - 224 с.

5. Теоретические основы информатики и информационная безопасность / Под ред. В.А. Минаева. -М., 2000. -С. 232-269.