КИБЕРБЕЗОПАСНОСТЬ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ В УСЛОВИЯХ ОСУЩЕСТВЛЕНИЯ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ

Стародубцев Ю. И.[1], Закалкин П. В.[2], Карасев С. В.[3]

DOI: 10.21681/2311-3456-2025-1-136-146

Цель исследования: *рассмотреть порядок осуществления информационно-технических воздействий на системы видеонаблюдения; оценить существующие требования информационной безопасности к системам видеонаблюдения в Российской Федерации; сформировать обобщенные предложения по обеспечению информационной безопасности существующих систем видеонаблюдения в условиях преднамеренных информационно-технических воздействий.*

Методы исследования: *системный анализ, классификация, сравнительный анализ.*

Полученные результаты: *сформирована обобщенная схема порядка осуществления информационно-технических воздействий на системы видеонаблюдения; сформулированы обобщенные предложения по обеспечению информационной безопасности существующих систем видеонаблюдения; сформулированы предложения по разработке нормативно-правовой документации регуляторами (в области информационной безопасности).*

Научная новизна: *осуществлен анализ конфликтной ситуации в области систем видеонаблюдения, что позволило выявить начальные мероприятия, необходимые для последующего развития информационной безопасности систем видеонаблюдения.*

Ключевые слова: *киберпространство, информационно-технические воздействия, кибербезопасность, видеонаблюдение, угрозы, нарушитель, информационная безопасность.*

Введение

Сложившаяся военно-политическая обстановка привела к началу специальной военной операции (СВО) и, как следствие, к переформатированию мирового порядка. Одним из отличительных факторов данного военного конфликта является возросшая роль киберпространства при ведении военных действий. Резко возросло количество кибератак, осуществляемых противоборствующими сторонами (как открыто, так и посредством своих «прокси» группировок), появились новейшие вооружения, навигация и управление которыми осуществляется посредством киберпространства [1;2].

Киберпространство сформировалось в результате развития систем связи и их трансформации в информационно-коммуникационные системы с последующей интеграцией с навигационными, технологическими, экономическими и другими процессами в различных областях деятельности человечества. Произошла интеграция процессов генерации, сбора, передачи, обработки и распределения информационных ресурсов в автоматизированном и автоматическом режиме, что непрерывно порождает множество новых технологических процессов в различных областях деятельности человечества, в том числе в управлении отдельными индивидуумами, группами и обществом в целом [3–5].

В рамках статьи под киберпространством будем понимать искусственное неоднородное технологическое пространство с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе антагонистических систем управления. При этом свойства киберпространства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей [6–8].

Киберпространство обеспечивает функционирование множества систем различного назначения, в том числе систем наблюдения за общественным порядком, дорожным движением и т.д., которые в своей основе имеют систему видеонаблюдения, контролирующую дорожный трафик, пешеходные зоны городов, общественные места, метро, общественный транспорт и т.д. В своей совокупности эти системы создают своеобразные зоны покрытия страны видеонаблюдением с онлайн трансляцией видео и сохранением потока на центральных серверах.

В первые дни СВО эти системы продолжали свое функционирование, что позволяло вооруженным

1 Стародубцев Юрий Иванович, Заслуженный деятель науки РФ, Заслуженный изобретатель РФ, доктор военных наук, профессор, профессор кафедры, Военная академия связи, Санкт Петербург, Россия. e-mail: prof.starodubtsev@gmail.com, https://orcid.org/0000-0001-5140-4476

2 Закалкин Павел Владимирович, кандидат технических наук, Академия Федеральной Службы Охраны Российской Федерации, Орёл, Россия. e-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586

3 Карасев Станислав Владимирович, Академия Федеральной Службы Охраны Российской Федерации, Орёл, Россия. -mail: ilmaglu@mail.ru

силам Украины (ВСУ) на своей территории в режиме реального времени наблюдать за передвижениями Вооруженных Сил Российской Федерации (ВС РФ) и, соответственно, планировать оборонительные действия, осуществлять ракетно-артиллеристские удары по движущимся колоннам техники, устраивать засады и т.д. В совокупности с системой распознавания лиц и OSINT возможно было определить личности конкретных военнослужащих и организационно-штатную принадлежность их подразделений [12–14].

В 2024 году при заходе на территорию Курской области ВСУ осуществили информационно-технические воздействия (ИТВ) на инфраструктуру РФ и получили доступ как к специализированным системам видеонаблюдения (например, систем наблюдения за общественным порядком, наблюдения за дорожным движением и т.п.), так и отдельных видеокамер частных лиц (web-камеры, установленные в частных домовладениях).

Полученные таким образом разведданные были использованы противником как для планирования боевых действий, так и для нанесения огневых ударов по объектам и подразделениям ВС РФ. В ряде случаев они способствовали вооруженным силам Украины в получении разведывательных данных о дислокации и перемещении подразделений и частей российской армии[4].

Аналогичные ИТВ, осуществляемые посредством киберпространства, приводили к компрометации критических систем на территории РФ. Так, по информации телеграмм-каналов[5] проект «Безопасный регион» был скомпрометирован из-за утечек и уязвимостей. Сотни незарегистрированных и не верифицированных пользователей получили доступ к системе. В результате в сети можно встретить множество видеозаписей с различными чрезвычайными происшествиями, которые были скачаны или пересняты из этой системы. По данным спецслужб ряд преступлений (в том числе резонансные) готовился и координировался по камерам Московской области.

Получается, что системы видеонаблюдения оказали влияние на ход боевых действий и на тактическом уровне значительно облегчали действия ВСУ, а также использовались криминальными элементами для планирования и осуществления противоправных действий.

Основными целями представляемого исследования является:

- рассмотрение обобщенного порядка осуществления информационно-технических воздействий на системы видеонаблюдения;
- рассмотрение существующих требований информационной безопасности к системам видеонаблюдения в РФ;
- формирование обобщенных предложений по обеспечению безопасности существующих систем видеонаблюдения в условиях преднамеренных информационно-технических воздействий.

Обобщенный порядок осуществления информационно-технических воздействий на системы видеонаблюдения

Комплексно обобщив представленную в отрытом доступе информацию[6], была сформирована обобщенная блок-схема порядка осуществления информационно-технических воздействий на системы видеонаблюдения (рисунок 1).

