

Секция «Компьютерное право и информационная безопасность»

Правовое обеспечение информационной безопасности систем автоматизации зданий

Научный руководитель – Морозов Андрей Витальевич

Трапи Валерия Юрьевна

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

E-mail: trapsh45@mail.ru

Секция «Компьютерное право и информационная безопасность»

Правовое обеспечение информационной безопасности систем автоматизации зданий
Научный руководитель – Морозов Андрей Витальевич
Трапи Валерия Юрьевна

Студент (магистр)

Московский государственный университет имени М. В. Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

Системы автоматизации зданий (Building Automation Systems, BAS) активно внедряются для управления инженерными системами, обеспечения энергосбережения и повышения безопасности. Однако их цифровая природа создает новые угрозы информационной безопасности (ИБ), такие как кибератаки, утечка данных и несанкционированный доступ. В этой связи особое значение приобретает правовое регулирование, направленное на защиту данных и предотвращение инцидентов ИБ.

Системы BAS уязвимы из-за использования IoT-устройств (датчиков, камер, умных замков) и их интеграции с интернетом. Основные угрозы включают удаленное управление объектами злоумышленниками, нарушение конфиденциальности персональных данных пользователей и сбои в работе критической инфраструктуры.

Правовое регулирование:

Для обеспечения ИБ в BAS применяются как национальные законы, так и международные стандарты. В России ключевыми документами являются:

- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ № 127 о защите критической информационной инфраструктуры (КИИ).

Международные стандарты включают ISO/IEC 27001 (управление ИБ) и NIST Cybersecurity Framework. Для объектов с международным взаимодействием важно соблюдать Общий регламент ЕС по защите данных (GDPR).

Меры обеспечения безопасности

Защита BAS достигается за счет технических и организационных мер:

1. Технические меры:

- Использование шифрования данных и защищенных протоколов передачи (HTTPS, VPN).
- Ограничение доступа к системам через пароли и двухфакторную аутентификацию.

- Регулярное обновление программного обеспечения.

2. Организационные меры:

- Разработка политик информационной безопасности.
- Обучение сотрудников правилам работы с данными.
- Проведение аудитов и мониторинга систем.

Особое внимание уделяется защите персональных данных, которые собираются BAS (например, данные о доступе или местоположении пользователей). Операторы обязаны соблюдать законодательство о защите данных, включая их шифрование и минимизацию.

Нарушение требований ИБ влечет административную, гражданско-правовую и уголовную ответственность. К примеру, за утечку данных или несанкционированный доступ к системам могут быть наложены штрафы или предусмотрены другие санкции.

С развитием технологий IoT и концепции "умных городов" требования к ИБ будут ужесточаться. Возможны введение обязательной сертификации устройств для BAS, усиление ответственности производителей IoT-устройств и разработка новых стандартов безопасности.

Информационная безопасность систем автоматизации зданий — это не только техническая задача, но и правовая необходимость. Совершенствование законодательства и внедрение современных стандартов защиты помогут минимизировать риски и обеспечить надежную работу умных зданий.

Источники и литература

- 1) 1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». 2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных». 3. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «О мерах по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». 4. Международный стандарт ISO/IEC 27001:2013 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью». 5. NIST Cybersecurity Framework (Национальный институт стандартов и технологий США).