Д. В. Шустова
Научный руководитель
А. В. Медведев
Белорусский торгово-экономический
университет потребительской кооперации
г. Гомель, Республика Беларусь

ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ БУХГАЛТЕРСКОГО УЧЕТА

Защита информации в бухгалтерском учете играет важную роль. Хищение учетной финансовой информации, такой как сведения о клиентах, прибыли компании, себестоимости продукции, заработной плате сотрудников, может стать причиной серьезных последствий.

Под защитой учетной информации понимается невозможность случайных или преднамеренных воздействий на нее естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям этой информации.

К объектам информационной безопасности в учете относятся как информационные ресурсы, так и средства системы информатизации.

Угроза информационной безопасности бухгалтерского учета заключается в потенциально возможном воздействии на компоненты учетной системы, способном нанести ущерб владельцам информационных ресурсов или пользователям системы.

Выделяют 3 вида потенциальных угроз в защите информации бухгалтерского учета:

– естественные угрозы вызываются объективными причинами, как правило, не зависящими от бухгалтера, ведущими к полному или частичному уничтожению бухгалтерии (землетрясения, пожары и т. п.);

– непреднамеренные (неумышленные), вызванные способностью сотрудников делать какие-либо ошибки в силу невнимательности либо усталости, болезненного состояния, например, при вводе сведений в компьютер нажать не ту клавишу, сделать неумышленные ошибки в программе, занести вирус, случайно разгласить пароли;

– преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников), намеренно создающих недостоверные документы.

Исходя из вышеперечисленных проблем предлагаются следующие методы защиты бухгалтерской информации:

– административные методы защиты информации – довольно эффективный способ, чтобы обезопасить сведения, если сотрудники компании вызывают доверие, территория предприятия охраняется, персонал не имеет возможности выйти в глобальную сеть;

– защита информации средствами операционных систем и блокированием загрузки, в настоящее время на базе MS-DOS разработано много программных продуктов (кодируемые диски, блокираторы); однако эти средства не являются эффективными, действия хакеров и квалифицированных программистов легко сведут на нет все используемые системы защиты;

– уничтожение накопителя информации – старый эффективный способ, заключающийся в уничтожении винчестера, сменного диска и другого носителя информации; информацию можно быстро восстановить с помощью резервного копирования;

– стирание данных – потеря информации, а не накопителя; восстановить данные можно также с помощью резервной копии;

– шифрование данных – самый эффективный способ, который заключается в преобразовании открытой информации с помощью шифровальных ключей в зашифрованную и наоборот; шифровальные системы очень стойкие, однако их использование может быть уголовно наказуемым.

Средства контроля, разработанные по требованиям безопасности, в автоматизированных учетных системах размещаются в тех точках, где возможный риск способен обернуться убытками. Такие точки называются точками риска или контрольными. Это те точки, где контроль будет наиболее эффективным и экономичным.

Как бы ни были эффективны средства защиты информации бухгалтерского учета, они не могут обеспечить полную гарантию.