Рис. 1. Обобщенная блок-схема порядка осуществления информационно-технических воздействий на системы видеонаблюдения

Для обнаружения web-камер, подключенных к киберпространству на территории конкретного населенного пункта, используются IP-адреса. Из-за наличия большого количества устройств, подключенных к киберпространству (либо являющихся его ядром), все IP-адреса группируются в рамках заданных диапазонов. При этом, диапазон IP-адресов от региона к региону изменяется. Вся информация об IP-диапазонах является открытой и аккумулируется в базах данных, которыми пользуются в том числе и Интернет-провайдеры.

Выявленные IP-диапазоны анализируются с помощью специализированных поисковых сервисов. Среди наиболее часто используемых специализированных поисковых сервисов основными являются сервисы Shodan, Censys, Zomey. Данные сервисы позволяют обнаруживать, отслеживать и анализировать устройства, подключенные к киберпространству, либо являющиеся его ядром (например, магистральные маршрутизаторы операторов связи).

Информация, предоставляемая вышеописанными сервисами, достаточно подробна и позволяет получить доступ к обнаруженным web-камерам

4 Счет может идти на тысячи: ВСУ взламывают камеры наблюдения в России и шпионят за военными России [Электронный ресурс] URL: https://www.gazeta.ru/tech/2024/08/20/19602931.shtml

5 Телеграмм канал «ВЧК-ОГПУ» [Электронный ресурс] URL: t.me/vchkogpu

6 ИИ и взломанные камеры видеонаблюдения помогают ВСУ успешнее атаковать Россию [Электронный ресурс] URL: https://www.gazeta.ru/tech/news/2024/08/20/23733349.shtml.

(в бесплатных версиях к ограниченному количеству). Платные версии имеют расширенный функционал, позволяют осуществлять настройку фильтрации, а также предоставляют расширенный доступ к информации об обнаруженных устройствах (согласно правилам фильтрации).

Разумно предположить, что информация, предоставляемая данными сервисами (даже на максимальных тарифах), является весьма ограниченной. Максимально полный объем данных в первую очередь предоставляется иностранным спецслужбам и уже после дополнительной обработки и фильтрации по остаточному принципу идет в условно открытый доступ.

Получение доступа к web-камерам в подавляющем большинстве случаев заключается в эксплуатации уязвимостей в программном обеспечении (ПО) камер, либо в вводе установленных по умолчанию логина и пароля в панели администрирования (пароли, установленные производителями по умолчанию). При наличии времени и необходимых ресурсов осуществляется подбор пароля по словарю, либо с использованием специализированных средств подбора пароля.

Получение доступа к большому количеству web-камер дает доступ к видеопотоку большого объема, просмотр и сортировка (исключение – камеры, которые не информативны) которого вручную требует значительного количества времени и человеческих ресурсов. Соответственно, к моменту, когда будет выявлена необходимая информация, обнаружена корреляция между различными камерами (например, построен маршрут передвижения штурмовых групп, колонн техники и т.д.) полученная информация будет неактуальна.

Для повышения эффективности анализа получаемого видеопотока ВСУ использовали искусственный интеллект (ИИ), с помощью которого обрабатывалось полученное с web-камер изображение. Искусственный интеллект позволяет в режиме реального времени отсеивать ненужные записи, фиксировать на нужных материалах корреляции, которые человеком, вероятно, остались бы незамеченными, а также осуществлять в автоматическом режиме добавление вновь обнаруженных web-камер.

Таким образом, используя данный (относительно простой) подход, ВСУ при наступлении на территорию Курской области имели доступ к множеству web-камер, находящихся на территории РФ, и использовали исходящий от них видеопоток в своих интересах.

Исходя из этого задача обеспечения информационной безопасности распределенных систем видеонаблюдения является актуальной и требует тщательного рассмотрения. Исходя из сложившихся подходов к обеспечению информационной безопасности [7–9] прежде всего необходимо рассмотреть нормативно-правовые акты, распространяющие свое действие на системы видеонаблюдения.

Существующие нормативно-правовые акты, распространяющие свое действие на системы видеонаблюдения

Согласно ГОСТ[7] системы видеонаблюдения относятся к комплексным системам безопасности. Помимо этого, имеется ряд других документов и ГОСТ, в той или иной степени регулирующих построение и применение систем видеонаблюдения[8].

Существующие нормативные документы не предполагают унификацию требований для разных типов объектов, но позволяют выделить следующие группы требований к системам видеонаблюдения:

- функциональные требования;
- требования к видеоаналитике и системам хранения;
- требования к зонам наблюдения.

При этом, в явном виде требования по информационной безопасности к системам видеонаблюдения не предъявляются.

В РФ имеется два основных регулятора в области информационной безопасности (ИБ): ФСБ и ФСТЭК. Их задачи представлены в соответствующих руководящих документах[9].[1]

В рамках исследования рассматриваемый вопрос относится к ведению ФСТЭК. Исходя из этого далее будем использовать руководящие документы

7 ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования.

8 1) ГУВО МВД РФ Рекомендации по комплексному оборудованию банков, пунктов обмена валюты, оружейных и ювелирных магазинов, коммерческих и других фирм и организаций техническими средствами охраны, видеоконтроля и инженерной защиты. Типовые варианты Р 78.36.003-99.

2) ГУВО МВД РФ Выбор и применение телевизионных систем видеоконтроля. Рекомендации. Р 78.36.002-99

3) Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности».

4) Постановление Правительства РФ от 25.03.2015 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)».

5) Постановление Правительства РФ от 08.06.2023 № 944 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальных органов, а также подведомственных и относящихся к их сфере деятельности организаций».

6) Постановление Правительства РФ от 26 сентября 2016 г. № 969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности» (с изменениями и дополнениями).

7) Распоряжение Правительства Москвы от 20 июля 2007 г. № 1529-РП «О Концепции по повышению безопасности и антитеррористической защищенности гостиничных предприятий города Москвы».

9 1) Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности».

2) Указ Президента РФ от 16.08.2004 № 1085 (ред. от 08.11.2023) «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

ФСТЭК. Также в рамках статьи будем рассматривать типовую распределенную систему видеонаблюдения критической инфраструктуры РФ[10] (не путать с критической информационной инфраструктурой). В первую очередь это обусловлено ограниченностью объема статьи (дополнительное рассмотрение web-камер во дворах частных домовладений значительно увеличит объем статьи), а также несоизмеримостью затрачиваемого ресурса на добывание информации из частного домовладения и ее ценностью в оперативных масштабах (в условиях ограниченности временного ресурса).

В то же время получение доступа к многофункциональной интеллектуальной системе контроля дорожного движения в заданном регионе даст практически неограниченный разведывательный ресурс без необходимости физического присутствия на территории противника.

