УДК *004.056.55*

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

А.Н. Морозова, А.Ю. Ефремова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В современных условиях системы видеонаблюдения широко используются для обеспечения безопасности и мониторинга различных объектов. Однако с ростом их популярности увеличивается и количество угроз, связанных с несанкционированным доступом к видеоданным. В данной статье рассматриваются основные методы и технологии технической защиты информации в системах видеонаблюдения, включая шифрование данных, аутентификацию пользователей, безопасную конфигурацию сети и физическую защиту оборудования. Особое внимание уделяется современным стандартам и протоколам, таким как ONVIF и DEPA, обеспечивающим совместимость и безопасность компонентов систем видеонаблюдения. Рассмотрены также рекомендации по регулярному обновлению программного обеспечения и управлению уязвимостями для повышения уровня защиты видеоданных.

Ключевые слова: видеонаблюдение; информационная безопасность; шифрование данных; аутентификация; ONVIF; DEPA; кибербезопасность; защита информации; сетевые протоколы; обновление ПО.

TECHNICAL PROTECTION OF INFORMATION IN VIDEO SURVEILLANCE SYSTEMS

A.N. Morozova, A.Y. Yafremava
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. In modern conditions, video surveillance systems are widely used to ensure the security and monitoring of various objects. However, with their growing popularity, the number of threats related to unauthorized access to video data is also increasing. This article discusses the main methods and technologies for the technical protection of information in video surveillance systems, including data encryption, user authentication, secure network configuration, and physical equipment protection. Particular attention is paid to modern standards and protocols, such as ONVIF and DEPA, which ensure compatibility and security of video surveillance system components. Recommendations for regular software updates and vulnerability management are also considered to enhance the level of video data protection.
Keywords: video surveillance; information security; data encryption; authentication; ONVIF; DEPA; cybersecurity; information protection; network protocols; software updates.

Введение

Системы видеонаблюдения стали неотъемлемой частью современных средств обеспечения безопасности, применяясь в различных сферах – от частных домов до крупных промышленных объектов. Однако интеграция таких систем в общие сети и их подключение к интернету повышают риски несанкционированного доступа к видеоданным. Для эффективной защиты информации в системах видеонаблюдения необходимо применять комплексный подход, включающий как технические, так и организационные меры.

Основная часть

Шифрование видеоданных является одним из ключевых методов защиты информации. Применение алгоритмов шифрования, таких как AES (Advanced Encryption Standard), позволяет преобразовать видеопоток в формат, недоступный для несанкционированного просмотра, обеспечивая конфиденциальность и целостность данных. Шифрование должно применяться как при передаче данных по сети, так и при их хранении на носителях.

Аутентификация и управление доступом. Надежная аутентификация пользователей предотвращает несанкционированный доступ к системе видеонаблюдения. Рекомендуется внедрение многофакторной аутентификации, требующей от пользователя предоставления нескольких подтверждений личности, таких как пароль и одноразовый код. Кроме того, необходимо использовать сложные, уникальные пароли для всех устройств и учетных записей, а также регулярно их обновлять:

– безопасная конфигурация сети;

– правильная настройка сети играет важную роль в защите систем видеонаблюдения.

Основные меры включают:

– сегментация сети: разделение сети видеонаблюдения и общей корпоративной сети для ограничения потенциальных путей атаки;

– использование брандмауэров: контроль входящего и исходящего трафика для предотвращения несанкционированного доступа.

– внедрение VPN: обеспечение безопасного удаленного доступа к системе через виртуальные частные сети;

– отключение ненужных сервисов: минимизация потенциальных уязвимостей путем деактивации неиспользуемых сетевых служб и портов.

Стандарты и протоколы безопасности:

– ONVIF (Open Network Video Interface Forum): международная организация, разрабатывающая стандарты для взаимодействия различных устройств в системах безопасности. Использование оборудования, соответствующего стандартам ONVIF, обеспечивает совместимость и повышает уровень безопасности системы;

– DEPA (Distributed Enhanced Processing Architecture): архитектура, предложенная компанией Sony, предусматривающая распределение вычислительных ресурсов между компонентами системы видеонаблюдения. Это позволяет улучшить обработку данных и повысить устойчивость системы к отказам.

