Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Орловский юридический институт Министерства внутренних дел Российской Федерации имени В. В. Лукьянова»

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ: ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ И ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ

Сборник научных статей

Орел
ОрЮИ МВД России имени В. В. Лукьянова
2018

УДК 004
ББК 32.97
И74

Редакционная коллегия:
канд. юрид. наук Л. Д. Матросова (председатель);
канд. юрид. наук Д. С. Мишин (заместитель председателя);
канд. пед. наук В. П. Шумилин, канд. тех. наук В. В. Линьков;
Л. В. Колесникова (ответственный секретарь)

И74 **Информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности :** сборник научных статей / редкол. : Л. Д. Матросова [и др.]. – Орел : Орловский юридический институт МВД России имени В. В. Лукьянова, 2018. – 69 с.
ISBN 978-5-88872-230-5

Сборник содержит статьи профессорско-преподавательского состава и аспирантов, посвященные проблемам применения технологий компьютерной обработки информации в деятельности ОВД и обеспечения информационной безопасности в открытых каналах связи.

Статьи публикуются в авторской редакции.

УДК 004
ББК 32.97

ISBN 978-5-88872-230-5 **© ОрЮИ МВД России имени В. В. Лукьянова, 2018**

Содержание

Введение…….. 5
Линьков В. В.
Вопросы автоматизации подразделений Госавтоинспекции……. 6
Семенов Е. Ю.
Аппаратно-программный комплекс «Центр управления нарядами ГИБДД»……. 10
Шумилин В. П.
Проблемы исследований в сфере организации дорожного движения и пути их решения……. 16
Карпика А. Г., Петрищева Е. Н.
Некоторые аспекты обеспечения безопасности компьютерных систем от вредоносных программ…… 21
Матросова Л. Д.
Основные направления и организационно-методические аспекты использования компьютерных технологий при расследовании дорожно-транспортных преступлений…… 26
Мишин Д. С., Паньков С. Л.
Актуальные вопросы построения и обеспечения безопасности информационного портала…… 38
Кузнецов А. С.
Описание возможности создания системы интеллектуальной поддержки принятия управленческих решений в ГИБДД МВД РФ при использовании статистических данных …….. 42
Орешин Н. А., Черепков С. А., Лазарев С. Н., Евсеев Т. С.
Теоретические аспекты автоматизации процессов передачи и обработки видеоизображений в системе контроля и управления доступом на основе цифровых технологий……. 45
Лазарев С. Н., Орешин Н. А., Матвеев А. М., Закиров И. И.
Математические аспекты автоматизации процессов передачи и обработки видеоизображений в системе контроля и управления доступом на основе цифровых технологий……. 53

Костин С. В., Ванюков Р. Ю.
Предложения по обеспечению надежности электроснабжения малогабаритных индивидуальных телекоммуникационных систем мобильных объектов телекоммуникаций силовых ведомств…… 60
Черепков С. А., Орешин Н. А., Шеховский Д. А., Викторов М. А.
Алгоритмические аспекты автоматизации процессов передачи и обработки видеоизображений в системе контроля и управления доступом на основе цифровых технологий……. 63

ВВЕДЕНИЕ

Формирование единого информационного пространства и развитие телекоммуникационных технологий занимает значительное место в современном обществе. Это связано с тем, что в вычислительных системах интегрируется информация о различных сторонах деятельности государства, населения, конкретных граждан и их личной жизни в политическом, экономическом, моральном и имущественном аспектах.

Широкое применение технологий компьютерной обработки информации в деятельности ОВД, значительно повысило эффективность ее повседневной деятельности. Применение автоматизированных рабочих мест и управляющих систем позволило снизить время реагирования на различные ситуации. Автоматизация деятельности региональных подразделений позволила сократить время на принятие управленческих решений и объединить в единую информационную систему все подразделения ОВД, находящиеся на территории региона. Используемые в настоящее время информационные системы позволяет автоматизировать все направления деятельности региональных подразделений ОВД, что обеспечивает оперативный обмен информацией и улучшенный доступ к информационным ресурсам.

ВОПРОСЫ АВТОМАТИЗАЦИИ ПОДРАЗДЕЛЕНИЙ ГОСАВТОИНСПЕКЦИИ

Линьков В. В.,
старший преподаватель кафедры
ИТвДОВД, канд. тех. наук
(ОрЮИ МВД России
имени В. В. Лукьянова)

Безопасность дорожного движения является одной из важных социально-экономических и демографических задач Российской Федерации. От аварийности наносится внушительных масштабов материальный и моральный ущерб обществу.