Система видеонаблюдения, являясь элементом комплексной системы безопасности, позволяет в режиме реального времени осуществлять визуальный контроль охраняемого объекта и своевременно реагировать на инциденты. Получаемая от web-камер информация в режиме реального времени отражает состояние охраняемого объекта (либо объектов), за которыми ведется наблюдение (автомобильные дороги, железнодорожные пути и другие объекты критической инфраструктуры).

Сама по себе информация, передаваемая с каждой из web-камер по отдельности в явном виде, не относится ни к одному из видов информации, определенных нормативными документами в РФ:

1. Общедоступная информация[11].
2. Информация ограниченного доступа:
   - информация, содержащая сведения, составляющие государственную тайну[12];
   - конфиденциальная информация (служебная тайна, персональные данные)[13].

Получаемая с web-камер информация (например, с камер торгового центра, камер контроля дорожного движения, камер, установленных в общественном транспорте, в метро и т.д.) в явном виде не является общедоступной, в то же время она не относится к информации, содержащей сведения, составляющие государственную тайну, и не относится к конфиденциальной информации[14].

Таким образом, циркулирующая в системах видеонаблюдения информация, в явном виде не относится к первым двум категориям, но при этом вся ее совокупность относится к защищаемой информации. Циркулирующая информация однозначно является информацией ограниченного доступа, но в то же время согласно руководящим документам эта информация не относится ни к одному виду информации, которая подлежит защите.

В данном случае сам процесс отнесения информации к защищаемой требует от регулятора четких рекомендаций, определяющих порядок:

- классификации подобной информации и отнесения ее либо к существующим видам информации, либо создания нового класса информации (например: «информация, циркулирующая в комплексных системах безопасности») для комплексных систем безопасности;
- обеспечения информационной безопасности для комплексных систем безопасности (а в частности, для систем видеонаблюдения на объектах критической инфраструктуры).

Основные угрозы для типовых систем видеонаблюдения. Предлагаемые меры безопасности

На основе открытых источников, включающих в себя руководства администраторов, инструкции по монтажу и эксплуатации и т.п. различных коммерческих структур, предлагающих готовые решения для систем видеонаблюдения (в том числе контроля трафика, пропускного режима и контроля транспорта на объектах) была сформирована типовая структура территориально распределенной системы видеонаблюдения (рис. 2).

Исходя из типовой структуры территориально распределенной системы видеонаблюдения далее сформируем перечень угроз и актуальных мер защиты от них. Для решения задач этого типа ФСТЭК России создал специализированный онлайн инструмент[15], в данный момент проходящий этап опытной эксплуатации. Дальнейшее исследование проводилось с использованием этого инструментария.

На первоначальном этапе формирования перечня угроз и актуальных мер защиты ФСТЭК предполагает определение негативных последствий, которые могут возникнуть в результате нарушения функционирования системы видеонаблюдения. Из предлагаемого ФСТЭК перечня негативных последствий (52 негативных последствия), напрямую с системами видеонаблюдения связано 24 последствия. Также к негативным были отнесены не явные на первый взгляд последствия. Например: «Н.1 Угроза жизни или здоровью», «Н.31 Причинение ущерба жизни

10 Что такое критическая инфраструктура [Электронный ресурс] URL: https://esg.kaspersky.com/ru/future-tech/what-is-critical-infrastructure

11 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

12 Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1.

13 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

14 Перечень нормативных актов, относящих сведения к категории ограниченного доступа (Материал подготовлен специалистами КонсультантПлюс) [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_93980/

15 Банк данных угроз безопасности информации [Электронный ресурс] URL: https://bdu.fstec.ru/threat-section/potential

Рис. 2. Типовая структура территориально распределенной системы видеонаблюдения

и здоровью людей», были выбраны как негативные последствия, т.к. с помощью систем видеонаблюдения ВСУ осуществляли контроль за перемещением штурмовых групп, отдельных подразделений ВС РФ и т.д., наносили ракетно-артиллеристские удары и т.п.

В качестве основных актуальных угроз (ФСТЭК выделяет 11 угроз) для систем видеонаблюдения были выбраны:

- УБИ.1 – Угроза утечки информации.
- УБИ.2 – Угроза несанкционированного доступа.
- УБИ.5 – Угроза удаления информационных ресурсов.
- УБИ.6 – Угроза отказа в обслуживании.
- УБИ.7 – Угроза ненадлежащего (нецелевого) использования.
- УБИ.8 – Угроза нарушения функционирования (работоспособности).
- УБИ.9 – Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника.
- УБИ.11 – Угроза несанкционированного массового сбора информации.

Угрозы УБИ.3 (угроза несанкционированной модификации (искажения)), УБИ.4 (угроза несанкционированной подмены) и УБИ.10 (угроза распространения противоправной информации) теоретически возможны, но их реализация достаточно сложна и ресурсозатратна, в связи с чем эти угрозы не рассматривались.

На этапе выбора объекта воздействия были отобраны следующие объекты, свойственные для распределенных систем видеонаблюдения:

- 0.1 – Автоматизированное рабочее место;
- 0.2 – Сервер;
- 0.3 – Периферийное оборудование;
- 0.4 – Устройство хранения данных;
- 0.5 – Устройство интернета-вещей;
- 0.6 – Активное сетевое оборудование;
- 0.11 – Информация (данные), содержащаяся в системах и сетях;
- 0.12 – Физические линии связи.

Объекты воздействия 0.7 Обеспечивающие системы, 0.8 Телефония (VoIP, GSM), 0.9 Средства защиты информации, 0.10 Мобильное устройство – вынесены в ограничения, т.к. не являются обязательными для систем видеонаблюдения.

На следующем шаге было осуществлено уточнение компонент объектов воздействия и определен тип нарушителей. Согласно руководящим документам, ФСТЭК выделяет 4 уровня возможностей нарушителя[16] (рис. 3).

