

## **ПРИМЕНЕНИЕ ИНСТРУМЕНТОВ КРИПТОГРАФИИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ**

За 2020 г. в Республике Беларусь сегмент e-commerce показал стремительный рост на 40 % — до 2,3 млрд руб. Доля интернет-продаж в розничном товарообороте страны составила 4,5 %. Но с ростом электронной коммерции также увеличилось и количество правонарушений в сети. Если говорить о Республике Беларусь, то с 2018 по 2020 гг. количество киберпреступлений увеличилось в 10 раз [1]. Для пресечения киберпреступлений в электронной коммерции используются инструменты криптографии. Криптография — это наука об использовании математики для зашифрования и расшифрования данных. Механизмы цифровой подписи основаны на сложных математических задачах — это набор цифр, позволяющий идентифицировать лицо, сформировавшее эту подпись, и обеспечить неизменность документа после подписи. Отправляемый документ шифруется закрытым (ставится электронная подпись), а расшифровывается открытым ключом (позволяет только проверять ЭЦП, но не позволяет подписывать документ).

Для определения связи открытого ключа с закрытым ключом необходима верификация открытого ключа. Для этих целей используются электронные сертификаты. Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с конкретным пользователем и одновременно включает в себя открытый ключ ЭЦП.

Сертификат выдается удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи (содержит электронную цифровую подпись уполномоченного лица удостоверяющего центра) [2].

Таким образом, применение инструментов криптографии позволяет обеспечить такие преимущества для электронной коммерции, как конфиденциальность, контроль и управление доступом, проверка подлинности, целостность данных.

### **Источники**

1. В Беларуси за последние три года количество киберпреступлений увеличилось в 10 раз [Электронный ресурс] // БелТА. — Режим доступа: <https://www.belta.by/society/view/v-belarusi-za-poslednie-tri-goda-kolichestvo-kiberprestuplenij-velichilos-v-10-raz-457812-2021/>. — Дата доступа: 17.11.2021.
2. Мельников, Д. А. Криптографические методы защиты информации : учебник / Д. А. Мельников. — М. : Юрайт, 2016. — 210 с.