Ежегодно в Российской Федерации в результате дорожно-транспортных происшествий (ДТП) погибают или получают ранения свыше 270 тыс. человек.

В ряде стратегических и программных документов вопросы обеспечения безопасности дорожного движения обладают высоким приоритетом.

Внедрение программ повышения безопасности является одной из актуальных задач развития страны. Целью Федеральной целевой программы «Повышение безопасности дорожного движения в 2013–2020 годах» является сокращение смертности в результате дорожно-транспортных происшествий, в том числе детей, к 2020 году на 8 тыс. человек (28,82 процента) по сравнению с 2012 годом. Только комплексная реализация мероприятий может обеспечить должный уровень безопасности дорожного движения. В число основных мероприятий входит:

- формирование у граждан негативного отношения к правонарушениям в сфере дорожного движения за счет создания системы пропагандистского воздействия;
- формирование у детей навыков безопасного поведения на дорогах;
- повышение культуры вождения;
- совершенствование системы оказания помощи пострадавшим в дорожно-транспортных происшествиях;
- повышение требований к подготовке водителей на получение права на управление транспортными средствами и установление более жестких требований к автошколам [1].

В связи со сложившейся ситуацией в области дорожного движения требуется стабильный и полный учёт ДТП. Это необходимо, в первую очередь, для сокращения количества происшествий в дальнейшем, путём предотвращения условий и факторов, послуживших причиной предыдущих происшествий. Полная картина состояния дорожной безопас-

ности в стране позволяет проводить статистическую и аналитическую работу, по итогам которой происходит акцентирование внимания, в том числе и участников дорожного движения, к примеру, на расположении опасных участков дорог, передвижение по которым требует осторожности и осмотрительности. Учёт ДТП позволяет также определить наиболее возможные варианты происшествий в зависимости от организации движения на каком-либо участке дороги или прилегающей территории, состояния дорожного покрытия и условий видимости и, соответственно, избежать их силами самих же водителей и пешеходов.

Для осуществления оперативного сбора информации о дорожно-транспортных происшествиях, ведения государственного статистического учета данных о ДТП приказом МВД России от 16 августа 2014 года №700 «О порядке эксплуатации в органах внутренних дел Российской Федерации автоматизированных систем оперативного сбора, учета и анализа сведений о показателях в области обеспечения безопасности дорожного движения» введены в эксплуатацию автоматизированная информационно-управляющая система (АИУС) Госавтоинспекции, автоматизированная система учета дорожно-транспортных происшествий (АС УДТП) и многопараметрическая информационно-аналитическая система прогнозирования и моделирования ситуации в области обеспечения безопасности дорожного движения (МИАС).

АИУС Госавтоинспекции обеспечивает автоматизированный сбор, обработку и хранение информации о ДТП и предоставление оперативной информации о состоянии дорожно-транспортной аварийности на территории Российской Федерации.

АС УДТП предназначена для автоматизированного сбора, обработки, и хранения информации о ДТП с пострадавшими и дальнейшего включения в государственную статистическую отчетность.

МИАС обеспечивает формирование единого информационно-аналитического пространства показателей ситуации в области обеспечения безопасности дорожного движения; анализ причин, фактов, времени, сопутствующих условий и мест совершения дорожно-транспортных происшествий, а также характеристик участников происшествий и выявление наиболее проблемных направлений аварийности за счет мониторинга показателей сложившейся ситуации [2].

МИАС разработана в целях повышения оперативности и обоснованности принимаемых управленческих решений в сфере безопасности дорожного движения, как в разрезе регионов РФ, так и в стране в целом, на основе использования современных информационных технологий анализа и мониторинга.

Инструменты МИАС сгруппированы по следующим подсистемам:

– Картограмма;
– Аналитические панели;

– Отчеты;

– Конструктор запросов.

Картограмма отображает показатели аварийности и показатели, рассчитываемые на данных формы «Сведения Госавтоинспекции», на карте России в разрезе регионов.

Аналитические панели предназначены для оценки пороговых уровней показателей, характеризующих ситуацию в области обеспечения безопасности дорожного движения как с учетом оперативной и годовой информации, так и посредством использования методов многомерного статистического анализа.