В рассматриваемой нами ситуации нарушителями являются специальные службы иностранных государств, т.е. согласно рис. 3 – нарушитель, обладающий высокими возможностями. Однако, как правило, для защиты от специальных служб иностранных

16 Банк данных угроз безопасности информации [Электронный ресурс] URL: https://bdu.fstec.ru/threat-section/potential

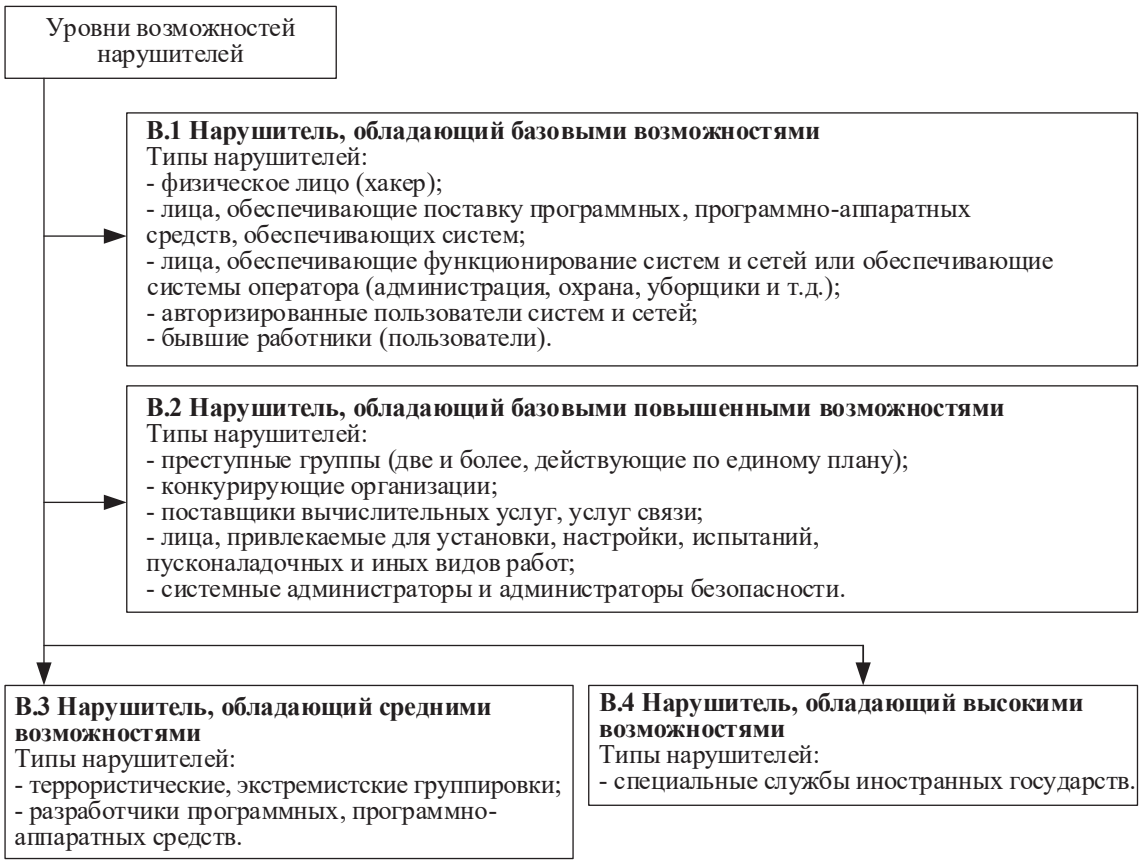

Рис. 3. Уровни возможностей нарушителей (согласно ФСТЭК)

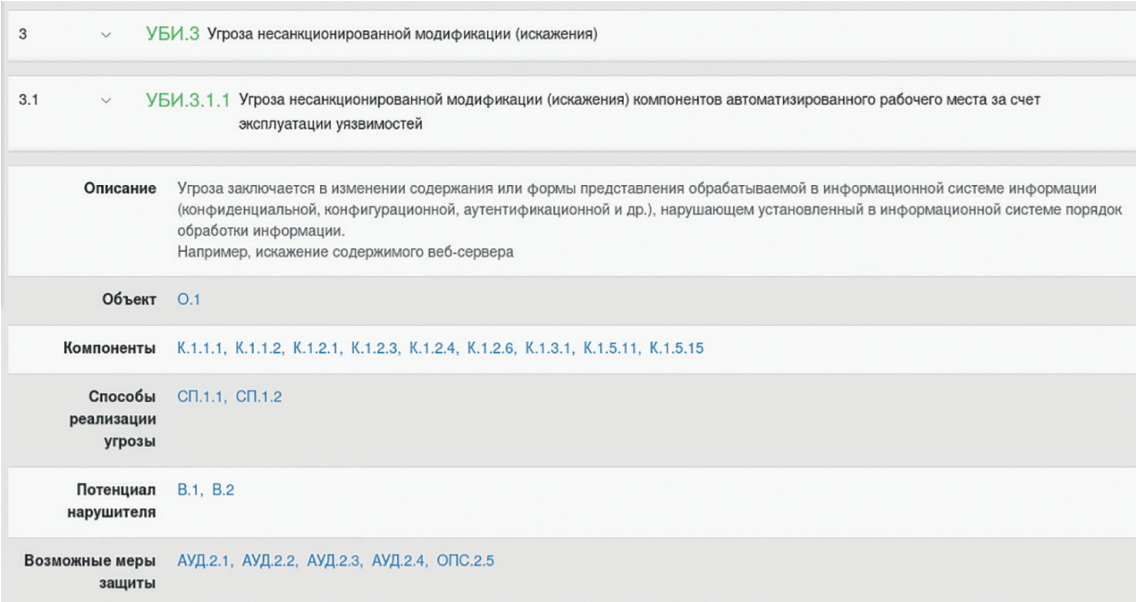

Рис. 4. Пример описания угроз безопасности информации

государств необходимо реализовать обширный перечень требований информационной безопасности с соответствующими значительными финансовыми вложениями. Также для иностранных спецслужб интерес представляет ограниченное число систем видеонаблюдения, которое существенно меньше общего количества существующих систем. Исходя из этого нарушитель В.4 был вынесен в ограничения. Далее в качестве нарушителей будем рассматривать нарушителей В.1, В.2 и В.3.

Исходя из описанных выше исходных данных, программным средством ФСТЭК был сформирован

перечень возможных угроз безопасности информации. Пример описания угрозы представлен на рис. 4.

Полученные результаты были сохранены в файл формата *.JSON и посредством специально разработанного для этой задачи парсера были преобразованы в 39 страничный документ формата *.pdf . Учитывая ограниченный объем статьи, далее будут представлены основные результаты исследования.

Согласно руководящим документам ФСТЭК с учетом описанных выше исходных данных, для распределенных систем видеонаблюдения актуальными угрозами являются угрозы, представленные в Таблице 1.

Таблица 1.

