

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Гуломова Дилхумор

Курсант Академии МВД Республики Узбекистан.

Иминов Абдурасул

Научный руководитель: Начальник кафедры цифровых технологий и информационной безопасности Академии Министерства внутренних дел, кандидат физико-математических наук, подполковник

Аннотация: В данной статье рассматривается проблема защиты персональных данных в условиях современного информационного общества. Раскрывается понятие персональных данных, их значение и основные угрозы, связанные с незаконным использованием информации. Особое внимание уделяется вопросам кибербезопасности, методам защиты личных сведений, а также роли государства и организаций в обеспечении конфиденциальности данных.

Ключевые слова: Персональные данные, защита данных, информационная безопасность, конфиденциальность, утечка данных, фишинг, вредоносные программы, шифрование, надежные пароли, двухфакторная аутентификация, цифровая безопасность, личная информация, безопасность в интернете, защита информации, законодательство, информационные технологии.

Annotation: This article discusses the issue of personal data protection in the modern information society. It explains the concept of personal data, its importance, and the main threats related to the illegal use of information. Special attention is paid to cybersecurity, methods of protecting personal information, and the role of governments and organizations in ensuring data confidentiality.

Keywords: Personal data, data protection, information security, privacy, confidential information, data leakage, phishing, malware, encryption, strong passwords, two-factor authentication, digital security, personal information, internet safety, data confidentiality, legislation, information technology.

ВВЕДЕНИЕ

В современном мире информационные технологии стали неотъемлемой частью жизни общества. Практически каждый человек ежедневно использует интернет, мобильные приложения, банковские сервисы, социальные сети и государственные электронные услуги. При этом люди постоянно предоставляют свои личные сведения: фамилию, имя, номер телефона, адрес проживания, паспортные данные, фотографии и другую информацию. Все эти сведения относятся к персональным данным и требуют надежной защиты.

Защита персональных данных является одной из самых актуальных проблем в настоящее время. С развитием цифровых технологий увеличивается количество случаев незаконного использования личной информации, кражи данных, интернет-мошенничества и утечки конфиденциальной информации. Именно поэтому государства, организации и сами граждане должны уделять особое внимание вопросам информационной безопасности.

Цель данной статьи — рассмотреть понятие персональных данных, основные угрозы их безопасности, методы защиты и значение законодательства в данной сфере. Персональные данные — это любая информация, относящаяся к определенному человеку или позволяющая установить его личность. К таким данным относятся:

- фамилия, имя и отчество;
- дата и место рождения;
- адрес проживания;
- номер телефона;
- адрес электронной почты;
- паспортные данные;
- банковские реквизиты;
- фотографии и видеозаписи;
- биометрические данные.

Сегодня персональные данные активно используются государственными учреждениями, банками, медицинскими организациями, интернет-магазинами и социальными сетями. Например, при регистрации на сайте пользователь указывает свои контактные данные, а при оформлении банковской карты предоставляет паспортную информацию. Персональные данные имеют большую ценность, так как с их помощью можно идентифицировать человека, получить доступ к его финансам или личной жизни. Поэтому защита такой информации становится важной задачей как для государства, так и для каждого гражданина. Существует множество угроз, связанных с использованием персональных данных. Наиболее распространенными являются:

1. Утечка информации

Утечка информации — это незаконное или непреднамеренное распространение конфиденциальных данных, при котором личная или служебная информация становится доступной посторонним лицам. Это происходит в результате взлома серверов, ошибок сотрудников или недостаточной защиты информационных систем. В результате личная информация миллионов пользователей может оказаться в открытом доступе.

2. Кибермошенничество

Мошенники используют персональные данные для получения доступа к банковским счетам, оформления кредитов и совершения незаконных операций. Часто злоумышленники применяют методы социальной инженерии, представляясь сотрудниками банков или государственных организаций.

3. Фишинг

Фишинг — это вид интернет-мошенничества, при котором злоумышленники пытаются получить личные данные пользователя: логины, пароли, номера банковских карт и другую конфиденциальную информацию. Человеку отправляют поддельные письма или ссылки на фальшивые сайты, внешне похожие на официальные ресурсы.

4. Вредоносные программы

Компьютерные вирусы и программы-шпионы способны собирать личную информацию пользователя без его ведома. Они могут перехватывать пароли, сообщения и данные банковских карт.