Подсистема «Отчеты» позволяет получить статистическую информацию в области обеспечения безопасности дорожного движения. Кроме того, при помощи средств анализа информации, заложенных в МИАС, реализована возможность производить ранжирование регионов Российской Федерации по показателям безопасности дорожного движения, составлять паспорта субъектов на основе этих показателей, а также оценивать эффективность деятельности подразделений ГИБДД, направленной на снижение аварийности на основе структурного анализа административной практики и аварийности, выполнение федеральных целевых программ и т. д.

Конструктор запросов обеспечивает возможность формирования пользовательских многопараметрических запросов к базе данных, содержащей массив карточек учета ДТП (АС УДТП), или базе данных, содержащих информацию по форме ведомственной статистической отчетности «Сведения Госавтоинспекции», и отображения полученных результатов в табличном, графическом и картографическом видах.

Информационный обмен данных о ДТП происходит следующим образом. Первичный сбор данных осуществляется АИУС Госавтоинспекции, где формируется массив электронных карточек оперативного учета, которые содержат текстовое описание, место (включая географические координаты), время, фотоматериалы, схему ДТП, информацию о неудовлетворительных дорожных условиях (при их наличии), сопутствующие нарушения. Из АИУС Госавтоинспекции производится выгрузка данных о ДТП с погибшими и пострадавшими в АС УДТП для включения в государственную статистическую отчетность. Из АС УДТП данные передаются в МИАС, где формируется единое информационно-аналитическое пространство показателей для статистического анализа ситуации в области обеспечения безопасности дорожного движения [3].

Такая схема сбора, обработки и хранения данных, несомненно, способствует повышению качества учета дорожно-транспортных происшествий. Однако при этом также целесообразно произвести сопряжение АИУС Госавтоинспекции с автоматизированными информационными системами экстренных служб, участвующих в ликвидации послед-

ствий ДТП. В настоящее время участие экстренных служб лишь отражается в карточке ДТП АИУС Госавтоинспекции, но эти данные вводятся операторами со стороны Госавтоинспекции, а не средствами автоматизированного взаимодействия. Совершенствование информационного обмена в этом направлении позволит организовать надежное и своевременное информационное взаимодействие экстренных служб, что позволит сократить время прибытия на место ДТП всех служб, участвующих в ликвидации их последствий и повысить эффективность оказания помощи пострадавшим.

Таким образом, внедрение автоматизированных информационных систем в деятельность подразделений по обеспечению безопасности дорожного движения способствует повышению качества сбора, обработки и хранения информации о ДТП. Аналитический инструментарий обеспечивает возможность статистического анализа, на основании которого становится возможным принимать обоснованные управленческие решения в сфере безопасности дорожного движения. Выход системы сбора и анализа данных о ДТП на качественно новый уровень, несомненно, способствует снижению тяжести последствий при ДТП за счет своевременного обнаружения проблемных показателей и формирования комплекса мер по их устранению. При этом направлением развития данной системы может стать решение вопросов автоматизированного взаимодействия экстренных служб при ликвидации последствий ДТП, что позволит снизить тяжесть последствий за счет своевременного оказания помощи пострадавшим.

---

1. Повышение безопасности дорожного движения в 2013–2020 годах: Федеральная целевая программа.
2. О порядке эксплуатации в органах внутренних дел Российской Федерации автоматизированных систем оперативного сбора, учета и анализа сведений о показателях в области обеспечения безопасности дорожного движения: Приказ МВД России от 16 августа 2014 г. № 700.
3. Линьков В. В. Основные аспекты повышения эффективности хранения цифровых изображений в автоматизированных информационных системах Госавтоинспекции // Известия ОрелГТУ. Серия «Информационные системы и технологии». Орел: Изд-во ОрелГТУ, 2015. № 2(88). С. 31–34.

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС «ЦЕНТР УПРАВЛЕНИЯ НАРЯДАМИ ГИБДД»

Семенов Е. Ю.,
старший преподаватель кафедры
ИТвДОВД, канд. юрид. наук,
Долгова А. В.
(ОрЮИ МВД России
имени В. В. Лукьянова)

Аппаратно-программный комплекс (АПК) – это продукт, в состав которого входят технические средства и программное обеспечение, совместно применяемые для решения задач определенного типа. В качестве аппаратно-программных комплексов могут рассматриваться интеллектуальные системы хранения данных, современные офисные АТС, комплексы пожарно-охранной сигнализации, контроля доступа, видеонаблюдения, всевозможные решения для промышленной автоматизации и многое другое.