Актуальные угрозы безопасности

Угроза	Номер угрозы
Угроза утечки информации	УБИ.1.1.1[17], УБИ.1.1.2, УБИ.1.1.3, УБИ.1.1.4, УБИ.1.1.5, УБИ.1.1.7, УБИ.1.1.8, УБИ.1.1.9, УБИ.1.1.10, УБИ.1.1.11, УБИ.1.1.12, УБИ.1.1.13, УБИ.1.1.16, УБИ.1.1.18, УБИ.1.1.24, УБИ.1.1.25, УБИ.1.2.1, УБИ.1.2.2, УБИ.1.2.3, УБИ.1.2.4, УБИ.1.2.5, УБИ.1.2.7, УБИ.1.2.8, УБИ.1.2.9, УБИ.1.2.10, УБИ.1.2.11, УБИ.1.2.12, УБИ.1.2.13, УБИ.1.2.16, УБИ.1.2.18, УБИ.1.2.25, УБИ.1.3.1, УБИ.1.3.2, УБИ.1.3.3, УБИ.1.3.4, УБИ.1.3.5, УБИ.1.3.10, УБИ.1.3.18, УБИ.1.4.1, УБИ.1.4.2, УБИ.1.4.3, УБИ.1.4.4, УБИ.1.4.5, УБИ.1.4.10, УБИ.1.4.18, УБИ.1.5.1, УБИ.1.5.2, УБИ.1.5.3, УБИ.1.5.4, УБИ.1.5.5, УБИ.1.5.10, УБИ.1.5.18, УБИ.1.6.1, УБИ.1.6.2, УБИ.1.6.3, УБИ.1.6.4, УБИ.1.6.5, УБИ.1.6.7, УБИ.1.6.10, УБИ.1.6.11, УБИ.1.6.16, УБИ.1.6.18, УБИ.1.6.25, УБИ.1.12.3, УБИ.1.12.7, УБИ.1.12.10, УБИ.1.12.11, УБИ.1.12.16, УБИ.11.1.1, УБИ.11.1.2, УБИ.11.1.3, УБИ.11.1.4, УБИ.11.1.5, УБИ.11.1.7, УБИ.11.1.8, УБИ.11.1.9, УБИ.11.1.13, УБИ.11.1.18, УБИ.11.1.25, УБИ.11.2.1, УБИ.11.2.2, УБИ.11.2.3, УБИ.11.2.4, УБИ.11.2.5, УБИ.11.2.7, УБИ.11.2.8, УБИ.11.2.9, УБИ.11.2.13, УБИ.11.2.18, УБИ.11.2.25, УБИ.11.3.1, УБИ.11.3.2, УБИ.11.3.3, УБИ.11.3.4, УБИ.11.3.5, УБИ.11.3.9, УБИ.11.3.18, УБИ.11.5.1, УБИ.11.5.2, УБИ.11.5.3, УБИ.11.5.4, УБИ.11.5.5, УБИ.11.5.9, УБИ.11.5.18, УБИ.11.6.1, УБИ.11.6.2, УБИ.11.6.3, УБИ.11.6.4, УБИ.11.6.5, УБИ.11.6.7, УБИ.11.6.9, УБИ.11.6.18, УБИ.11.6.25
Угроза несанкционированного доступа	УБИ.2.1.1, УБИ.2.1.2, УБИ.2.1.3, УБИ.2.1.4, УБИ.2.1.5, УБИ.2.1.7, УБИ.2.1.10, УБИ.2.1.13, УБИ.2.1.16, УБИ.2.1.17, УБИ.2.1.18, УБИ.2.1.19, УБИ.2.1.23, УБИ.2.1.24, УБИ.2.1.25, УБИ.2.2.1, УБИ.2.2.2, УБИ.2.2.3, УБИ.2.2.4, УБИ.2.2.5, УБИ.2.2.7, УБИ.2.2.10, УБИ.2.2.13, УБИ.2.2.16, УБИ.2.2.17, УБИ.2.2.18, УБИ.2.2.19, УБИ.2.2.23, УБИ.2.2.25, УБИ.2.3.1, УБИ.2.3.2, УБИ.2.3.3, УБИ.2.3.4, УБИ.2.3.5, УБИ.2.3.10, УБИ.2.3.17, УБИ.2.3.18, УБИ.2.3.23, УБИ.2.4.1, УБИ.2.4.2, УБИ.2.4.3, УБИ.2.4.4, УБИ.2.4.5, УБИ.2.4.10, УБИ.2.4.17, УБИ.2.4.18, УБИ.2.4.23, УБИ.2.5.1, УБИ.2.5.2, УБИ.2.5.3,УБИ.2.5.4, УБИ.2.5.5, УБИ.2.5.10, УБИ.2.5.17, УБИ.2.5.18, УБИ.2.5.23, УБИ.2.6.1, УБИ.2.6.2, УБИ.2.6.3, УБИ.2.6.4, УБИ.2.6.5, УБИ.2.6.7, УБИ.2.6.10, УБИ.2.6.16, УБИ.2.6.17, УБИ.2.6.18, УБИ.2.6.23, УБИ.2.6.25, УБИ.2.12.3, УБИ.2.12.7, УБИ.2.12.10, УБИ.2.12.16, УБИ.2.12.17.
Угроза удаления информационных ресурсов	УБИ.5.1.1, УБИ.5.1.2, УБИ.5.1.3, УБИ.5.1.4, УБИ.5.1.5, УБИ.5.1.10, УБИ.5.1.13, УБИ.5.1.14, УБИ.5.1.15, УБИ.5.1.16, УБИ.5.1.18, УБИ.5.1.19, УБИ.5.1.21, УБИ.5.1.23, УБИ.5.1.24, УБИ.5.1.25, УБИ.5.2.1, УБИ.5.2.2, УБИ.5.2.3, УБИ.5.2.4, УБИ.5.2.5, УБИ.5.2.10, УБИ.5.2.13, УБИ.5.2.14, УБИ.5.2.15, УБИ.5.2.16, УБИ.5.2.18, УБИ.5.2.19, УБИ.5.2.21, УБИ.5.2.23, УБИ.5.2.25, УБИ.5.4.1, УБИ.5.4.2, УБИ.5.4.3, УБИ.5.4.4, УБИ.5.4.5, УБИ.5.4.10, УБИ.5.4.18, УБИ.5.4.23, УБИ.5.6.1, УБИ.5.6.2, УБИ.5.6.3, УБИ.5.6.4, УБИ.5.6.5, УБИ.5.6.10, УБИ.5.6.14, УБИ.5.6.16, УБИ.5.6.18, УБИ.5.6.23, УБИ.5.6.25, УБИ.5.12.3, УБИ.5.12.10, УБИ.5.12.14, УБИ.5.12.16

17 УБИ – угроза безопасности информации, 1.1.1 – номер угрозы в банке угроз информационной безопасности ФСТЭК

