УДК 377.031

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Е.Г. Ручаевская, В.В. Шаталова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж», Минск, Беларусь

Аннотация. Безопасность любой информационной системы можно определить как свойство, которое заключается в способности информационной системы обеспечить полную конфиденциальность и целостность хранимой информации, т.е. защиту данных от несанкционированного доступа, например в целях ее раскрытия, изменения или разрушения. Обеспечение информационной безопасности в информационно-вычислительных системах сегодня очень актуально. Информационную безопасность можно выделить как одну из основных информационных проблем XXI века. На самом деле, проблемы хищения информации, искажения смысла информации и ее уничтожения часто приводят к последствиям, ведущим не только к банкротствам фирм, но даже возможным жертвам (не говоря о возможных военных конфликтах). Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности. Поэтому правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем.

Ключевые слова: информационные системы; информационные технологии; информационная безопасность; защита данных; несанкционированный доступ; информация; хищение информации; информационные проблемы; целостность информации; защита информации.

INFORMATION PROTECTION IN INFORMATION COMPUTING SYSTEM

E.G. Ruchaevskaya, V.V. Shatalova

Educational Institution "Belarusian State University of Informatics and Radioelectronics", branch "Minsk Radio Engineering College", Minsk, Belarus

Abstract. The security of any information system can be defined as a property that consists in the ability of an information system to ensure complete confidentiality and integrity of stored information, i.e. protection of data from unauthorized access, for example for the purpose of its disclosure, modification or destruction. Ensuring information security is very important today. Information security can be identified as one of the main information problems of the 21st century. In fact, problems of information theft, distortion of the meaning of information and its destruction often lead to consequences leading not only to the bankruptcy of companies, but even to possible victims (not to mention possible military conflicts). Information protection is a set of measures aimed at ensuring information security. Therefore, a methodologically correct approach to information security problems begins with identifying the subjects of information relations and the interests of these subjects associated with the use of information systems.

Keywords: information systems; information Technology; information security; data protection; unauthorized access; information; theft of information; information problems; integrity of information; information protection.

Введение

Проблемы обеспечения защиты информации являются одними из важнейших при построении надежной информационной системы на базе ПЭВМ. Эти проблемы охватывают как защиту от несанкционированного доступа к данным, так и физическую защиту данных и системных программ, особенно защиту от компьютерного вируса. Таким образом, в понятие защиты данных включаются вопросы сохранения целостности данных и управления доступа к данным (санкционированность).

Основная часть

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Цель защиты информации – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение нанесения ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение. Эти действия являются базовыми для дальнейшего рассмотрения.

Придерживаясь принятой классификации будем разделять все источники угроз на внешние и внутренние.

Источниками внутренних угроз являются:

– Сотрудники организации;

– Программное обеспечение;

– Аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

– ошибки пользователей и системных администраторов;

– нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;

– ошибки в работе программного обеспечения;

– отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

– компьютерные вирусы и вредоносные программы;

– организации и отдельные лица;

– стихийные бедствия.

Формами проявления внешних угроз являются:

– заражение компьютеров вирусами или вредоносными программами;

– несанкционированный доступ (НСД) к корпоративной информации;

– информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;

– действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;

– аварии, пожары, техногенные катастрофы.

Угрозы для информационных систем можно представить следующими группами:

– угроза раскрытия – имеющаяся возможность доступа к определенной информации лицу, не имеющему права знать данную информацию.

– угроза целостности – намеренное несанкционированное изменение данных, которые хранятся в вычислительной системе или передаются из одной системы в другую по каналам связи (модификация или удаление).

Средства, которыми может быть обеспечена информационная безопасность, в зависимости от способа реализации можно разбить на следующие группы методов:

– организационные методы предполагают конфигурирование, организацию и администрирование информационной системы. Прежде всего, это относится к сетевым информационным системам и их операционным системам, полномочиям системного администратора, набору инструкций, которые определяют порядок доступа и функционирования в сети пользователей;

– технологические методы, охватывающие технологии осуществления сетевого администрирования, мониторинга и аудита безопасности ресурсов данных, ведения журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации;

– аппаратные методы, которые должны реализовать физическую защиту информационной системы от возможного несанкционированного доступа, аппаратные средства идентификации внешних терминалов системы и пользователей и т.д.;

– программные методы относятся к самым распространенным методам защиты информации (программы идентификации пользователей, программы парольной защиты, программы проверки полномочий, брандмауэры, криптопротоколы и т.д.). Без применения программной составляющей фактически невыполнимы даже первые три группы методов. При этом нужно учитывать, что стоимость реализации сложных программных комплексов по защите информации может значительно превосходить по затратам аппаратные, технологические и тем более организационные решения.