С точки зрения документирования аппаратно-программный комплекс занимает промежуточное положение между устройством или программным продуктом в чистом виде и автоматизированной системой. Как правило, производитель тиражируемого аппаратно-программного комплекса не знает заранее, где именно на основе последнего будет развернута система и как именно она будет функционировать.

Тем не менее в большинстве случаев он исходит из одного или нескольких типовых сценариев применения комплекса в составе системы, что отражается и в устройстве комплекса, и в эксплуатационной документации на него.

В Госавтоинспекции наиболее часто используемыми являются АПК, предназначенные для работы на дорогах с целью автоматической фотовидеофиксации нарушений правил дорожного движения.

Измерительными элементами, в зависимости от конструкции, могут выступать:

- радиочастотный радар (доплеровский радар), предназначен для измерения скорости объекта (обычно автомобиля), излучает высокочастотный радиосигнал X-, K- или Kадиапазона.

Частота отраженного импульса изменяется пропорционально скорости перемещения движущегося транспорта. Приняв отраженный сигнал, он измеряет отклонение частоты и вычисляет скорость автомобиля;

Появившиеся разновидности доплеровский радаров позволяют проводить измерение скорости с движущегося патрульного автомобиля,

где радар получает из отраженного от дороги сигнала информацию о скорости патрульного автомобиля.

Пример:

«Искра-1В» предназначена для работы в стационарном режиме, в основном в одном направлении. Радар позволяет практически в любых условиях распределять в дорожном потоке транспортное средство с максимальной скоростью, превышающее скорость потока всего на 5 км/ч.

При этом радар практически невидим для всех неадаптированных под российские условия радар-детекторов зарубежного производства: все они воспринимают короткоимпульсный сигнал «Искры» как помеху.

«Искра-1Д» – первый российский радар, способный работать во всех направлениях в движущемся патрульном автомобиле. В течение одной секунды радиолокатору удается выполнить пятикратное измерение собственной скорости и целевой скорости, исключить возможные ошибки, обработать результаты измерений и отобразить их на табло, который последовательно отображает скорость цели, собственную скорость и время с самого начала измерения.

Для измерения скорости движущегося транспортного средства существуют лазерные радары.

- Лазерный радар (лидар).

Его также нередко называют оптическим. Он излучает короткие импульсы лазера вне зрительного диапазона с установленным интервалом времени в направлении автомашины, которые отражаются от транспортного средства и принимаются лазерным измерителем. Лазерный радар зафиксировав изменение дальности до объекта по времени задержки каждого отраженного импульса вычисляет скорость автомобиля, используя данные об изменении дальности за нужный промежуток времени.

Пример:

Лазерный радар Amata имеет ряд преимуществ по сравнению с более ранними радарными моделями и намного удобнее в эксплуатации. С его помощью вы можете измерять скорость объекта, не выходя из автомобиля, фиксируя радар в кабине. Как и в предыдущих радарных моделях, его можно установить на штатив. Этот радар имеет широкий диапазон измерений скорости от 1,5 до 280 км/ч. Средняя погрешность измерения составляет 1 км/ч, максимальное расстояние для измерения скорости составляет около семисот метров, номерной знак определяется на расстоянии от 15 до 250 метров. Комплекс видеокамер Amata способен снимать видео с частотой 5, 10 и 15 кадров в секунду. разрешение дисплея составляет 640x480 пикселей, фотографии – 1600x1200 пикселей. Минимальное расстояние для фотографирования составляет 15 м. Радар можно управлять с помощью пульта дистанционного управления. Передача данных на компьютер осуществляется с помощью универсального

интерфейса USB 2.0, поддерживается возможность обновления программного обеспечения.

Телевизионный измеритель (анализ видеоряда) – определяет скорость движения транспортных средств безрадарным методом (по видеокадрам), что делает «антирадары» бесполезными.

Пример:

Метр ІТ-08 представляет собой многофункциональное измерительное малогабаритное портативное устройство, состоящее из двух блоков.

Основным блоком является базовый модуль МВ-08, предназначенный для индикации, управления, генерации напряжения питания от аккумуляторов и внешнего источника питания.

Дополнительный блок МС-08 представляет собой сменный измерительный модуль, который взаимодействует с модулем управления для получения определенного набора функций измерения или пользователя.

Радиометка (RFID) – специальный чип радиочастотной идентификации (транспондер), размещаемый на автомобильном номере. Перспективная технология, позволяющая считывать данные посредством радиосигналов на расстоянии, может применяться и для дистанционной идентификации автомобиля в случае, если госномер автомобиля не считался обычной видеокамерой.

