

УДК 004.77

**Е.В. Черноокая, А.А. Ледницкая, В.П. Прокопович**  
Белорусский государственный экономический университет  
Минск, Беларусь

## **ИНФОРМАЦИЯ БУХГАЛТЕРСКОГО УЧЕТА КАК ОХРАНЯЕМЫЙ АКТИВ ОРГАНИЗАЦИИ**

*Аннотация.* В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности организации становится обеспечение информационной безопасности. В работе рассматривается защита бухгалтерской информации, которая подразумевает ее защищенность от случайных или преднамеренных воздействий с целью нанесения ущерба владельцам или пользователям информации.

**E.V. Chernookaya, A.A. Lednitskaya, V.P. Prokopovich**  
Belarusian State Economic University  
Minsk, Belarus

## **ACCOUNTING INFORMATION AS A PROTECTED ASSET OF THE ORGANIZATION**

*Abstract.* In connection with the development of information technologies and the computerization of the economy, one of the most important issues in the organization's activities is ensuring information security. The paper considers the protection of accounting information, which implies its protection from accidental or intentional influences with the aim of causing damage to the owners or users of information.

Информация – это один из самых ценных и важных активов любой организации, которая должна быть надлежащим образом защищена. В соответствии с Постановлением Совета безопасности Республики Беларусь от 18.03.2019 г. №1, информационная безопасность – это состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности. Ее целью является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие [1].

В современном мире системы бухгалтерского учета хозяйствующих субъектов независимо от организационно-правовых

форм собственности наиболее подвержены воздействию угроз информационной безопасности вследствие наличия вероятности разглашения информации, содержащей коммерческую тайну. Наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологий работы с информацией (в том числе, персональных данных), несанкционированного доступа к ней.

На сегодняшний день наиболее распространенными угрозами для данных бухгалтерского учета являются: утечка данных; некомпетентность и недобросовестность сотрудников; распространение вирусов или взлом программ; несанкционированное использование активов организации; непреднамеренные ошибки при обработке данных; преднамеренные действия, направленные на умышленное причинение ущерба, либо нелегальное использование (получение, изменение, уничтожение) информации.

Для успешного внедрения систем информационной безопасности внутри организации и защиты бухгалтерской (финансовой) информации от несанкционированного доступа необходимо придерживаться трех главных принципов:

1. Конфиденциальность. То есть доступ к информации должны иметь те лица, для кого эта информации предназначена. Она должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.

2. Целостность. Для того, чтобы руководитель мог принимать важные управленческие решения, информация должна быть достоверной, точной, а также внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.

3. Доступность. Данный критерий обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно [2].

Для обеспечения безопасности необходимо соразмерять технические и организационные меры с возможностями организации и ее информационной системой. При этом, обеспечение безопасности должно основываться на одновременном применении всего комплекса мер, предусмотренных законом или предлагаемых специалистами. В

связи с этим, мероприятия по защите информации в области бухгалтерского учета включают в себя:

- установка системы обеспечения сохранности информации, которая гарантирует, что любое движение данных бухгалтерского учета идентифицируется, авторизуется, обнаруживается и документируется.

- обеспечение технической защиты помещений и оборудования с дальнейшей сертификацией классов защиты, определение их соответствия нормативно-правовым требованиям;

- внедрение только проверенных программных решений, уже не раз протестированных другими предприятиями, плюсы и минусы которых очевидны;

- минимальные доработки имеющихся лицензионных программных продуктов силами собственных или привлеченных исполнителей;

- использование только проверенного программного обеспечения, а также установка и регулярное обновление антивирусных баз.

В последнее время широкое распространение в области защиты информации получили так называемые электронные ключи.

Долгое время такие устройства подсоединялись к разъему параллельного порта компьютера, что ввиду неудобства сдерживало широкое внедрение электронных ключей. Позже появились технологии, позволяющие подсоединять электронные ключи и через последовательные порты. В настоящее время это – наиболее надежный и удобный метод защиты тиражируемого программного обеспечения средней и высшей ценовой категории. Он обладает высокой стойкостью к взлому и не ограничивает использование легальной копии программы.

Электронными ключами, в основном, защищают так называемый «деловой» софт: бухгалтерские и складские программы, правовые и корпоративные системы, строительные сметы, электронные справочники, аналитический софт и т. п. Затраты на разработку таких программ велики, а соответственно высока их стоимость. Как следствие, ущерб от пиратского распространения будет значителен. Здесь электронные ключи являются оптимальной защитой [3].

Таким образом, предпринимательская деятельность в настоящее время невозможна без получения, накопления, хранения, обработки и использования разнообразных информационных потоков. И сегодня возникает масса проблем, связанных с обеспечением сохранности коммерческой (предпринимательской) информации как вида

интеллектуальной собственности. Информация все чаще подвергается числу угроз и уязвимостей. В связи с этим все большее значение имеет организация эффективной системы информационной безопасности, при создании которой использование, потеря или искажение любой информации о состоянии организации, в том числе бухгалтерской и финансовой, работниками организации или внешними лицами (пользователями) с высокой степенью вероятности не приведут в обозримом будущем к возникновению угроз прерывания деятельности этой организации.

### Список использованных источников

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: Постановление Совета Респ. Беларусь, 18 марта 2019 г., № 1// Онлайн-сервис готовых правовых решений iLex / ООО «ЮрСпектр». – Минск, 2022.
2. Информационная безопасность [Электронный ресурс]. – Режим доступа: <https://pirit.biz/resheniya/informacionnaja-bezopasnost>. – Дата доступа: 30.09.2022.
3. Электронный ключ – средство предохранения софта [Электронный ресурс]. – Режим доступа: <https://www.guardant.ru/press-center/publication/2001-08-01.html>. – Дата доступа: 30.09.2022.

УДК 004.855

**А.А. Шавейко**

Белорусский государственный технологический университет  
Минск, Беларусь

### ПРОГНОЗИРОВАНИЕ РЕЗУЛЬТАТОВ СПОРТИВНЫХ МАТЧЕЙ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

*Аннотация.* В статье рассмотрена возможность и актуальность прогнозирования результатов спортивных матчей на основе методов машинного обучения. Рассмотрены этапы и особенности построения модели обучения.

**A.A. Shaveyko**

Belarusian State Technological University  
Minsk, Belarus

### PREDICTING THE RESULTS OF SPORTS MATCHES BASED ON MACHINE LEARNING METHODS