АНАЛИЗ УЯЗВИМОСТЕЙ И УГРОЗ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Алефиренко Виктор Михайлович,
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

E-mail: alefirenko@bsuir.by

Морозова Анна Николаевна,
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

E-mail: annamorozova417@gmail.com

Аннотация. В статье проведен системный анализ уязвимостей и угроз информационной безопасности современных *IP*-систем видеонаблюдения. Рассмотрены методы несанкционированного доступа к видеоинформации, классифицированные по способу воздействия и физической природе носителя: физическое вмешательство, визуально-оптические, радиочастотные, электромагнитные и сетевые атаки. Предложены обобщенная структурная схема СВН с выделением критичных точек съема и иерархическое «дерево угроз», создающие методологическую основу для анализа рисков и выбора мер защиты.

Ключевые слова: *IP*-системы видеонаблюдения, несанкционированный доступ, каналы утечки информации, классификация угроз, сетевые атаки, «дерево угроз».

Современные *IP*-системы видеонаблюдения (СВН) – сложные программно-аппаратные комплексы, каждый компонент которых может стать объектом атаки. Методы несанкционированного доступа (НСД) к информации разнообразны и направлены как на физический перехват данных, так и на нарушение функционирования системы. На рисунке 1 представлена обобщенная структурная схема СВН с указанием наиболее уязвимых мест и каналов утечки информации.

На схеме цифрами обозначены:

1 – несанкционированное параллельное подключение к линии передачи данных/видеосигнала;

2 – несанкционированное последовательное подключение промежуточного устройства в линию передачи данных/видеосигнала;

3 – подключение к сервисному (технологическому) интерфейсу видеокамеры;

4 – несанкционированный доступ к распределительной коробке (коммутационному узлу);

5 – подключение к коммутационным линиям в коммутационном узле (шкафу связи / зоне размещения сетевого оборудования);

6 – несанкционированное подключение к порту коммутатора (в т.ч. *PoE*-коммутатора);

7 – подключение к интерфейсам видеорегистратора (*NVR/DVR*) / сервера *VMS*;

8 – подключение к локальной вычислительной сети (ЛВС), по которой передаются видеоданные;

9 – несанкционированный доступ к АРМ оператора;

10 – визуально-оптический съем информации с экрана монитора поста наблюдения;

11 – визуальный съем отображаемой информации с интерфейса АРМ оператора;

12 – перехват данных при удаленном доступе через сеть передачи данных;

13 – несанкционированный доступ к архиву видеозаписей;

14 – несанкционированное копирование/экспорт фрагментов видеоархива на носители;

15 – утечка информации за счет побочных электромагнитных излучений и наводок технических средств СВН;

16 – утечка информации за счет наводок информативных сигналов на смежные линии и цепи;

17 – оптическое наблюдение за размещением камер и определение зон обзора/«слепых зон»;

18 – оптический съем сведений о конфигурации СВН (маркировка, индикация, схема подключения);

19 – оптическое воздействие на видеокамеру (засветка/создание помех наблюдению);

20 – несанкционированный доступ к удаленному клиентскому/мобильному устройству доступа.