С каждым годом на дорогах нашей страны появляются все больше автомобилей. К сожалению, не все водители строго следуют правилам дорожного движения, что часто приводит к различным видам аварий. Для общего улучшения ситуации с дорожным движением, а также для снижения уровня аварийности, ГИБДД использует в своей работе радиолокационное обнаружение нарушений правил дорожного движения. Прогресс в этой области не стоит на месте, а стареющие камеры заменяются новыми более сложными техническими средствами, которые не всегда видны радарным извещателям, установленным в автомобилях. По типу установки радары делятся на 2 группы – мобильные и стационарные.

Стационарные радиолокационные камеры фиксируются в определенном месте на постоянной основе на жесткой опоре над проезжей частью. Как правило, данные этого вида радиолокационных потоков поступают в Центр по рассмотрению административных правонарушений в Государственной инспекции безопасности дорожного движения или на ближайший стационарный пост ДПС. На дорогах при приближении к стационарным камерам, согласно правилам, должен быть установлен знак 8.23 «Фотовидеофиксация».

В настоящее время широко применяется АПК «Центр управления нарядом ГИБДД» – автоматизированный аппаратно-программный комплекс, предназначенный для эффективного и эффективного управления

оборудованием дорожной полиции при выполнении служебных обязанностей, а также оперативного мониторинга ситуации на дорогах города и региона.

АПК «Центр управления нарядом ГИБДД» – автоматизированный аппаратно-программный комплекс, предназначенный для эффективного и эффективного управления оборудованием дорожной полиции при выполнении служебных обязанностей, а также оперативного мониторинга ситуации на дорогах города и региона.

АПК ЦУН ГИБДД объединяет следующие элементы:

1. Геоинформационная система (электронная карта) с базой данных линий автомобильного сообщения и объектов городской инфраструктуры;

2. Сертифицированная подсистема определения местоположения мобильных объектов (ГЛОНАСС/GPS);

3. Подсистема городского видеонаблюдения;

4. Подсистема видеонаблюдения на трассах;

5. Подсистема видеофиксации нарушений правил дорожного движения;

6. Подсистема взаимодействия с диспетчерским центром;

7. Подсистема фиксации, сохранения и отображения событий;

8. Автоматизированные рабочие места (АРМ) операторов системы, объединённые сетью передачи данных.

АПК ЦУН ГИБДД предоставляет сотрудникам информацию для проведения оперативной и следственной деятельности, предоставления отчетов и резюме, проведения аналитической работы. Операторы системы AWS являются элементами единой сети оперативных сотрудников. Фиксированные события и назначенные задачи доступны для других операторов.

Информационная система АПК ЦУН ГИБДД позволяет записывать (в автоматическом или ручном режиме) важные события и отображать их на электронной карте. Это обеспечивает эффективность принятия решений при управлении нарядами. обеспечивает сотрудников информацией для проведения оперативно-следственных мероприятий, предоставления отчётов и сводок, ведения аналитической работы. АРМ операторов системы являются элементами единой сети оперативных дежурных. Зафиксированные события и назначенные задачи становятся доступны другим операторам.

Информационная система АПК ЦУН ГИБДД позволяет фиксировать (в автоматическом или ручном режиме) важные события и отображать их на электронной карте. Это обеспечивает эффективность принятия решений при управлении нарядами.

Типы регистрируемых и отображаемых событий:

- данные от подсистемы видеофиксации нарушений правил дорожного движения;

- информация об изменении расположения мобильных отрядов;

- сообщения по каналам связи;

- данные о состоянии проезжей части автодорог (состояние покрытия, ремонтные работы, заторы);

- информация о ДТП;

- нарушения ПДД;

- вызовы, происшествия;

- изображение с камер видеонаблюдения.

АРМ оператора системы обеспечивает:

- отображение местоположения мобильных отрядов на электронной карте автомобильных дорог;

- отображение событий (ДТП, вызовы) и состояния дорог на электронной карте с привязкой к участку дороги по километражу;

- отображение на электронной карте фактов нарушения правил дорожного движения, зафиксированных подсистемой видеофиксации нарушений;

- поиск ближайших мобильных отрядов к месту события на автодороге;

- определение расстояния в километрах от места события до отрядов на автодороге (путь по автодороге, а не абсолютное расстояние между точками на карте);

- определение ближайшего адреса в городе для точки события на электронной карте;