Для защиты персональных данных используются различные методы, направленные на предотвращение утечки информации и незаконного доступа к ней. Одним из основных способов защиты является использование надежных паролей, содержащих буквы, цифры и специальные символы. Также важную роль играет двухфакторная аутентификация, при которой помимо пароля требуется дополнительное подтверждение личности через SMS-код или специальное приложение. Эффективным методом защиты считается шифрование данных, позволяющее сделать информацию недоступной для посторонних лиц. Для обнаружения и удаления вредоносных программ применяются антивирусные системы. Кроме того, доступ к персональным данным должен быть ограничен только уполномоченными лицами. Большое значение имеет и осторожное поведение пользователей в интернете: необходимо избегать подозрительных ссылок, сайтов и сообщений, а также не передавать личную информацию неизвестным людям. Регулярное обновление программного обеспечения и создание резервных копий данных также помогают повысить уровень информационной безопасности и защитить персональные данные от различных угроз.

В Республике Узбекистан защита персональных данных регулируется специальным законодательством. Основным нормативным документом является Закон Республики Узбекистан «О персональных данных», который был принят в 2019 году. Данный закон определяет порядок сбора, хранения, обработки и использования персональных данных граждан, а также устанавливает меры по обеспечению их безопасности.

Согласно законодательству Узбекистана, обработка персональных данных допускается только с согласия человека, кроме случаев, предусмотренных законом. Организации и учреждения обязаны обеспечивать конфиденциальность информации, принимать необходимые технические и организационные меры защиты, а также предотвращать незаконный доступ к данным.

Закон также предоставляет гражданам право знать, какие именно данные о них собираются и как они используются. Человек имеет право требовать исправления, обновления или удаления своих персональных данных в случае их неправильного использования.

За нарушение законодательства о персональных данных предусмотрена ответственность. Незаконный сбор, распространение или использование личной

информации может повлечь административное наказание, штрафы и другие меры ответственности в соответствии с законодательством Республики Узбекистан.

Таким образом, законодательство Узбекистана направлено на защиту прав и свобод граждан, обеспечение конфиденциальности личной информации и повышение уровня информационной безопасности в стране.

Защита персональных данных играет важную роль в современном обществе. От уровня информационной безопасности зависит доверие граждан к государству, банкам, интернет-сервисам и другим организациям.

Надежная защита данных способствует:

- сохранению личной безопасности граждан;
- предотвращению финансовых преступлений;
- защите личной жизни;
- развитию цифровой экономики;
- укреплению доверия пользователей к информационным технологиям.

Таким образом, защита персональных данных является одной из важнейших задач современного общества. В условиях стремительного развития цифровых технологий количество угроз постоянно увеличивается, поэтому необходимо совершенствовать методы информационной безопасности.

Государства принимают специальные законы, организации внедряют современные системы защиты, а пользователи должны соблюдать правила безопасного поведения в интернете. Только совместные усилия государства, компаний и граждан помогут обеспечить надежную защиту персональных данных и сохранить право человека на конфиденциальность и безопасность.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Конституция Республики Узбекистан (ред. 2023 г.).
2. Саидов А.Х., Хамроев Ш.Т. Уголовное право. Общая часть. – Ташкент: ТГЮУ, 2019.
3. Закон Республики Узбекистан от 02.07.2019 г. №ЗРУ-547 «О персональных данных»
4. Закон Республики Узбекистан от 15.04.2022 г. №ЗРУ-764 «О кибербезопасности»
5. Abdazimov, S., L. (2022). Ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimoligini bashoratlash va ulardan himoyalash usuli va modellari. Central Asian Research Journal for Interdisciplinary Studies (CARJIS), 2(5), 109-115.
6. Махкамова М. «Сравнительный анализ регулирования персональных данных: Узбекистан и международные стандарты» // Общество и инновации, 2024.
7. Abdazimov, S., & Djamatov M, (2026). Biometric authentication: modern methods of ensuring information security. Научный Фокус, 3(34), 222-230.
8. Abdazimov, S., & Djamatov M,. (2026). Zamonaviy axborot xavfsizligi tizimlarini loyihalash: ai va iot yondashuvlari ASOSIDA. Научный Фокус, 3(34), 313-321.

9. Азимжонов Д.Д. «Правовые механизмы защиты персональных данных в условиях цифровых угроз Республики Узбекистан» // Центральноазиатский журнал академических исследований, 2025.