Со стороны разработчиков и потребителей в настоящее время наибольшее внимание вызывают следующие тенденции защиты информации:

– защита от несанкционированного доступа информационных ресурсов компьютеров, работающих автономно и в сети. В первую очередь эта проблема определяется для серверов и пользователей Интернета. Эта функция может быть реализована многочисленными программными, а также программно-аппаратными и аппаратными средствами;

– защита различных информационных систем от компьютерных вирусов, имеющих возможность не только разрушить необходимую информацию, но даже повредить технические компоненты системы;

– защита секретной, конфиденциальной и личной информации от чтения посторонними лицами и целенаправленного ее искажения. Эта функция может обеспечиваться как средствами защиты от несанкционированного доступа, так и с помощью криптографических средств, традиционно выделяемых в отдельный класс.

Также активно развиваются средства защиты от утечки информации по силовым каналам, каналам электромагнитного излучения компьютера или монитора (для решения данной проблемы может применяется экранирование помещений, использование генераторов шумовых излучений), средства защиты от электронных «жучков», устанавливаемых непосредственно в комплектующие компьютера и т. д.

Защита информации от несанкционированного доступа. Защита от несанкционированного доступа к информационным ресурсам компьютера представляется комплексной проблемой, которая предполагает решение следующих задач:

– присвоение пользователю, файлам, компьютерным программам и каналам связи идентификаторов – уникальных имен и кодов;

– установление подлинности при обращениях к вычислительной системе и информации, по сути, проверка соответствия лица или устройства, сообщившего идентификатор (такая идентификация пользователей, программ, терминалов при доступе к системе зачастую выполняется посредством проверки паролей или обращением в службу, которая отвечает за сертификацию пользователей).

Информационная безопасность включает меры по защите процессов создания данных, их ввода, обработки и вывода. Главная цель состоит в том, чтобы защитить и гарантировать точность и целостность информации, минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, когда информация создается, модифицируется, когда к ней обеспечивается доступ и когда она распространяется.

Информационная безопасность гарантирует достижение следующих целей:

– конфиденциальность критической информации;

– целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода);

– доступность информации в случае необходимости;

– учет всех процессов, связанных с информацией.

Угроза безопасности компьютерной системы – это потенциально возможное происшествие, неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Уязвимость компьютерной системы – это некая ее неудачная характеристика, которая делает возможным возникновение угрозы. Другими словами, именно из-за наличия уязвимостей в системе происходят нежелательные события.

Атака на компьютерную систему – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака – это реализация угрозы. Заметим, что такое толкование атаки (с участием человека, имеющего злой умысел), исключает присутствующий в определении угрозы элемент случайности, но, как показывает опыт, часто бывает невозможно различить преднамеренные и случайные действия, и хорошая система защиты должна адекватно реагировать на любое из них.

Угроза раскрытия заключается том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова «раскрытие» используются термины «кража» или «утечка».

Заключение

В заключении можно отметить, что защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу и государству.

Список использованных источников

1. Абразовский Ю.Д., Ручаевская Е.Г. (2024) Безопасность информационных технологий. *60 Научно-практическая конференция аспирантов, магистрантов и студентов БГУИР. Научная конференция учащихся филиала БГУИР «Минский радиотехнический колледж»*, 17–18.

References

1. Abrazovski J.D., Ruchaevskaya E.G. (2024) Safety information technologies. *60 Scientific practical conference-практическая конференция of postgraduates, masters and students BSUIR. Scientific students conference branch «Minsk Radio Engineering College»*, 17–18.

Сведения об авторах

Ручаевская Е.Г., канд. пед. наук, доц., преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж». elenruch@gmail.com.
Шаталова В.В., канд. техн. наук, доц., директор, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж». shatalova@bsuir.by.

Information about the authors

Ruchaevskaya E. Cand. Sci. Ped., Associate Professor, teacher. educational institution «Educational Institution "Belarusian State University of Informatics and Radioelectronics". branch "Minsk Radio Engineering College", elenruch@gmal.com.
Shatalova V., Cand. Sci. Tech., Associate Professor. director. Educational Institution "Belarusian State University of Informatics and Radioelectronics". branch «Minsk Radio Engineering College». Shatalova@bsuir.by.