- доступ к постам видеонаблюдения на дорогах города и на трассах из интерфейса электронной карты, вызов видеопотока от камеры путём её выбора на электронной карте;

- задание маршрутов патрулирования для мобильных отрядов в абсолютных координатах на карте и в объектах ГИС по названию улиц, наименованию трасс;

- контроль отклонений мобильных отрядов от маршрутов;

- контроль превышения допустимой скорости мобильными отрядами;

- протоколирование всех событий в системе с возможностью воспроизведения в том же порядке, на той же или на повышенной скорости, в том числе отображение маршрутов следования мобильных отрядов;

- путь мобильного отряда за промежуток времени;

- плановый маршрут отряда;

- адрес, ближайшие перекрёстки или километраж на трассе по точке местонахождения отряда.

- события и происшествия

- посты видеонаблюдения;

- схему поста видеонаблюдения с отображением углов обзора камер;

- улицы, дома, объекты города – областного центра с фиксацией адресов и названий для осуществления поиска.

Таким образом, рассмотренные АПК, которые используются в Государственной инспекции дорожного движения МВД России, преодолевают задачи реализации Федеральной целевой программы «Повышение безопасности дорожного движения в 2013-2020 годах».

Принимаемые меры по снижению дорожно-транспортных происшествий и их последствий в России ощутимого эффекта пока не приносят; данная проблема требует поиска новых подходов к ее решению.

Однако, рассмотренные в научной работе аппаратно-программные комплексы, применяемые в Госавтоинспекции МВД России, позволяют эффективно решать задачи по выполнению Федеральной целевой программы «Повышение безопасности дорожного движения в 2013–2020 годах». Совершенствование государственного регулирования является необходимым условием для повышения безопасности дорожного движения.

Бесконечная борьба между водителями и сотрудниками Госавтоинспекции не прекращается. И для водителей изобрели специальные устройства, которые принимают сигналы установленных по дороге радаров, предупреждая тем самым водителя о снижении скорости до допустимых параметров. Антирадары или как их еще называют радары-детекторы, также отличаются своими техническими характеристиками, стоимостью и принципом работы.

Согласно статистике, ежегодно приобретаются системы автоматического контроля и выявления нарушений ПДД, что говорит об актуальности данного направления совершенствования деятельности по обеспечению безопасности дорожного движения.

Используемые сегодня в Госавтоинспекции АПК позволяют повысить эффективность решения широкого спектра повседневных задач. Упомянутые системы позволяют накапливать и выдавать в удобном для пользователя виде большие массивы данных, собираемых при помощи автоматизированных средств фиксации.

ПРОБЛЕМЫ ИССЛЕДОВАНИЙ В СФЕРЕ ОРГАНИЗАЦИИ ДОРОЖНОГО ДВИЖЕНИЯ И ПУТИ ИХ РЕШЕНИЯ

Шумилин В. П.,
старший преподаватель кафедры
ИТвДОВД, канд. пед. наук
(ОрЮИ МВД России
имени В. В. Лукьянова)

Исследования, проводимые в сфере дорожного движения, можно определить как деятельность ученых, специалистов по изучению условий дорожного движения, выявлению проблем в организации дорожного движения, обоснованию мероприятий по предупреждению дорожно-транспортных происшествий и снижению тяжести их последствий.

При этом целью данной деятельности является максимальное обеспечение безопасности дорожного движения.

Как справедливо отмечал В. В. Лукьянов, под дорожным движением понимается процесс движения транспортных средств по дорогам, в котором действия всех его участников определяются правилами [1].

Интересно отметить, что с точки зрения ученых существует несколько подходов к определению безопасности дорожного движения. Так, В. И. Майоров делит БДД на следующие категории:

1) научно-правовую;

2) правовую;

3) социально-правовую [2].

Об уровне обеспечения безопасности дорожного движения свидетельствуют, прежде всего, статистические данные. Сведения об аварийности отражают дорожную ситуацию, сложившуюся к определенному моменту. По мнению Б. В. Россинского, колебания общего уровня аварийности на автомобильном транспорте определяются более глобальными причинами, в частности связанными с экономической и политической ситуацией в стране. По мере автомобилизации страны и, как следствие, увеличения интенсивности движения транспортных средств абсолютные значения числа ДТП, несмотря ни на какие этапы и циклы их колебаний, растут [3].