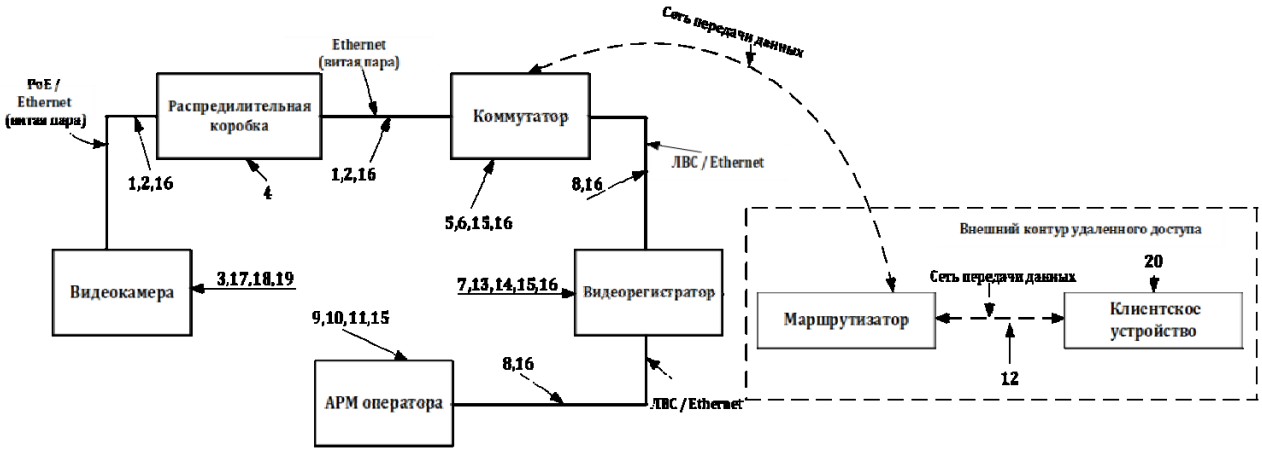

Рис. 1 Обобщенная структурная схема современной *IP*-системы видеонаблюдения с указанием наиболее уязвимых мест и потенциальных каналов утечки информации

Анализ методов НСД целесообразно проводить по способу воздействия и физической природе носителя информации. Исходя из представленной схемы, все методы можно разделить на несколько групп.

Методы, основанные на физическом доступе к компонентам системы.

Наиболее традиционным, но не теряющим актуальности способом является физическое вмешательство в работу компонентов СВН. Злоумышленник, получивший доступ к оборудованию, может осуществить контактное подключение к линии передачи данных. Как показано на рисунке 1, такое подключение может быть параллельным (1), когда устройство подключается к линии без ее разрыва, или последовательным (2), требующим разрыва кабеля и включения в разъем. Также объектами атаки становятся сервисные интерфейсы самих камер (3), порты коммутаторов (6) и видеорегистраторов (7). Помимо перехвата данных, физический доступ позволяет злоумышленнику вывести камеру из строя, перекрыв ее объектив или повредив кабельную трассу, либо создать помехи наблюдению, например, путем засветки мощным источником света (19). Кроме того, доступ к распределительным коробкам и коммутационным узлам (4, 5) дает возможность организовать точку съема в наименее защищенном месте кабельной трассы [1].

Визуально-оптические методы съема информации.

Являясь пассивными, эти методы направлены на получение информации без вмешательства в работу системы. Объектом съема могут выступать непосредственно наблюдаемые объекты, однако для компрометации самой СВН используется анализ размещения камер для выявления так называемых «слепых зон» (17), в которых перемещение нарушителя останется незафиксированным. Кроме того, путем визуального наблюдения за индикацией на оборудовании или его маркировкой (18) можно получить информацию о конфигурации системы. Наиболее критичным с точки зрения последствий является визуально-оптический съем информации непосредственно с экранов мониторов на посту наблюдения (10, 11), который может быть осуществлен как невооруженным глазом, так и с использованием специальных оптических приборов, например, биноклей или монокуляров.

Радиочастотные и электромагнитные методы съема и перехвата информации.

Для беспроводных камер, передающих видеосигнал по радиоканалу, основной угрозой является перехват сигнала с использованием сканирующих приемников или анализаторов спектра. Злоумышленник, настроившись на рабочую частоту передатчика, может не только просматривать видео в реальном времени, но и детектировать сам факт наличия работающего устройства.

Особую сложность для обнаружения представляют так называемые полуактивные закладные устройства, не имеющие собственного передатчика. Принцип их работы основан на модуляции отраженного внешнего зондирующего сигнала [2].

Кроме того, любое активное электронное оборудование, включая видеокамеры, регистраторы и сетевые коммутаторы, является источником побочных электромагнитных излучений и наводок (ПЭМИН). Специализированная аппаратура позволяет перехватывать эти излучения на расстоянии и восстанавливать информативный сигнал (15). Наводки информативных сигналов могут также возникать в цепях питания и заземления, а также на смежных линиях связи (16), что создает дополнительный, часто недооцениваемый, канал утечки.

Сетевые методы атак.

IP-системы видеонаблюдения унаследовали все уязвимости, присущие компьютерным сетям. К ним относятся:

пассивный перехват трафика (сниффинг), позволяющий злоумышленнику, получившему доступ к сегменту сети (8), анализировать передаваемые пакеты данных;

активные атаки, такие как подмена или повторная передача пакетов, атаки типа «человек посередине» (*Man-in-the-Middle*), целью которых является перехват управления или искажение информации;

атаки на отказ в обслуживании (*DoS/DDoS*), направленные на вывод из строя серверов записи, сетевого оборудования или самой камеры путем создания чрезмерной нагрузки;

внедрение вредоносного программного обеспечения (вирусов, программ-вымогателей), которое может привести к блокированию доступа к видеоархивам (13, 14) или их полному уничтожению [1,3,4];

несанкционированный доступ к архивам с целью копирования, модификации или удаления критически важной видеоинформации (13, 14);

использование удаленных клиентских устройств (20) как точки входа для компрометации всей системы.