Угроза	Номер угрозы
Угроза отказа в обслуживании	УБИ.6.1.1, УБИ.6.1.2, УБИ.6.1.4, УБИ.6.1.5, УБИ.6.1.14, УБИ.6.1.15, УБИ.6.1.19, УБИ.6.1.21, УБИ.6.1.23, УБИ.6.1.24, УБИ.6.1.25, УБИ.6.2.1, УБИ.6.2.2, УБИ.6.2.4, УБИ.6.2.5, УБИ.6.2.14, УБИ.6.2.15, УБИ.6.2.19, УБИ.6.2.21, УБИ.6.2.23, УБИ.6.2.25, УБИ.6.3.1, УБИ.6.3.2, УБИ.6.3.4, УБИ.6.3.5, УБИ.6.3.14, УБИ.6.3.23, УБИ.6.4.1, УБИ.6.4.2, УБИ.6.4.4, УБИ.6.4.5, УБИ.6.4.14, УБИ.6.4.23, УБИ.6.5.1, УБИ.6.5.2, УБИ.6.5.4, УБИ.6.5.5, УБИ.6.5.14, УБИ.6.5.23, УБИ.6.6.1, УБИ.6.6.2, УБИ.6.6.4, УБИ.6.6.5, УБИ.6.6.7, УБИ.6.6.14, УБИ.6.6.23, УБИ.6.6.25, УБИ.6.12.7, УБИ.6.12.14
Угроза ненадлежащего (нецелевого) использования	УБИ.7.1.1, УБИ.7.1.2, УБИ.7.1.4, УБИ.7.1.5, УБИ.7.1.11, УБИ.7.1.18, УБИ.7.1.19, УБИ.7.1.23, УБИ.7.1.24, УБИ.7.1.25, УБИ.7.2.1, УБИ.7.2.2, УБИ.7.2.4, УБИ.7.2.5, УБИ.7.2.11, УБИ.7.2.18, УБИ.7.2.19, УБИ.7.2.23, УБИ.7.2.25, УБИ.7.4.1, УБИ.7.4.2, УБИ.7.4.4, УБИ.7.4.5, УБИ.7.4.18, УБИ.7.4.23, УБИ.7.5.1, УБИ.7.5.2, УБИ.7.5.4, УБИ.7.5.5, УБИ.7.5.18, УБИ.7.5.23, УБИ.7.6.1, УБИ.7.6.2, УБИ.7.6.4, УБИ.7.6.5, УБИ.7.6.11, УБИ.7.6.18, УБИ.7.6.23, УБИ.7.6.25
Угроза нарушения функционирования (работоспособности)	УБИ.8.1.1, УБИ.8.1.2, УБИ.8.1.4, УБИ.8.1.5, УБИ.8.1.13, УБИ.8.1.14, УБИ.8.1.15, УБИ.8.1.16, УБИ.8.1.18, УБИ.8.1.19, УБИ.8.1.21, УБИ.8.1.23, УБИ.8.1.24, УБИ.8.1.25, УБИ.8.2.1, УБИ.8.2.2, УБИ.8.2.4, УБИ.8.2.5, УБИ.8.2.13, УБИ.8.2.14, УБИ.8.2.15, УБИ.8.2.16, УБИ.8.2.18, УБИ.8.2.19, УБИ.8.2.21, УБИ.8.2.23, УБИ.8.2.25, УБИ.8.3.1, УБИ.8.3.2, УБИ.8.3.4, УБИ.8.3.5, УБИ.8.3.18, УБИ.8.3.23, УБИ.8.4.1, УБИ.8.4.2, УБИ.8.4.4, УБИ.8.4.5, УБИ.8.4.18, УБИ.8.4.23, УБИ.8.5.1, УБИ.8.5.2, УБИ.8.5.4, УБИ.8.5.5, УБИ.8.5.18, УБИ.8.5.23, УБИ.8.6.1, УБИ.8.6.2, УБИ.8.6.4, УБИ.8.6.5, УБИ.8.6.7, УБИ.8.6.16, УБИ.8.6.18, УБИ.8.6.23, УБИ.8.6.25, УБИ.8.7.1, УБИ.8.7.2, УБИ.8.7.4, УБИ.8.7.5, УБИ.8.7.18, УБИ.8.7.23, УБИ.8.12.7, УБИ.8.12.16
Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника	УБИ.9.11.2, УБИ.9.11.4, УБИ.9.11.5, УБИ.9.11.13, УБИ.9.11.25
Угроза несанкционированного массового сбора информации	УБИ.11.1.1, УБИ.11.1.2, УБИ.11.1.3, УБИ.11.1.4, УБИ.11.1.5, УБИ.11.1.7, УБИ.11.1.8, УБИ.11.1.9, УБИ.11.1.13, УБИ.11.1.18, УБИ.11.1.25, УБИ.11.2.1, УБИ.11.2.2, УБИ.11.2.3, УБИ.11.2.4, УБИ.11.2.5, УБИ.11.2.7, УБИ.11.2.8, УБИ.11.2.9, УБИ.11.2.13, УБИ.11.2.18, УБИ.11.2.25, УБИ.11.3.1, УБИ.11.3.2, УБИ.11.3.3, УБИ.11.3.4, УБИ.11.3.5, УБИ.11.3.9, УБИ.11.3.18, УБИ.11.5.1, УБИ.11.5.2, УБИ.11.5.3, УБИ.11.5.4, УБИ.11.5.5, УБИ.11.5.9, УБИ.11.5.18, УБИ.11.6.1, УБИ.11.6.2, УБИ.11.6.3, УБИ.11.6.4, УБИ.11.6.5, УБИ.11.6.7, УБИ.11.6.9, УБИ.11.6.18, УБИ.11.6.25

Актуальными способами реализации угроз являются:

1. Эксплуатация уязвимостей (СП.1.1[18], СП.1.2).
2. Атака типа «человек посередине» (СП.10.1, СП.10.2, СП.10.4, СП.10.7).
3. Применение скрытых каналов (СП.11.1).
4. Считывание вводимой и выводимой информации (СП.12.1, СП.12.3, СП.12.6, СП.12.9).
5. Реализация социальной инженерии (СП.13.1, СП.13.2, СП.13.3, СП.13.4, СП.13.5, СП.13.6, СП.13.7, СП.13.8).
6. Атака типа «отказ в обслуживании» (СП.14.1, СП.14.10, СП.14.2, СП.14.3, СП.14.4, СП.14.5, СП.14.6, СП.14.7, СП.14.8).
7. Шифрование данных (СП.15.1, СП.15.2).
8. Нарушение изоляции (СП.16.2, СП.16.3).
9. Подбор (восстановление) аутентификационной информации (СП.17.1, СП.17.10, СП.17.11, СП.17.2, СП.17.3, СП.17.8, СП.17.9).

