Н.И. Новикова

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

ФГБОУ ВО «Саратовская государственная юридическая академия»
Научный руководитель: доцент В.К. Фёдоров

Развитие информационных технологий, их вторжение в среду человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё больше актуальными - и параллельно более сложными. Технологии обработки информации непрерывно совершенствуются, а совместно с ними меняются и практические методы обеспечения информационной безопасности.

На самом деле, совершенных способов защиты не найдено, во многом успех при построении механизмов безопасности для существующей системы будет зависеть от её индивидуальных особенностей, учёт которых плохо подаётся формализации. Поэтому часто информационную безопасность рассматривают как некую совокупность неформальных рекомендаций по построению систем защиты информации того или иного типа.

На сегодняшний день информационная сфера – не просто одна из главных сфер международной работы, но и объект столкновения интересов. Страны с развитой информационной инфраструктурой, определяя некие технологические стандарты и предлагая потребителям свои ресурсы, создают условия формирования и осуществления деятельности информационных инфраструктур в других странах, оказывают воздействие на развитие их информационной сферы. Поэтому в более промышленно развитых странах при формировании национальной политики почетное место получают развитие средств защиты и обеспечение безопасности информационной сферы[1].

Концентрация данных в компьютерных системах вынуждает наращивать усилия по её защите. Национальная безопасность, тайна государственного

1. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. краткий курс М.: Изд-во Феникс 2008

масштаба и пр. - все эти юридические аспекты требуют усиления контроля над информацией в коммерческих и государственных организациях.

В настоящие дни общество эффективно развиваться и совершенствовать свои внутренние механизмы может только в условиях правового государства, которое основывается на неукоснительном соблюдении законодательных норм. Роль права в жизни информационного общества становится определяющей, все его члены должны исполнять нормы законов и разрешать возникающие споры цивилизованным способом на основе законодательства[2].

Современные методы изменения, переработки, хранения и передачи информации создают благоприятную среду для появление информационных угроз, которые связаны с вероятностью раскрытия, утери и изменения данной информации. Вследствие этого обеспечение информационной безопасности – это наиболее важное, определяющее направление развития информационных технологий.

Непосредственными исполнителями злокачественного действия, которое негативно воздействует на информацию, могут выступать:

- люди;
- технические устройства;
- модели, алгоритмы, программы;
- технологические схемы обработки;
- внешняя среда.

Существуют следующие предпосылки, или причины появления угроз:

- объективные (количественная или качественная недостаточность элементов системы) - не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;
- субъективные - непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и

2. Правовое обеспечение информационной безопасности: учеб. Пособие для студ. высш. учеб. заведений/(С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др.); под ред. С. Я. Казанцева. - 2-е изд., испр. и доп. - М.: Издательский центр «Академия», 2007. - 240 с.

недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации[3].

Опасность вмешательства в информационные ресурсы заключается в овладении личной и конфиденциальной информацией, которая впоследствии может быть использована против ее первоначального обладателя и нанесение ему вреда.

Осуществление угроз информационной безопасности может быть произведено:

- через агентурные источники в органах коммерческих структур, государственного управления, имеющих возможность получения конфиденциальной информации;
- путём подкупа лиц, работающих на предприятии или в структурах, непосредственно связанных с его деятельностью;
- путём перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники, с помощью технических средств разведки и программно-математических воздействий на неё в процессе обработки и хранения;
- путём подслушивания переговоров, ведущихся в служебных помещениях, автотранспорте, в квартирах и на дачах;
- через переговорные процессы с зарубежными или отечественными фирмами, используя неосторожное обращение с информацией.
- через «инициативников» из числа сотрудников, которые хотят улучшить своё благосостояние с помощью «заработка» денег или проявляют инициативу по другим материальным или моральным причинам.

Способы и методы защиты информационных ресурсов

3Сёмкин С.Н, Э. В. Беляков, С. В. Гребенев, В. И. Козачок. Основы организованного обеспечения информационной безопасности объектов информатизации. М.: Изд-во «Гелиос АРВ» 2005

Параллельно развитию методов изменения и переработки информации, развиваются и способы ее защиты. Если ранее эта проблема была не столь явная и распространенная, то сейчас ставится вопрос о нарушении национальной безопасности через информационные ресурсы. Проблема имеет два комплексных решения:

К первому относится охрана конфиденциальности государственных сведений, которая обеспечит невозможность взлома и несанкционированного доступа. При этом под конфиденциальными сведениями понимаются сведения ограниченного доступа общественного характера (коммерческая тайна, партийная тайна и т. д.).

Ко второму направлению относится защита от информации, которая в последнее время приобретает международный масштаб и стратегический характер. При этом выделяют три основных направления защиты от так называемого информационного оружия (воздействия):

- на технические системы и средства;

- общество;

- психику человека.

Сервисы сетевой безопасности представляют собой механизмы защиты информации, обрабатываемой в распределённых вычислительных системах и сетях.

Инженерно-технические методы ставят своей целью обеспечение защиты информации от утечки по техническим каналам - например, за счёт перехвата электромагнитного излучения или речевой информации.

Правовые и организационные методы защиты информации создают нормативную базу для организации различного рода деятельности, связанной с обеспечением информационной безопасности.

Теоретические методы обеспечения информационной безопасности, в свою очередь, решают две основных задачи. Первая из них - это формализация разного рода процессов, связанных с обеспечением информационной

безопасности. Так, например, формальные модели управления доступом позволяют строго описать все возможные информационные потоки в системе - а значит, гарантировать выполнение требуемых свойств безопасности. Отсюда непосредственно вытекает вторая задача - строгое обоснование корректности и адекватности функционирования систем обеспечения информационной безопасности при проведении анализа их защищённости. Такая задача возникает, например, при проведении сертификации автоматизированных систем по требованиям безопасности информации.

Процесс информатизации касается практически всех сфер человеческой деятельности. С появлением новых информационных технологий информация начинает являться необходимым атрибутом обеспечения деятельности государств, юридических лиц, общественных объединений и граждан. От качества и достоверности информации, от её оперативности передачи зависят многие решения, принимаемые на самых разных уровнях - от глав государств до рядового гражданина.

Обеспечение информационной безопасности – одна из ведущих задач, стоящих перед государствами, ведь информационная среда – очень сложный механизм, который обеспечивает стабильное функционирование электронного оборудования, программного обеспечения и прочее.

Для того чтобы успешно справляться с поставленной задачей необходимо действовать на законодательном, программно-техническом, организационном и идеологическом уровне. Лишь комплексное решение проблемы приведет к желаемому результату и обеспечению должного уровня защиты информационных ресурсов.