



## ЭЛЕКТРОННАЯ КОММЕРЦИЯ И ПУТИ ОБЕСПЕЧЕНИЯ ЕЁ БЕЗОПАСНОСТИ

*Тўлабоева Назокат Дедамирзаевна – преподаватель специальных дисциплин 2-го техникума Янгикурганского района Наманганской области*

*Аннотация: В данной статье анализируются понятие электронной коммерции, её роль в современной экономике, а также вопросы обеспечения информационной безопасности в процессе электронных торговых операций. Освещаются основные киберугрозы, возникающие в системах электронной коммерции, и механизмы их предотвращения. По результатам исследования установлено, что устойчивое развитие электронной коммерции напрямую связано с внедрением современных технологий безопасности.*

*Ключевые слова: электронная коммерция, информационная безопасность, кибербезопасность, шифрование, аутентификация, SSL/TLS, цифровая экономика, электронная подпись, конфиденциальность, фишинг.*

### **Введение**

На сегодняшний день можно с уверенностью сказать, что все развитые страны мира осуществили цифровизацию своей экономики. Распространение компьютерных технологий в западных странах в 60-е годы XX века стало основой развития цифровой экономики и, соответственно, электронной коммерции.

В нашей стране также проводятся масштабные реформы по развитию данной сферы.

В результате стремительного развития цифровых технологий многие отрасли экономики претерпевают трансформацию. В частности, торговые отношения переходят от традиционной формы к электронной.



Электронная коммерция (e-commerce) сегодня является важной составляющей глобальной экономики и охватывает процессы купли-продажи товаров и услуг через интернет.

Вместе с тем значительный объём финансовых и персональных данных, передаваемых в электронных торговых системах, делает вопросы безопасности особенно актуальными.

Под электронной коммерцией понимается осуществление торговли товарами и услугами с использованием компьютерных сетей, таких как интернет.

Она базируется на следующих технологиях:

- мобильная коммерция
- электронные денежные переводы
- управление цепочками поставок
- интернет-маркетинг
- обработка онлайн-транзакций
- электронный обмен данными (EDI)
- системы управления запасами
- автоматизированный сбор данных

Говоря простыми словами, электронная коммерция — это осуществление купли-продажи товаров и услуг посредством электронных средств, включая социальные сети и другие интернет-платформы.

### **Основная часть**

Сущность электронной коммерции и обеспечение безопасности.

Электронная коммерция — это торговая деятельность, осуществляемая с использованием информационно-коммуникационных технологий.

Она подразделяется на следующие направления:

B2B (Business to Business) – торговля между предприятиями

B2C (Business to Consumer) – торговля между предприятием и потребителем



C2C (Consumer to Consumer) – торговля между потребителями

C2B (Consumer to Business) – предоставление услуг потребителем бизнесу

Формы электронной коммерции:

- Электронный обмен данными (Electronic Data Interchange – EDI)

- Электронные переводы денежных средств (Electronic Funds Transfer – EFT)

- Электронная торговля (e-trade)

- Электронные деньги (e-cash)

- Электронный маркетинг (e-marketing)

- Электронный банкинг (e-banking)

- Электронные страховые услуги (e-insurance)

Преимущества электронной коммерции: круглосуточная деятельность (24/7), отсутствие географических ограничений, снижение издержек, быстрота платежей, доступ к глобальному рынку.

Понятие безопасности в электронной коммерции.

Безопасность электронной коммерции — это совокупность технических и организационных мер, направленных на обеспечение конфиденциальности, целостности и доступности информации в процессе онлайн-торговли.

Основные принципы информационной безопасности:

Конфиденциальность (Confidentiality)

Конфиденциальность означает, что доступ к информации имеют только уполномоченные лица. Это уровень защиты персональных и корпоративных данных от передачи третьим лицам — другим организациям или физическим лицам.

В любом бизнесе конфиденциальная информация должна оставаться защищённой и быть доступной только предназначенному получателю. Однако в условиях электронной коммерции эта задача усложняется из-за онлайн-среды.



Обеспечение конфиденциальности включает: защиту электронных записей и файлов от несанкционированного доступа; безопасную передачу данных; защищённое хранение информации.

Для этого применяются такие инструменты, как: шифрование данных, межсетевые экраны (firewall), защищённые протоколы передачи данных.