18 СП – способ реализации угрозы, 1.1 – номер угрозы в банке угроз информационной безопасности ФСТЭК

10. Использование недостатков механизмов разграничения доступа (СП.18.1, СП.18.2).
11. Модификация ОС (подмена системных файлов, внедрение вредоносного кода в системные процессы и ядро ОС) (СП.19.1, СП.19.2, СП.19.3, СП.19.4).
12. Использование недостатков конфигурации (СП.2.1, СП.2.10, СП.2.11, СП.2.2, СП.2.3, СП.2.4, СП.2.6, СП.2.7, СП.2.8, СП.2.9).
13. Повреждение данных (СП.21.2, СП.21.3).
14. Модификация (подмена) прошивки (микропрограммы) (СП.23.1, СП.23.2).
15. Физическое воздействие (СП.24.2, СП.24.3).
16. Использование недостатков архитектуры (СП.3.1).
17. Внедрение вредоносного программного обеспечения (СП.4.1, СП.4.10, СП.4.12, СП.4.2, СП.4.3, СП.4.4, СП.4.5, СП.4.6, СП.4.8, СП.4.9).
18. Внедрение программных и аппаратных закладок (СП.5.1, СП.5.2, СП.5.3, СП.5.4, СП.5.5, СП.5.7).
19. Прослушивание (захват) сетевого трафика (СП.7.1, СП.7.2, СП.7.3, СП.7.4, СП.7.5, СП.7.6, СП.7.7).
20. Сканирование сетевой инфраструктуры (СП.8.1, СП.8.2, СП.8.4, СП.8.5, СП.8.6).
21. Изучение информации о системе (СП.9.1, СП.9.2, СП.9.3, СП.9.4, СП.9.5, СП.9.6, СП.9.7).

С учетом актуальных угроз и способов их реализации программным средством ФСТЭК был сформирован перечень актуальных мер защиты в количестве 221 меры.

Представленное исследование показывает, что обеспечение информационной безопасности систем видеонаблюдения не является тривиальной задачей, а требует большого количества мер защиты и как следствие значительных финансовых вложений. Но даже при наличии финансовой составляющей имеются объективные причины, не позволяющие одномоментно обеспечить информационную безопасность систем видеонаблюдения. Среди основных причин можно выделить:

- отсутствие нормативной базы, однозначно определяющей порядок обеспечения информационной безопасности комплексных систем безопасности;
- необходимость подготовки (доподготовки) специалистов, обладающих соответствующими компетенциями в области обеспечения информационной безопасности систем комплексной безопасности.

Выводы

Результаты исследования показывают, что для защиты систем видеонаблюдения необходимо реализовать достаточно обширный список мероприятий. Однако необходимо учитывать, что исследование ориентировано на нарушителя В.3, и для нарушителей В.1 и В.2 перечень мероприятий будет существенно уменьшен.

Тем не менее одномоментное введение требований по информационной безопасности (описанных в результатах исследования) для систем видеонаблюдения по объективным причинам для большинства систем будет сложно реализуемо. В связи с чем, необходим переходной этап с пошаговым усилением требований ИБ и постепенной тестовой эксплуатацией систем с функционирующей на них системой информационной безопасности.

Касательно нормативной базы применительно к системам видеонаблюдения необходима разработка:

- нормативных документов, определяющих требования информационной безопасности к системам видеонаблюдения;
- типовых моделей угроз и нарушителя для систем видеонаблюдения;
- методических документов, позволяющих осуществлять классификацию информации, циркулирующей в системах видеонаблюдения и отнесения ее либо к существующим видам информации, либо к созданию нового класса информации (например: «информация, циркулирующая в комплексных системах безопасности») для комплексных систем безопасности;
- методических рекомендаций, регулирующих порядок обеспечения информационной безопасности для комплексных систем безопасности (а в частности, для систем видеонаблюдения на объектах критической инфраструктуры);
- методических рекомендаций, регулирующих порядок проведения тематических исследований программного обеспечения используемого в системах видеонаблюдения на отсутствие недекларированных возможностей.

Литература

1. *Стародубцев Ю. И., Закалкин П. В. Структурно-функциональный анализ конфликтной ситуации между государственной системой обеспечения информационной безопасности и иностранной системой деструктивных воздействий // Вопросы кибербезопасности. 2024. №4(62). С.82–91. DOI: 10.21681/2311-3456-2024-4-82-91.*
2. *Иванов С. А. Трансформация роли единой сети электросвязи Российской Федерации в системе военного управления в результате реализации процессов цифровой трансформации и глобализации // Вопросы радиоэлектроники. Серия: Техника телевидения. 2021. №3. С.17–23.*
3. *Иванов С. А. Устойчивость сетей связи общего пользования в условиях глобализации // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 86–90. DOI: 10.24412/2071-6168-2021-9-86-90.*

4. Коцыняк М.А., Лаута О.С., Нечепуренко А.П. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1–2 (127-128). С. 58–62.
5. Бречко А.А., Сазыкин А.М. Проблема управления параметрами киберпространства в интересах субъектов критической информационной инфраструктуры Российской Федерации // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2022. № 5–6 (167-168). С. 36–43.
6. Закалкин П.В. Аспекты использования киберпространства в интересах корпоративных систем управления // Труды Научно-исследовательского института радио. 2021. № 4. С. 23–32. DOI: 10.34832/NIIR.2021.7.4.003.
7. Starodubtsev Y.I., Balenko E.G., Zakalkin P.V., Fedorov V.H. Change dynamics for forms and opportunities of centers of power under globalization // В сборнике: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. С. 9271172. DOI: 10.1109/FarEastCon50210.2020.9271172
8. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Многовекторный конфликт в киберпространстве как предпосылка формирования нового вида вооруженных сил // Военная мысль. 2021. №12. С. 126–135.
9. Hwang Y.-W., Lee I.-Y., Kim H., Lee H., Kim D. Current status and security trend of OSINT // Wireless Communications and Mobile Computing. 2022. Т. 2022. С. 1290129. DOI: 10.1155/2022/1290129.
10. Махнин В.Л. О законах и формах войны // Вестник академии военных наук. 2024. №2(87). С.45–53.
11. Гаврилов А.Д., Грудинин И.В., Майбуров Д.Г., Новиков В.А. Два года специальной военной операции: некоторые итоги, вероятные перспективы // Вестник академии военных наук. 2024. №2(87). С. 54–64.
12. Белов А.С., Добрышин М.М., Шугуров Д.Е. Научно-методический подход к оцениванию качества систем обеспечения информационной безопасности // Приборы и системы. Управление, контроль, диагностика. 2022. № 11. С. 34–40. DOI: 10.25791/pribor.11.2022.1373.
13. Добрышин М.М. Выбор структуры и механизмов адаптивного управления системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2022. № 2. С. 214–223. DOI: 10.24412/2071-6168-2022-2-214-223.
14. Толстой А.И. Системотехника обеспечения безопасности объектов в информационной сфере // Вопросы кибербезопасности. 2024. № 5 (63). С. 47–57 DOI: 10.21681/2311-3456-2024-5-47-57.

