УДК 004.056.5

Н. И. Глухов[1], В. В. Иванов[1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

НЕКОТОРЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Аннотация. Главной целью данной статьи является обзор некоторых методов обеспечения информационной безопасности при использовании систем электронного документооборота на предприятиях и в современных организациях. Авторами представлен анализ некоторых информационных технологий на основе отечественных и зарубежных публикаций.

***Ключевые слова*:** Информационная безопасность, система электронного документооборота, защита информации, информация, цифровизация.

N. I. Glukhov[1], V.V. Ivanov [1]

[1] Irkutsk State Transport University, Irkutsk, Russian Federation

SOME METHODS OF INFORMATION PROTECTION WHEN USING ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Abstract. The main purpose of this article is to study organizational methods of ensuring information security in the use of electronic document management systems. As a result of the work, the author uses theoretical and empirical research methods. In order to obtain more detailed and up-to-date information, scientific materials of domestic and foreign authorship are used in the work. The predominant part of the article is devoted specifically to the issue of ensuring information security in modern information systems.

Keywords. Information security, electronic document management system, information protection, information, digitalization.

Повсеместная цифровизация современного общества ставит перед современным ИТ-сектором множество актуальных и сложных задач, связанных с обеспечением информационной безопасности (ИБ). На сегодняшний день ведутся активные разработки и интеграции инновационных технологий, значительно повышающих уровень обеспечения ИБ компаний, использующих в своей деятельности различные цифровые средства. Несмотря на это, сегмент ИБ нуждается в повышении качества и эффективности работы алгоритмов, препятствующих несанкционированному доступу к информации. Одной из наиболее актуальных и требующей особого внимания задачей из области ИБ является управление доступом [1].

Используемые на сегодняшний день информационные системы имеют недостаточный уровень ИБ, являясь при этом уязвимыми перед потенциальными атаками и несанкционированным проникновением в информационные ресурсы предприятия. С целью снижения подобного рода рисков в современном мире ведутся активные разработки механизма безопасности, посредством которого выполняется управление процессами взаимодействия пользователей с информационными системами и ресурсами, называемыми управлением доступом. Основная проблема, которой посвящена представленная статья, заключается в необходимости повышения качества и эффективности работы систем, обеспечивающих ИБ на предприятиях и в современных организациях, в частности, в системах электронного документооборота (ЭДО)[2].

Появление крупномасштабных информационных систем обуславливается рядом факторов, связанных с развитием, расширением и цифровизацией современного бизнеса. Одной из основных проблем эффективного функционирования информационных систем на предприятиях является уязвимость перед вредоносными атаками, реализующими угрозы ИБ. Проблемы, связанные с недостаточным уровнем обеспечения ИБ способны привести к нарушению конфиденциальности, потере, уничтожению или изменению информации, а так-

же сбою и колоссальным экономическим потерям. Исходя из этого, актуальность обеспечения информационной безопасности на основе контроля и управления доступом находится на высоком уровне среди задач современного ИТ сегмента.

Комплекс программно-технических средств по защите информации от несанкционированного доступа к системам ЭДО должен включать в себя подсистему управления доступом для всех классов информационных систем, используемых на предприятии. Таким образом, задача адекватного построения политики разграничения доступа является одним из наиболее важных аспектов в задачах обеспечения информационной безопасности. Реализация программно-технических инструментов по разграничению и управлению доступом способна обеспечить эффективное решение задачи защиты информационных ресурсов информационной системы от несанкционированного доступа (рис. 1) [3].

Рис. 1. Модель разграничения доступом в системе комплексного обеспечения ИБ

Основным требованием, предъявляемым к новым технологиям, используемым в системах контроля и управления доступом, является автоматизация процессов построения и разграничения доступа. Исходя из этого, наиболее целесообразно использование подходов, основанных на процессах поддержки принятия решений. Таким образом, в качестве инструмента повышения эффективности функционирования систем управления доступа могут быть задействованы различные интеллектуальные средства, методы иерархий, технология блокчейна и другое. Новые подходы, интегрируемые в системах управления доступом, должны обеспечивать работоспособность системы ИБ по мере увеличения числа находящихся в информационной системе пользователей [4].