## 2 Целостность (Integrity)

Целостность означает неизменность и полноту информации. Надёжная система электронной коммерции должна обеспечивать: защиту данных от несанкционированных изменений, корректную аутентификацию пользователей, сохранность информации при передаче.

Одним из базовых шагов является отказ от устаревшего протокола HTTP и переход на защищённый протокол HTTPS.

Кроме того, особое внимание необходимо уделять:

безопасности серверов и административных панелей;

защите платёжных шлюзов;

использованию антивирусных и антишпионских программ;

применению межсетевых экранов;

регулярному обновлению программного обеспечения;

резервному копированию данных.

## 3 Доступность (Availability)

Доступность означает возможность своевременного доступа к системе и данным.

Сетевые сервисы должны функционировать непрерывно. Защита от атак типа DoS (Denial of Service) обеспечивает бесперебойную работу сервисов.

Например, если представить, что кто-то блокирует входные двери компании, то задача сетевой безопасности — обеспечить, чтобы эти «двери» всегда оставались открытыми для законных пользователей.



Системы электронной коммерции подвержены большому количеству рисков по сравнению с традиционными бизнес-системами, поэтому их комплексная защита имеет особое значение. Клиенты, поставщики, сотрудники и другие пользователи ежедневно взаимодействуют с такими системами и ожидают сохранности своих персональных данных. Одной из серьёзных угроз являются хакеры.

Основные наиболее распространённые киберугрозы в системах электронной коммерции

относятся:

- Phishing-атаки
- Вредоносные программы (вирусы, трояны, spyware)
- Кража данных платёжных карт
- DDoS (Distributed Denial of Service) атаки
- Несанкционированный доступ к базам данных

Эти угрозы могут привести к финансовым потерям, снижению доверия клиентов и ущербу деловой репутации компании.

Меры обеспечения безопасности электронной коммерции

Существуют технические и организационные меры защиты обеспечения безопасности электронной коммерции.

□ Технические меры: Использование сертификатов SSL/TLS для шифрования данных; Двухфакторная аутентификация (2FA); Политика надёжных паролей; Межсетевые экраны (Firewall); Антивирусное программное обеспечение; Резервное копирование данных (backup)

Объяснение основных средств защиты простыми словами:

\*Firewall (межсетевой экран) — подобен охраннику у входа: пропускает только доверенный трафик.

\*Антивирус — обнаруживает и устраняет вредоносные программы внутри системы.

\*Шифрование — аналог передачи данных в закрытом конверте.



\*VPN — защищённый «туннель» для передачи конфиденциальной информации.

\*IDS/IPS — система обнаружения и предотвращения вторжений, функционирующая как видеонаблюдение и сигнализация.

2. Организационные меры: Обучение сотрудников и пользователей основам информации-онной безопасности; Разработка и внедрение политики конфиденциальности, Регулярное обновление информационных систем, Внедрение системы аудита и мониторинга безопасности.

Одним из эффективных способов защиты онлайн-информации является использование цифровой подписи. Если документ содержит цифровую подпись, никто не сможет изменить данные незаметно. В случае внесения изменений это можно выявить при проверке подлинности документа. Использование цифровой подписи основано на сочетании криптографии и технологии хеширования сообщений (message digest). Сначала с помощью хеш-функции формируется уникальное значение документа (хеш). Затем это значение шифруется с использованием закрытого ключа отправителя. Таким образом обеспечиваются подлинность, целостность и неотказуемость информации.

С развитием цифровой экономики в Узбекистане электронная коммерция также активно расширяется. Современные онлайн-платёжные системы, такие как: Click, Payme, Uzum создают удобные условия для населения и способствуют развитию онлайн-торговли. Кроме того, сформирована нормативно-правовая база, регулирующая сферу электронной коммерции.

### Заключение

Электронная коммерция является неотъемлемой частью современной экономической системы. Её эффективное и устойчивое развитие тесно связано с обеспечением информационной безопасности.



Только при использовании современных технологий шифрования, систем аутентификации и организационных мер возможно создание надёжной и безопасной инфраструктуры электронной торговли.

Если необходимо, могу оформить весь материал в виде полноценной научной статьи с единым стилем, списком литературы и оформлением по требованиям журнала.