Секция «Правовая информатика, информационное и цифровое право»

Особенности правовои защиты личного цифрового кабинета гражданина

Научный руководитель – Воронин Максим Валерьевич

Солоухина Анастасия Сергеевна

Студент (бакалавр)

Финансовый университет, Юридический факультет, Москва, Россия

E-mail: solouhina.anastasiay@yandex.ru

1. Личный кабинет гражданина является частью реализации конституционного права на доступ к государственным услугам и информации. Законодательство РФ обеспечивает защиту персональных данных через нормы Конституции и федеральные законы.

2. Федеральный закон №152-ФЗ "О персональных данных", именно этот нормативный акт устанавливает правила обработки и хранения персональных данных граждан, определяет обязанности операторов, обеспечивающих работу личных кабинетов, а также меры ответственности за нарушение требований закона.

3. Законодательством предусмотрены механизмы контроля над доступом третьих лиц к персональной информации, хранящейся в личном кабинете. Это включает процедуры аутентификации, авторизации и мониторинга действий пользователей.

4. Граждане имеют право требовать конфиденциальности своей личной информации. Государственные органы обязаны обеспечивать сохранение тайны частной жизни, включая данные, находящиеся в личном цифровом кабинете.

5. В случае нарушения прав граждан на неприкосновенность их данных они вправе обратиться в суд для восстановления нарушенных прав и получения компенсации ущерба.

6. Закон предусматривает административную и уголовную ответственность за несанкционированный доступ к личным данным, а также за другие виды нарушений в области информационной безопасности.

7. Персональные данные в личном кабинете защищены методами шифрования, что делает их недоступными для злоумышленников даже в случае перехвата трафика.

8. Для повышения уровня безопасности используется многоступенчатая система входа, включающая пароли, биометрические данные и одноразовые коды подтверждения.

9. Все операции внутри личного кабинета фиксируются в специальных журналах событий, что позволяет отслеживать любые подозрительные активности и предотвращать несанкционированный доступ.

10. Системы анализа поведения пользователей позволяют выявлять отклонения от нормального режима работы, такие как необычные запросы или попытки взлома.

11. Регулярное создание резервных копий данных помогает минимизировать риски потери информации в результате технических сбоев или кибератак.

12. Проводятся регулярные тесты на проникновение и аудит системы безопасности для выявления потенциальных слабых мест и своевременного устранения угроз.

13. Постоянное обновление программного обеспечения и внедрение новых решений в сфере кибербезопасности обеспечивают высокую степень защищенности личных цифровых кабинетов.