Необходимо помнить, что на статистику результатов исследования дорожного движения влияет много факторов. Можно сказать, что статистика при одинаковых условиях увеличивается, когда:

– количество происшествий, исходя из которых, формируются результаты, увеличивается;

– ДТП имеют высокую и стабильную степень регистрации;

– сведения относительно происшествий (например, пользование ремнями безопасности, нарушения скоростного режима) регистрируются с помощью хорошо разработанной методики.

Также одной из проблем исследования организации дорожного движения можно считать «человеческий» фактор. Так, практика свидетельствует о том, что органы исполнительной власти субъектов РФ не в полном объеме при проверке выявляют нарушения законодательства, а также принимают эффективные меры по их устранению и возмещению ущерба [4]. При выявлении нарушений законодательства федерального уровня ограничиваются лишь внесением предписаний, контроль за исполнением которых в большинстве случаев отсутствует [5].

Неоднозначно сложилась практика применения приказа МВД России от 30 марта 2015 г. № 380 [6].

Согласно данному приказу сотрудники ГИБДД имеют право давать юридическим и должностным лицам обязательные для исполнения предписания об устранении нарушений нормативных правовых актов в области обеспечения безопасности дорожного движения при строительстве, ремонте, реконструкции и содержании автомобильных дорог, а в случае непринятия по таким предписаниям необходимых мер привлекать виновных лиц к ответственности, предусмотренной законодательством РФ. Однако вопросы о принадлежности автомобильных дорог конкретным владельцам не всегда очевидны. В связи со спорными моментами лица, виновные в ненадлежащем содержании дорог и дорожной инфраструктуры, уклоняются от административной ответственности.

Далее рассмотрим следующую проблемную ситуацию. Согласно Федеральному закону № 257-ФЗ [7] в качестве владельца автомобильных дорог могут выступать как исполнительные органы государственной власти, так и местная администрация, физические и юридические лица, владеющие автомобильными дорогами на вещном праве в соответствии с законодательством РФ.

В соответствии с ч. 2 ст. 17 и ч. 2 ст. 18 данного Закона порядок содержания и ремонта автомобильных дорог устанавливается нормативными правовыми актами РФ, нормативными правовыми актами субъектов РФ и муниципальными правовыми актами.

В соответствии с п. 1 ст. 12 Федерального закона «О безопасности дорожного движения» [8] ремонт и содержание дорог на территории РФ должны обеспечивать безопасность дорожного движения.

В силу п. 2 ст. 12 указанного Закона обязанность по надлежащему соответствию состояния дорог установленным правилам, стандартам, техническим нормам и другим нормативным документам

возлагается на лиц, осуществляющих содержание автомобильных дорог.

Однако многие исследователи отмечают затруднение в применении данных норм.

Таким образом, механизм правового регулирования в сфере установления владельца автомобильных дорог не достаточно прозрачен.

Немаловажной проблемой при проведении исследований организации дорожного движения выявление причин и условий, приводящих к высокому уровню аварийности. Снижению уровня аварийности и количества транспортных заторов будет способствовать серьезная оценка причин и условий возникновения проблем на каждом участке улично-дорожной сети. Один из путей достижения этой цели – обобщение статистических данных и сведений оценочного характера, предоставляемых органами исполнительной власти и подведомственными им учреждениями. Указанные данные должны быть отражены в конкретном проекте изменений транспортной ситуации на проблемном участке улично-дорожной сети [9].

Также автор пишет о том, на современном этапе меры реагирования, способствующие ликвидации очагов аварийности не могут строиться только на результатах проверок административной деятельности ГИБДД. Необходимость мер, принимаемых уполномоченными лицами ГИБДД для снижения аварийности, должна оцениваться обоснованно и своевременно проводимым мероприятиям. Количественные показатели аварийности и административной практики подразделений ГИБДД не помогут объективному анализу.

Уместно привести мнение А. В. Кулешовой, которая считает, что к основным факторам, влияющим на уровень аварийности на территории РФ, необходимо отнести:

– пренебрежение требованиями безопасности дорожного движения со стороны участников дорожного движения, недостаточное понимание и поддержку проводимых мероприятий со стороны общества, отсутствие должной ответственности со стороны руководителей всех уровней;

– низкое качество подготовки водителей транспортных средств, приводящее к ошибкам в оценке дорожной обстановки, неудовлетворительную водительскую дисциплину, невнимательность и небрежность водителей при управлении транспортными средствами;

– высокий уровень автомобилизации общества;

– недостаточную деятельность по развитию и совершенствованию улично-дорожных сетей и совершенствованию организации дорожного движения [10].