CYBERSECURITY OF VIDEO SURVEILLANCE SYSTEMS IN THE CONTEXT OF INFORMATION TECHNOLOGY IMPACTS

Starodubtsev Yu. I.[19], Zakalkin P. V.[20], Karasev S. V.[21]

Keywords: *cyberspace, information technology impacts, cybersecurity, video surveillance, threats, intruder, information security.*

The purpose of the study: *to consider the procedure for the implementation of information technology impacts on video surveillance systems; to assess the existing information security requirements for video surveillance systems in the Russian Federation; to form generalized proposals to ensure the information security of existing video surveillance systems in conditions of deliberate information technology impacts.*

The results obtained: *a generalized scheme of the procedure for the implementation of information technology impacts on video surveillance systems has been formed; generalized proposals for ensuring the information security of existing video surveillance systems have been formulated; proposals for the development of regulatory documentation by regulators (in the field of information security) have been formulated.*

Scientific novelty: *the analysis of the conflict situation in the field of video surveillance systems has been carried out, which made it possible to identify the initial measures necessary for the subsequent development of information security of video surveillance systems.*

Research methods: *system analysis, classification, comparative analysis.*

References

1. Starodubcev Yu. I., Zakalkin P. V. Strukturno-funkcional'nyj analiz konfliktnoj situacii mezhdu gosudarstvennoj sistemoj obespecheniya informacionnoj bezopasnosti i inostrannoj sistemoj destruktivnyh vozdejstvij // Voprosy kiberbezopasnosti. 2024. №4(62). S. 82–91. DOI: 10.21681/2311-3456-2024-4-82-91.
2. Ivanov S. A. Transformaciya roli edinoj seti elektrosvyazi Rossijskoj Federacii v sisteme voennogo upravleniya v rezul'tate realizacii processov cifrovoj transformacii i globalizacii // Voprosy radioelektroniki. Seriya: Tekhnika televideniya. 2021. №3. S. 17–23.

19 Yuri Starodubtsev, Honored Scientist of the Russian Federation, Honored Inventor of the Russian Federation, Doctor of Military Sciences, Professor, Professor of the Department, Military Academy of Communications, Saint Petersburg, Russia. E-mail: prof.starodubtsev@gmail.com, https://orcid.org/0000-0001-5140-4476
20 Pavel Zakalkin, Ph.D., Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586
21 Stas Karasev, Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: llmaglu@mail.ru

3. *Ivanov S.A. Ustojchivost' setej svyazi obshchego pol'zovaniya v usloviyah globalizacii // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2021. № 9. S. 86–90. DOI: 10.24412/2071-6168-2021-9-86-90.*
4. *Kocynyak M.A., Lauta O.S., Nechepurenko A.P. Metodika ocenki ustojchivosti informacionno-telekommunikacionnoj seti v usloviyah informacionnogo protivoborstva // Voprosy oboronnoj tekhniki. Seriya 16: Tekhnicheskie sredstva protivodejstviya terrorizmu. 2019. № 1-2 (127-128). S. 58–62.*
5. *Brechko A.A., Sazykin A.M. Problema upravleniya parametrami kiberprostranstva v interesah sub"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii // Voprosy oboronnoj tekhniki. Seriya 16: Tekhnicheskie sredstva protivodejstviya terrorizmu. 2022. № 5-6 (167-168). S. 36–43.*
6. *Zakalkin P.V. Aspekty ispol'zovaniya kiberprostranstva v interesah korporativnyh sistem upravleniya // Trudy Nauchno-issledovatel'skogo instituta radio. 2021. № 4. S. 23–32. DOI: 10.34832/NIIR.2021.7.4.003.*
7. *Starodubtsev Y.I., Balenko E.G., Zakalkin P.V., Fedorov V.H. Change dynamics for forms and opportunities of centers of power under globalization // V sbornike: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. S. 9271172. DOI: 10.1109/FarEastCon50210.2020.9271172.*
8. *Starodubcev Yu.I., Zakalkin P.V., Ivanov S.A. Mnogovektornyj konflikt v kiberprostranstve kak predposylka formirovaniya novogo vida vooruzhennyh sil // Voennaya mysl'. 2021. №12. S. 126–135.*
9. *Hwang Y.-W., Lee I.-Y., Kim H., Lee H., Kim D. Current status and security trend of OSINT // Wireless Communications and Mobile Computing. 2022. T. 2022. S. 1290129. DOI: 10.1155/2022/1290129.*
10. *Mahnin V.L. O zakonah i formah vojny // Vestnik akademii voennyh nauk. 2024. №2(87). C. 45–53.*
11. *Gavrilov A.D., Grudinin I.V., Majburov D.G., Novikov V.A. Dva goda special'noj voennoj operacii: nekotorye itogi, veroyatnye perspektivy // Vestnik akademii voennyh nauk. 2024. №2(87). C. 54–64.*
12. *Belov A.S., Dobryshin M.M., SHugurov D.E. Nauchno-metodicheskij podhod k ocenivaniyu kachestva sistem obespecheniya informacionnoj bezopasnosti // Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2022. № 11. S. 34–40. DOI: 10.25791/pribor.11.2022.1373.*
13. *Dobryshin M.M. Vybor struktury i mekhanizmov adaptivnogo upravleniya sistemy obespecheniya informacionnoj bezopasnosti // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2022. № 2. S. 214–223. DOI: 10.24412/2071-6168-2022-2-214-223.*
14. *Tolstoj A.I. Sistemotekhnika obespecheniya bezopasnosti ob"ektov v informacionnoj sfere // Voprosy kiberbezopasnosti. 2024. № 5 (63). S. 47–57 DOI: 10.21681/2311-3456-2024-5-47-57.*