Таким образом, видно, что современные информационные системы являются объектом повышенной потенциальной и реальной опасности со стороны злоумышленников в лице хакеров, желающих завладеть личными данными, архивами или иной секретной информацией. Существующие на сегодняшний день средства и методы защиты информации становятся наиболее подверженными удачным взломам и несанкционированному доступу, в результате чего актуализируется роль разработки и интеграции инновационных средств обеспечения защищенности информации. Исходя из этого, наиболее актуальными на сегодняшний день становятся задачи, решения которых позволяют повысить эффективность и рациональность работы современных систем информационной безопасности на основе разработки и интеграции инновационных методов контроля и управления доступом.Одним из наиболее перспективных и инновационных методов управления доступом в информационных системах и системах ЭДО компаний является технология блокчейн [5].

Технология блокчейн представляет собой наиболее широкий класс технологий хранения и синхронизации данных. Основной особенностью управления в данном случае является отсутствие централизации. Каждый из узлов распределительной системы делает записи независимо относительно друг друга. Записи в технологии блокчейн соединяются в инкрементальную цепочку блоков, используя при этом криптографические алгоритмы (рис. 2). Таким образом, блокчейн является децентрализованной базой данных, записи в которой собираются в блоки и связываются на основе криптографических методов. Помимо этого, в блоки включаются хеш-суммы текущего и предыдущего блока. Именно они и являются результатом вычисления криптографических функций [6].

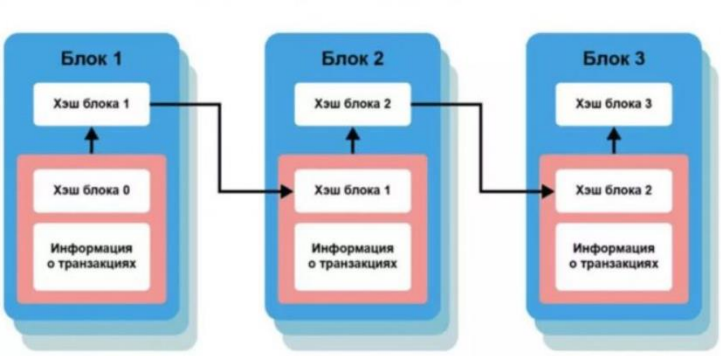

Рис. 2. Принципиальная схема работы технологии блокчейн

Блокчейн, включающий в себя свойства распределенного реестра и блочную структуру данных, реализовывает такие ключевые аспекты информационной безопасности, как целостность и доступность информации. В результате использования децентрализованной типологии наряду с криптографическими методами, манипуляции злоумышленников становятся дорогостоящими и достаточно сложными.

В сетях технологии блокчейн используются специальные криптографические механизмы (SHA-256 и ECDSA и другие), считающиеся достаточно стойкими относительно взлома существующими на сегодняшний день максимальными мощностями вычислительных систем. Таким образом, блокчейн может быть реализован в качестве инструмента контроля и управления доступом, решая задачи информационной безопасности на предприятии. В течение последних лет на ИТ рынке появляется все большее количество проектов кибербезопасности, использующих в своей основе данную технологию. Так, к примеру, разрабатываются системы контроля и управления доступом, системы проверки целостности прошивок устройств Интернета вещей, алгоритмы защиты от DDoS-атак, децентрализованная идентификация и аутентификация и другие [7].

Вопросы, ориентированные на обеспечение информационной безопасности, являются достаточно исследованными и изученными среди многих отечественных и зарубежных исследователей на сегодняшний день. Несмотря на данный факт, в современном мире все еще существуют колоссальные потенциальные угрозы, связанные с хищением или незаконным доступом к информации. Наряду с развивающимися технологиями из ИТ-индустрии развиваются и методы несанкционированного доступа со стороны злоумышленников. Современные организации должны иметь в своем арсенале самые инновационные и эффективные средства обеспечения информационной безопасности. Одними из самых актуальных и возможно эффективных средств предотвращения несанкционированного получения и доступа к информации является электронная подпись.

Понятие электронной подписи в нашей стране появилось относительно недавно, однако история создания данной технологии берет свое начало несколько десятилетий назад. Повсеместное распространение цифровой подписи создает предпосылки производства фальсификации электронных документов. Таким образом, на сегодняшний день актуализируется проблема, решение которой связано с предотвращением фальсификации электронных подписей в современных информационных системах. Авторами в представленной работе решаются такие задачи, как изучение электронной подписи в качестве элемента информационной безопасности, общепринятой схемы цифровой подписи, а также методы защиты от фальсификации электронной подписи [8].

