УДК 004.056.53

ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

А.С. Михайлова, С.С. Лапина
Ульяновский государственный технический университет, г. Ульяновск

Ключевые слова: защита, информация, угрозы.

Основными целями и задачами обеспечения информационной безопасности в ТКС являются:

Уязвимость ТКС - это определенное неблагоприятное свойство системы, позволяющее создавать и реализовывать угрозу. Атака на компьютерную систему - это действие, предпринятое злоумышленником, которое включает в себя поиск и использование определенной уязвимости в системе. Таким образом, атака-это реализация угрозы безопасности.

Противодействие угрозам безопасности является целью защиты систем обработки информации.

Под угрозой информационной безопасности мы будем понимать возникновение такого явления или события, следствием которого может быть негативное воздействие на информацию: нарушение физической целостности, логической структуры, несанкционированное изменение, несанкционированное получение, несанкционированное воспроизведение [2].

В соответствии с целью воздействия выделяют три основных типа угроз безопасности ТКС:

- угрозы конфиденциальности информации;
- угрозы целостности информации;
- угрозы работоспособности системы (отказ в обслуживании).

Угрозы конфиденциальности направлены на раскрытие конфиденциальной или секретной информации. Угрозы целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена злоумышленником умышленно, а также в результате объективных воздействий со стороны окружающей систему среды [2].

Для обеспечения безопасности информации проводятся различные мероприятия.

Традиционными методами защиты информации от несанкционированного доступа являются: идентификация и аутентификация, защита паролем.

Идентификация и аутентификация. В компьютерных системах концентрируется информация, право на использование которой принадлежит определенным лицам или группам лиц, действующим по собственной инициативе или в соответствии со своими служебными обязанностями. Для обеспечения безопасности информационных ресурсов, исключения возможности несанкционированного доступа и усиления

контроля за санкционированным доступом к конфиденциальной или секретной информации внедряются различные системы идентификации, аутентификации объекта (субъекта) и контроля доступа [1].

Защита паролем. При выборе пароля возникают вопросы о его размере, устойчивости к несанкционированному выбору и способах его использования. Естественно, чем длиннее пароль, тем большую безопасность обеспечит система, ведь для его угадывания потребуется немало усилий.

Пароль вводится пользователем в начале взаимодействия с компьютерной системой, а иногда и в конце сеанса (в особо критических случаях пароль обычного вывода может отличаться от входного). Для удобства пользователя пароль можно вводить через определенные промежутки времени. Пароль может быть использован для идентификации и аутентификации терминала, с которого пользователь входит в систему, а также для обратной аутентификации компьютера по отношению к пользователю [2].

Список использованных источников:

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.

2. Краковский, Ю.М. Защита информации: Учебное пособие /Ю.М. Краковский. - Рн/Д: Феникс, 2015. - 416 с.

Михайлова Алина Сергеевна, студентка 3 курса Ульяновского государственного технического университета, E-mail: cneg68@inbox.ru

Лапина Светлана Сергеевна, студентка 3 курса Ульяновского государственного технического университета, E-mail: sveta-lapina-2019@mail.ru

УДК 004.522; 57.087.1

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПО ГОЛОСУ НА ОСНОВЕ ИНТЕРФЕРОМЕТРИИ

М.Ю. Огнев, М.Д. Лимов, М.Н. Осипов
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: биометрия, биометрия по голосу, виброакустическая информация, интерференция, спекл-структура, спекл-интерферометрия.

Из года в год количество киберпреступлений, связанных с кражей персональных данных пользователей, растет. Одним из методов защиты персональных данных являются биометрическая аутентификация по голосу.