***Кашкин Евгений Владимирович***
канд. техн. наук, доцент
***Малахина Елена Валентиновна***
начальник УПОУ
***Антонова Ирина Игоревна***
канд. техн. наук, доцент, доцент
ФГБОУ ВО «Московский технологический университет»
г. Москва

# ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

***Аннотация:*** *основным приоритетным направлением работы с информацией на сегодняшний день является информационная безопасность. При обеспечении защиты информации на сегодняшний день используют большое количество алгоритмов и методов для обеспечения достоверности представляемых данных в информационных системах. В работе рассматриваются основные направления защиты информации. Обозначаются ключевые места при формировании политики безопасности информационной системы.*

***Ключевые слова:*** *информационная безопасность, информация, информационные технологии, информационные ресурсы, биометрические данные.*

Проблема идентификации объектов является одной из основных задач, требующих эффективных решений в условиях современного информационного общества. Объектами идентификации могут выступать как сам человек, так и, например, транспортное средство, предмет, оборудование, техническое средство. Основным решением для усовершенствования систем идентификации считается передача ЭВМ, аппаратным и программным средствам наибольшего количества функций по сбору и обработке информации, а также, принятию решений, тем самым освобождая человека от рутинной работы. Это в особенности необходимо при обеспечении безопасности объектов и, например, при автомати-

зации процесса производства, где несоблюдение мер информационной безопасности могут нанести очень большой ущерб. Однако очень важно снабдить сотрудника службы безопасности полными и точными сведениями о происходящих событиях и специальными средствами для оперативного принятия решений, связанных с обеспечением мер безопасности.

В контексте информационной безопасности техническая реализация защиты от несанкционированного доступа основывается на задаче разграничения доступа к данным, в этом случае процедура доступа пользователя предполагает три этапа: идентификацию, аутентификацию и авторизацию. Такой подход применяется в сетевой среде. Во время идентификации субъект сообщает своё имя. В процессе аутентификации (проверка подлинности) вторая сторона должна убедиться в соответствии данного субъекта тому субъекту, за которого он себя выдаёт. Аутентификация может быть односторонней и двусторонней. Авторизация заключается в проверке прав субъекта на выполнение определенных действий. В сетевой среде сервис (объект) определяет, что предоставляется пользователем в качестве аутентификатора. По отношению к сервису, для подтверждения своей подлинности субъект должен предъявить либо пароль (что знает пользователь), либо, например, личную карточку (чем обладает пользователь), либо биометрические данные (часть самого пользователя) [1; 2].

В контексте информационных систем идентификация определяется как сравнение идентификаторов, присвоенных субъекту и объекту. В качестве субъекта обычно выступает пользователь или программа (пользовательский агент), который пытается осуществить доступ к объекту. В компьютерной системе имеются некоторые идентифицирующие данные, связанные с каждым зарегистрированным пользователем, которые могут представлять собой как число, так и строку символов, именующие его. Такая информация называется идентификационной, которая может быть как постоянной, так и изменяемой в процессе эксплуатации. Носителем идентификационной информации считается идентификатор, определенное устройство или признак, в соответствии с которым определяется

объект. Каждый из идентификаторов характеризуется специфицированным двоичным кодом и может представлять собой, например, строку символов, штрих-код, электронные ключи, основанные на использовании бесконтактных технологий, радиотеги, отпечаток пальца, фотоизображение лица, звукозапись голоса и другие физические признаки. Идентификатор считывается и передаётся в систему, после чего производится процедура распознавания. По сути, идентификацией является распознавание по идентификатору субъекта или объекта [3; 4].

Таким образом использование комплексного подхода при авторизации пользователя в системе позволяет в максимальной степени реализовать политику безопасности подразделения и компании в целом. Использование биометрических аспектов информационной безопасности позволят в большей степени гарантировать степень защищенности информации.

***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 безопасность / 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. Разработка методов и средств планирования и управления производственными процессами и их результатами / М.А. Назаренко, Е.В. Кашкин, И.А. Маркова, В.И. Селиванов, И.В. Макарова // Международный журнал экспериментального образования. – 2016. – №11–1. – С. 114–115.