Создание цифровой экономики в Российской Федерации в настоящее время является одной из приоритетных задач государства, направленных на повышение конкурентоспособности страны в целом, качества жизни ее граждан, а также обеспечение экономического роста и национального суверенитета государства. Опираясь на то, что в настоящее время информация в цифровой форме является ключевым фактором производства во всех сферах со-

циально-экономической деятельности, роль электронного документа как способа оформления гражданско-правовых отношений неуклонно возрастает. При этом одной из основных проблем, тормозящих темп развития электронного документооборота, в том числе при осуществлении закупочной деятельности, остается отсутствие доверия к электронным документам.

Лидирующие эксперты отрасли управления документацией констатируют отсутствие в настоящее время надежных решений и алгоритмов, обеспечивающих сохранение в работоспособном состоянии подлинника электронного документа. Поэтому обеспечить долговременную сохранность подлинника электронного документа (75 лет и более) с сохранением его ключевых характеристик, а также юридической значимости и доказательной силы невозможно. Учитывая текущее положение дел, необходимо проводить реформу не только в технической и технологической плоскостях, но и в правовой сфере [9].

Как отмечалось выше, электронный документ получает юридическую силу только после его удостоверения электронной подписью и только обмен такого рода электронными документами может и должен признаваться как обмен документами в целях заключения гражданско-правовых договоров или оформления иных правоотношений. С точки зрения экономических отношений, под доверием понимается динамическая характеристика взаимоотношений, основанная на взаимной искренности и честности, когда партнер или система ведут себя так, как вы от них ожидаете. В этом случае доверие можно рассматривать как гармонизацию межсубъектных отношений в условиях цифровой экономики. Таким образом, можно утверждать, что гармонизация взаимодействия бизнес-структур в условиях цифровой экономики - это неотъемлемое условие существования и нормального функционирования компаний в единой цифровой среде доверия.

Таким образом, одним из наиболее актуальных средств подтверждения подлинности документа и личности является цифровая подпись, связанная с электронным документом. Посредством цифровой подписи предоставляется возможность идентификации подписавшего документ лица и защиты от подделки. Цифровые подписи создаются на основе криптографических преобразований данных с использованием специального ключа, включающем в себя определенную последовательность символов. Данный ключ является аналогом собственноручной подписи на стандартном бумажном носителе, имея при этом равную силу с юридической точки зрения [10].

На основе цифровых подписей устанавливается отсутствие какого-либо рода изменений информации в документе, а также определяются и выявляются подделки. Цифровая подпись имеет достаточно высокий уровень защиты, так как для подбора искомой комбинации символов криптографического узла злоумышленнику требуется выполнить колоссальное число сложных математических операций, что, в свою очередь, может потребовать недели и даже месяцы работы.

Помимо общих проблем, существующих на сегодняшний день в области внедрения систем электронного документооборота на автоматизированных системах предприятий, таких, как консерватизм персонала, недостаточный уровень компетенций в использовании информационных технологий, отсутствие желания обучаться и переобучаться, боязнь прозрачности собственной деятельности для руководства и других, специалисты из данной области сталкиваются и с другими особыми проблемами, которые касаются непосредственно разработки и внедрения систем ЭДО.

Таким образом, на сегодняшний день существует множество проблем, связанных с разработкой, интеграцией и поддержанием стабильной работы систем электронного документооборота на автоматизированных системах современных предприятий. Каждая из данных проблем должна незамедлительно решаться, ведь эффективное решение изученных ранее нюансов и проблемных вопросов позволяет предприятиям повысить свою эффективность и рационализировать рабочую деятельность. В заключение необходимо отметить, что современные предприятия, имеющие в своем составе различные информационные системы и системы электронного документооборота, обязаны обеспечивать должный уровень информа-

ционной безопасности. В противном случае могут появиться колоссальные последствия, связанные с утечкой персональных данных и корпоративной информации, снижение эффективности работы предприятия и множество иных. Таким образом, проблема обеспечения информационной безопасности является первостепенной в рамках развития и цифровизации современных организаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Асеев А.А., Макаров В.В., Наружный В.Е. Проблемы и практика использования электронной цифровой подписи // Экономика и бизнес: теория и практика. 2021. С. 20-23.

2. Пряников М.М., Чугунов А.В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // InternationalJournalofOpenInformationTechnologies. 2017. С. 49-55.

3. Тихонова И.В. Электронный документооборот в бухгалтерском учете: проблемы практического применения // Известия БГУ. 2018. С. 452-460.

4. Харченко О.И. Блокчейн в информационном обществе // Вестник Саратовского государственного социально-экономического университета. 2018. С. 28-30.