Физическая защита оборудования:

– физическая безопасность компонентов системы видеонаблюдения предотвращает прямой доступ злоумышленников к устройствам.

Рекомендуемые меры включают:

– установка камер в труднодоступных местах: размещение оборудования на высоте или в защищенных корпусах для предотвращения физического вмешательства;

– защита кабелей связи: использование бронированных или скрытых каналов прокладки кабелей для предотвращения их повреждения или перехвата сигнала.

Рис. 1. Бронированный кабель
Fig. 1. Armored cable

Контроль доступа в серверные помещения: ограничение физического доступа к серверам и устройствам хранения видеозаписей.

Комплексный подход к защите информации в системах видеонаблюдения включает не только программные, но и аппаратные меры безопасности. Применение современных алгоритмов шифрования, надежной аутентификации и управления доступом, а также использование передовых стандартов и архитектурных решений позволяет минимизировать риски утечек данных. При этом физическая защита оборудования и грамотная конфигурация сети играют важную роль в обеспечении надежности всей системы. Совокупность этих мер позволяет значительно повысить уровень безопасности и устойчивость видеонаблюдения к различным угрозам.

Заключение

Для обеспечения надежной технической защиты информации в системах видеонаблюдения необходимо применять комплексный подход, включающий шифрование данных, многофакторную аутентификацию, безопасную конфигурацию сети, использование стандартов безопасности и физическую защиту оборудования.

Регулярное обновление программного обеспечения и мониторинг уязвимостей также играют важную роль в снижении рисков несанкционированного доступа и обеспечения высокого уровня безопасности видеоданных.

Список использованных источников

1. Тельный А.В. Инженерно-техническая защита информации. Системы охранного телевидения: учебное пособие. – Владимир: ВлГУ. 2013. – 143 с..

2. Березкин Р.В., Власова Г.А. Аспекты применения криптографической защиты информации в системах видеонаблюдения // Технические средства защиты информации: тезисы докладов XVI Белорусско-российской научно-технической конференции, Минск. 5 июня 2018 г. – Минск: БГУИР, 2018. – С. 20.

3. Алефиренко. В. М. Технологии защиты информации от несанкционированного доступа в системах видеонаблюдения / В. М. Алефиренко, А. Н. Морозова // Современные средства связи : материалы XXIX Международной научно-технической конференции, Минск, 31 октября–1 ноября 2024 г. / Белорусская государственная академия связи [и др.] ; редкол : А. О. Зеневич [и др.]. – Минск : БГАС, 2024. – С. 74–75.

References

1. Telny A.V. Engineering and Technical Information Protection. Security Television Systems: Textbook. – Vladimir: VlGU. 2013. – 143 p (in Russian).

2. Beryozkin R.V., Vlasova G.A. Aspects of Cryptographic Information Protection in Video Surveillance Systems // Technical Means of Information Protection: Abstracts of the XVI Belarusian-Russian Scientific and Technical Conference, Minsk, June 5, 2018. – Minsk: BSUIR, 2018. – P. 20 (in Russian).

3. Alefirenko V.M., Morozova A.N. Technologies for Protecting Information from Unauthorized Access in Video Surveillance Systems // Modern Communication Technologies: Proceedings of the XXIX International Scientific and Technical Conference, Minsk, October 31 – November 1, 2024 / Belarusian State Academy of Communications [et al.]; ed. board: A.O. Zenevich [et al.]. – Minsk: BSAC, 2024. – P. 74–75 (in Russian).

Сведения об авторах

Морозова А.Н., магистрантка каф. проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», annamorozova417@gmail.com.
Ефремова А.Ю., ассистент каф. проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», al617e13@gmail.com.

Information about the authors

Morozova A.N., Master's degree student of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", annamorozova417@gmail.com.
Yafremava A.Y., Assistant Professor of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", al617e13@gmail.com.