Многообразие представленных методов несанкционированного доступа убедительно свидетельствует о необходимости применения системного подхода к анализу потенциальных угроз, что позволит в дальнейшем разработать адекватную модель нарушителя.

Для наглядного представления взаимосвязи между целями и действиями потенциального нарушителя, методами НСД и структурными элементами СВН была разработана схема в виде «дерева угроз» (рисунок 2). Она позволяет проследить логическую цепочку от обобщенных каналов утечки информации к конкретным объектам воздействия и возможным негативным последствиям, что существенно облегчает выбор адекватных контрмер.

Схема имеет иерархическую структуру. На верхнем уровне расположены обобщенные каналы утечки информации: визуально-оптический, электромагнитный, акустический, материально-вещественный. Далее, через типы уязвимостей (объективные, субъективные), осуществляется переход к конкретным объектам воздействия внутри СВН: компонентам (камеры, регистраторы, линии связи), рабочим местам операторов, информационным

объектам (видеопотоки, архивы, журналы событий). Нижний уровень схемы отображает последствия реализации угроз: нарушение конфиденциальности, целостности, доступности информации, а также снижение эффективности охраны объекта в целом.

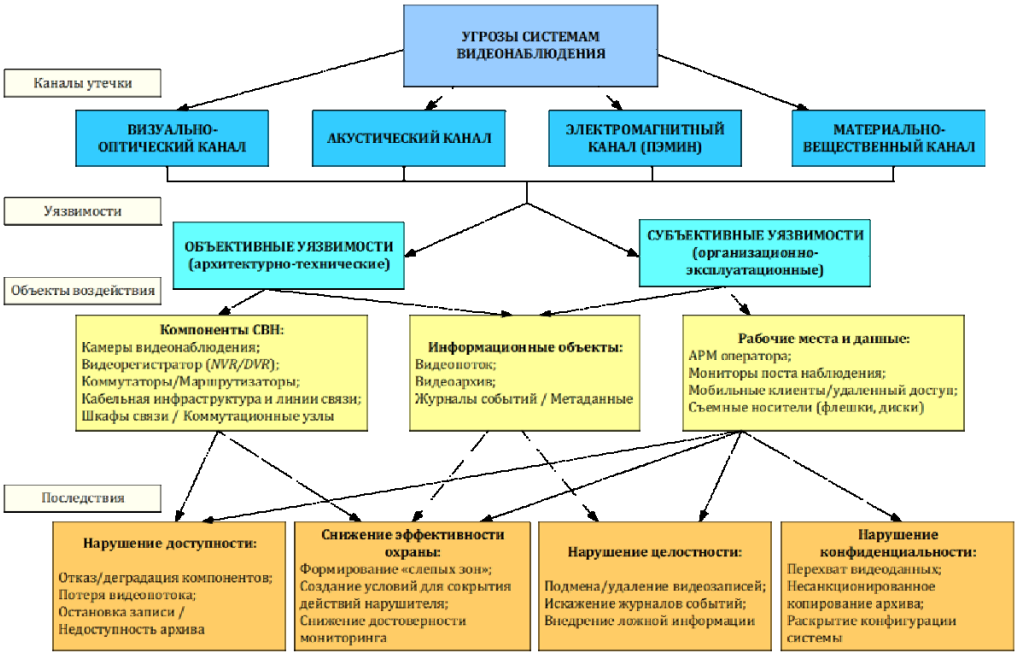

Рис.2 Структурная схема анализа угроз и уязвимостей системы видеонаблюдения «дерево угроз»

Таким образом, предложенная классификация методов НСД и «дерево угроз» создают методологическую основу для последующего анализа рисков и выбора мер защиты при построении конкретного вида системы видеонаблюдения.

Литература:

1. Лыткин, А. *IP*-видеонаблюдение. Наглядное пособие / Александр Лыткин. – [Б. м.], 2011. – 198 с.

2. Лысов, А. В. Организация перехвата информации, обрабатываемой в информационных системах, с помощью радиолокационных систем зондирования / А. В. Лысов // Защита информации. Инсайд. – 2024. – № 3. – С. 20–27.

3. Кругль, Г. Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового ССТУ / Герман Кругль ; пер. с англ. – 2-е изд. – Москва : Секьюрити Фокус, 2010. – 640 с.

4. Пескин, А. Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации / А. Е. Пескин. – 2-е изд. – Москва : Горячая линия – Телеком, 2022. – 360 с.