5. Spevakov A. G. Methods of identifying a person's personality by morphological signs // Optoelectronic devices and devices in image recognition systems, image processing and symbolic information. Recognition. 2017. С. 1-7.

6. Волошин И.П. Защита информации в информационных системах персональных данных // Информационная безопасность регионов. 2016. С. 12-15.

7. Komlev D.V. Ensuring the protection of personal data as an element of information security: the relevance of the problem and ways to solve it // Interdisciplinary research: the experience of the past, the possibilities of the present, the strategies of the future. 2021. С. 1-9

8. Голикова О.М., Федотова А.И. Способна ли криптовалюта, основанная на технологии «Блокчейн» решить проблемы информационной безопасности финансового сектора? // ИТпортал. 2017. С. 3.

9. Попова Е.В. Электронная цифровая подпись и информационная безопасность малых предприятий // Теория и практика сервиса: экономика, социальная сфера, технологии. 2011. С. 110-118.

10. Gnedkov A.V., Zakharov A.B., Mukhametyeva E.S., Khudorozhkov I.V., Khurmatshina A.A. The use of an electronic signature in the conditions of an educational organization // Scientific and methodological support for assessing the quality of education. 2019. С. 7-19

REFERENCES

1. Aseev A.A., Makarov V.V., Outdoor V.E. *Problems and Practice of Using Electronic Digital Signatures* // Economics and Business: Theory and Practice. 2021. С. 20-23.

2. Pryanikov M.M., Chugunov A.V. *Blockchain as a communication basis for the formation of the digital economy: advantages and problems* // International Journal of Open Information Technologies. 2017. С. 49-55.

3. Tikhonova I.V. *Electronic document flow in accounting: problems of practical application* // Izvestiya BSU. 2018. С. 452-460.

4. Kharchenko O.I. *Blockchain in the Information Society* // Bulletin of the Saratov State Social and Economic University. 2018. С. 28-30.

5. Spevakov A. G. *Methods of identifying a person's personality by morphological signs // Optoelectronic devices and devices in image recognition systems, image processing and symbolic information.* Recognition. 2017. С. 1-7.

6. Voloshin I.P. *Protection of information in information systems of personal data // Information security of regions*. 2016. С. 12-15.

7. Komlev D.V. *Ensuring the protection of personal data as an element of information security: the relevance of the problem and ways to solve it* // Interdisciplinary research: the experience of the past, the possibilities of the present, the strategies of the future. 2021. С. 1-9

8. Golikova O.M., Fedotova A.I. *Is the blockchain-based cryptocurrency capable of solving the information security problems of the financial sector?* // IT portal. 2017. С. 3.

9. Popova E.V. *Electronic digital signature and information security of small enterprises* // Theory and practice of service: economics, social sphere, technologies. 2011. С. 110-118.

10. Gnedkov A.V., Zakharov A.B., Mukhametyeva E.S., Khudorozhkov I.V., Khurmatshina A.A. *The use of an electronic signature in the conditions of an educational organization* // Scientific and methodological support for assessing the quality of education. 2019. С. 7-19

Информация об авторах

Николай Иванович Глухов – к. э. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: gni1953@mail.ru

Виктор Владимирович Иванов – магистрант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск,e-mail: vity.ivanov2010@yandex.ru

Authors

Nikolai Ivanovich Glukhov – Candidate of Science, Associate Professor of the Department of Information Systems and Information Protection, Irkutsk State University of Railway Transport, Irkutsk, e-mail: gni1953@mail.ru.

Victor Vladimirovich Ivanov – Master's student of the Department of Information Systems and Information Protection, Irkutsk State University of Railway Transport, Irkutsk, e-mail: vity.ivanov2010@yandex.ru

Для цитирования

Глухов Н.И., Иванов В.В. Некоторые методы защиты информации при использовании систем электронного документооборота // Информационные технологии и математическое моделирование в управлении сложными системами: электрон. науч. журн. 2021. – №4(12). – С. 47-52 – DOI: 10.26731/2658-3704.2021.4(12).47-52 – Режим доступа: http://ismm-irgups.ru/toma/412-2021, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 27.01.2022)

For citations

Glukhov N.I., Ivanov V.V. Some methods of information protection when using electronic document management systems // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2021. No. 4(12). P. 47-52. DOI: 10.26731/2658-3704.2021.4(12).47-52 [Accessed 27/01/22]