Кашкин Евгений Владимирович
канд. техн. наук, доцент
Дебунов Андрей Александрович
аспирант
Меркулов Алексей Андреевич
аспирант
ФГБОУ ВО «Московский технологический университет»
г. Москва

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: *в данной статье рассмотрена информационная безопасность как одно из приоритетных направлений современных информационных технологий. В работе исследованы новые направления защиты информации. Выделены особенности биометрических средств защиты и использования компьютерного почерка как уникального ключа, носителем которого является пользователь.*

Ключевые слова: *информационная безопасность, информация, информационные технологии, информационные ресурсы, биометрический ключ, компьютерный почерк, ЭВМ.*

Виды защиты информации подразделяются на защиту от несанкционированного доступа (далее – НСД), защиту от утечки информации по каналам побочных электромагнитных излучений, защиту от вредоносных программ и защиту от перехвата в системе связи. Целями защиты информации выступают такие действия, как предотвращение утечки и НСД к охраняемым данным, предотвращение уничтожения, модификации, блокирования охраняемых данных, обеспечение правового регулирования в сфере охраняемых данных, как объекта собственности, защита государственной тайны, защита конституционных прав граждан в сфере личной информации и конфиденциальности персональных данных. Понятие информационной безопасности – достаточно ёмкая и многогран-

ная область. Сутью защиты от НСД является защита конфиденциальных и ценных данных, которые выступают в качестве собственности пользователя, от противоправных действий злоумышленника, способных нанести материальный и нематериальный вред, на примере конкретной ЭВМ, либо в сети [1–3].

Идентификация пользователя относится к основным задачам, для которых требуется эффективное решение в контексте защиты информации от НСД. Метод идентификации личности на основе специфики работы с клавиатурой основывается на том факте, что пользователь при работе с информацией в ЭВМ использует устройства ввода информации, к которым относится и клавиатура.

Вышеуказанный метод является мощным средством защиты информации от преступных посягательств с целью её хищения, преобразования, удаления, что классифицируется как нанесение материального и морального ущерба владельцу, нарушение его законных прав и свобод. Использование данного метода может быть направлено как на защиту данных от пользователя, не зарегистрированного в системе, так и на выявление лица из ряда других пользователей посредством его уникальных поведенческих характеристик. Перспективой настоящего метода является выявление пользователя в сети на основе биометрических данных, что требует дополнительных исследований и его модификации. Разрабатываемая в рамках данного исследования система представляет собой программное средство, направленное на сбор биометрических данных лица, осуществляющего работу с ЭВМ посредством клавиатуры. Сравнивая получаемые в реальном времени биометрические данные с биометрическими характеристиками эталонного типа возможно сделать вывод о легальности пользователя, осуществляющего работу с ЭВМ в данный момент времени [4–5].

Данная тема является приоритетным направлениям в настоящее время, так как использование биометрических алгоритмов идентификации пользователей и их программных реализаций в информационных системах набирает популярность, в связи с тем, что применяемость данных методов снижают риски хищения, модификации, уничтожения ценной информации, а соответственно НСД к охраняемым данным нежелательных лиц. Помимо того, биометрические данные,

выступающие в качестве аутентификаторов, являются уникальными в своём роде для каждого человека.

Особая важность данного метода заключается в возможности идентифицировать личность, исследуя специфику работы с ЭВМ посредством устройств ввода. При использовании данного алгоритма идентификации при НСД возможно выявить хищение, модификацию, уничтожение информации без ведома злоумышленника, получившего доступ к ЭВМ.

Список литературы

1. Обеспечение информационной безопасности организации на основе системы менеджмента информационной безопасности / П.Ю. Филяк, В.М. Шварев // Информация и безопасность. – 2015. – Т. 18. – №4. С. 580–583.

2. Информационный стресс – фактор, снижающий качество систем управления безопасностью / С.А. Рыбин, Б.В. Чувыкин // Труды международного симпозиума Надежность и качество. – 2008. – Т. 2. – С. 172–175.

3. Математическая модель для обработки данных с тепловых датчиков для управления системой задвижек тепловых контуров зданий специального назначения / Е.В. Кашкин, Т.Ю. Морозова // Естественные и технические науки. – 2013. – №6 (68). – С. 289–292.

4. Система обработки диагностических данных машиностроительного производства с целью повышения надежности технологического оборудования / Е.В. Кашкин, А.А. Дебунов, А.А. Меркулов // Естественные и технические науки. – 2016. – №4 (94). – С. 175–178.

5. Разработка научных методов защиты компьютерных сетей / С.С. Черненко, М.А. Назаренко // Современные проблемы науки и образования. – 2014. – №3. – С. 34.