В.М.АЛЕФИРЕНКО[1], А.Н.МОРОЗОВА[2]

# ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, кандидат технических наук, доцент*

[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, магистрант*

Системы видеонаблюдения получили широкое применение в различных сферах, включая безопасность, контроль доступа и мониторинг. Однако с ростом их использования возрастает и риск несанкционированного доступа к видеоданным. Для эффективной защиты информации необходимо применять различные методы и технические средства.

Одним из ключевых средств защиты информации в системах видеонаблюдения является шифрование данных. Алгоритмы, такие как *AES* (*Advanced Encryption Standard*), преобразуют видеопоток в нечитаемый формат, обеспечивая защиту конфиденциальности и целостности данных [1].

Надежная аутентификация пользователей – еще один ключевой метод защиты. Внедрение многофакторной аутентификации, которая требует от пользователей несколько подтверждений их личности (например, пароль и код из *SMS*), значительно снижает риск несанкционированного доступа. Такой подход позволяет гарантировать, что только авторизованные пользователи могут получить доступ к системе.

Системы видеонаблюдения часто подключаются к интернету, что делает их уязвимыми для кибератак. Использование защищенных протоколов, таких как *HTTPS* и *VPN*, помогает создать безопасные каналы передачи данных. Применение межсетевых экранов и систем предотвращения вторжений *(IPS)* также позволяет фильтровать трафик и выявлять подозрительные активности, предотвращая атаки на систему [2].

Физическая защита оборудования, на котором установлены системы видеонаблюдения, играет важную роль. Установка камер на недоступных высотах и использование защитных корпусов помогают предотвратить несанкционированный доступ к оборудованию. Также стоит рассмотреть внедрение систем сигнализации, которые уведомляют о попытках доступа к камерам [3].

Регулярные обновления программного обеспечения и операционных систем помогают устранить уязвимости, которые могут быть использованы злоумышленниками. Проведение периодических аудитов безопасности позволяет выявлять и устранять потенциальные угрозы, обеспечивая защиту систем видеонаблюдения от новых атак [2].

Защита информации от несанкционированного доступа в системах видеонаблюдения требует комплексного подхода, включая шифрование данных, надежную аутентификацию, использование защищенных сетевых технологий, физическую защиту оборудования и регулярные обновления. Внедрение этих методов

значительно повысит уровень безопасности и защитит конфиденциальные данные от угроз.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Шевченко, К. В. Методы и алгоритмы защиты видеоданных. / К. В. Шевченко – Минск : БГУИР, 2017. – 16 с.

2. Кругль, Г. Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового *CCTV,* 2-е издание / Г. Кругль. – М. : Секьюрити Фокус, 2010. – 640 с.

3. Лыткин, А. IP-Видеонаблюдение. Наглядное пособие / А. Лыткин – Москва : Авторская книга, 2011. – 202 с.