Д. Б. Гущин
Научный руководитель
М. А. Дворкина
Белорусский торгово-экономический
университет потребительской кооперации
г. Гомель, Республика Беларусь

ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПУТИ ЕЕ ОБЕСПЕЧЕНИЯ

Широкое распространение вычислительной техники как средства обработки информации привело к информатизации общества и появлению принципиально новых, так называемых информационных технологий.

Появление любых новых технологий, как правило, имеет как положительные, так и отрицательные стороны. Информационные технологии, также не являются исключением из этого правила, и поэтому следует заранее позаботиться о безопасности при разработке и использовании таких технологий.

От степени безопасности информационных технологий в настоящее время зависит благополучие, а порой и жизнь многих людей. Такова плата за усложнение и повсеместное распространение автоматизированных систем обработки информации.

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации [1].

На практике важнейшими являются три аспекта информационной безопасности:

– доступность (возможность за разумное время получить требуемую информационную услугу);

– целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

– конфиденциальность (защита от несанкционированного прочтения) [1].

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

– аппаратные средства – компьютеры и их составные части;

– программное обеспечение – приобретенные программы, исходные, объектные, загрузочные модули и т. д.;

– данные, хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;

– персонал – обслуживающий персонал и пользователи [1].

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

– аварийные ситуации из-за стихийных бедствий и отключений электропитания;

– отказы и сбои аппаратуры;

– ошибки в работе персонала и т. д. [2].

Преднамеренные воздействия – это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

– недовольством служащего своей карьерой;

– взяткой;

– любопытством;

– конкурентной борьбой;

– стремлением самоутвердиться любой ценой [2].

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ (НСД). НСД использует ошибку любого вида в системе защиты и возможен при неправильном выборе средств защиты, их некорректной установке и настройке.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

Создание режима информационной безопасности – проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. Законодательный (законы, нормативные акты, стандарты и т. п.).

2. Морально-этический (всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации).

3. Административный (действия общего характера, предпринимаемые руководством организации).

4. Физический (механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей).

5. Аппаратно-программный (электронные устройства и специальные программы защиты информации) [2].

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Надежная система защиты должна соответствовать следующим принципам:

– стоимость средств защиты должна быть меньше, чем размеры возможного ущерба;

– каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы;

– защита тем более эффективна, чем проще пользователю с ней работать;

– возможность отключения в экстренных случаях [1].

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать. Под защитой должна находиться вся система обработки информации.

Таким образом, потеря конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях. Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз коммерческим секретам. Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

Список использованной литературы

1. **Информационная** безопасность [Электронный ресурс] // Учебные материалы. – Режим доступа : https://www.works.doklad.ru. – Дата доступа : 01.11.2020.

2. **Основные** аспекты информационной безопасности [Электронный ресурс] // Студенческая библиотека онлайн. – Режим доступа : https://www.studbooks.net. – Дата доступа : 01.11.2020.