Исследуя нормативно-правовую базу, регламентирующую деятельность субъектов обеспечения безопасности дорожного движения, можно обнаружить некоторые противоречия в правовых нормах.

Так, например, согласно п. 3.1.6 ГОСТ Р 50597 [11] сроки ликвидации зимней скользкости и окончания снегоочистки для автомобильных дорог в зависимости от категории дороги не должны превышать определенного количества часов, определяемого категорией дороги.

В то же время распоряжение Минтранса РФ от 16 июня 2003 г. № ОС-548-р [12], содержит норму о том, что после окончания снегопада необходимо произвести удаление оставшихся снежно-ледяных отложений или завершающее подметание (п. 4.4.2.8). При этом конкретный срок осуществления подобных мероприятий не указан.

Работники дорожных служб в своей деятельности руководствуются именно указанным Распоряжением. В то же время ГИБДД, а конкретнее подразделения дорожной инспекции, осуществляя контроль зимнего содержания дорог, требует устранения снежного покрытия в периоды времени, предписанные ГОСТом. В данной ситуации можно говорить о том, что субъекты, ответственные за содержание дорог, следуя указаниям различных правовых актов, сталкиваются с проблемой противоречия правовых норм.

Таким образом, резюмируя изложенную информацию, можно говорить о том, что к наиболее острым проблемам исследований в сфере дорожного движения относятся толкование положений отдельных нормативных правовых актов, вопросы разграничения компетенции федеральных органов как государственной власти, так и органов местного самоуправления по вопросам организации дорожного движения. Немаловажной проблемой в деятельности по ОДД является ликвидация очагов аварийности, что требует тщательного анализа причин каждого ДТП, устранения способствующих условий.

---

1. Лукьянов В. В. Безопасность дорожного движения. М., 1983. С. 12.

2. Майоров В. И. Государственно-правовое обеспечение безопасности в сфере дорожного движения: теоретико-прикладные проблемы: монография. Челябинск, 2008.

3. Россинский Б. В. Административные наказания в сфере дорожного движения и аварийность на автомобильном транспорте // Административное право и процесс. 2014. № 5. С. 8–17.

4. Россинский Б. В., Черепанова Е. В., Чеснокова М. Д.., Глазкова М. Е. О соблюдении законодательства в деятельности органов исполнительной власти // Журнал российского права. 2010. № 7.

5. В. Стрельников. Ударим КоАПом по бездорожью и разгильдяйству// ЭЖ-Юрист. 2013. № 5. С. 1, 4.
6. Об утверждении Административного регламента Министерства внутренних дел Российской Федерации исполнения государственной функции по осуществлению федерального государственного надзора в области безопасности дорожного движения в части соблюдения требований законодательства Российской Федерации о безопасности дорожного движения, правил, стандартов, технических норм и иных требований нормативных документов в области обеспечения безопасности дорожного движения при строительстве, реконструкции, ремонте и эксплуатации автомобильных дорог: Приказ МВД России от 30 марта 2015 г. № 380.
7. Об автомобильных дорогах и о дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации: Федер. закон Рос. Федерации от 8 ноября 2007 г. № 257-ФЗ: в ред. от 7 февраля 2017 г.) // Собр. законодательства Рос. Федерации. 2007. № 46, ст. 5553.
8. О безопасности дорожного движения: Федер. закон Рос. Федерации от 10 декабря 1995 г. № 196-ФЗ: в ред. от 3 июля 2016 г. // Собр. законодательства Рос. Федерации. 1995. № 50, ст. 4873.
9. Петров И. В. Надзор за исполнением законодательства об организации и безопасности дорожного движения // Законность. 2013. № 7. С. 50–52.
10. Кулешова А. В. К вопросу о конституционности норм Кодекса Российской Федерации об административных правонарушениях в области дорожного движения // Административное право и процесс. 2014. № 7. С. 48–54.
11. ГОСТ Р 50597-93. Государственный стандарт Российской Федерации. Автомобильные дороги и улицы. Требования к эксплуатационному состоянию, допустимому по условиям обеспечения безопасности дорожного движения: утв. Постановлением Госстандарта России от 11 октября 1993 г. № 221. М.: ИПК Издательство стандартов, 1993.
12. Руководство по борьбе с зимней скользкостью на автомобильных дорогах [Электронный ресурс]: утв. Распоряжением Минтранса Рос. Федерации от 16 июня 2003 г. № ОС-548-р. Доступ из справ.-правовой системы «КонсультантПлюс».

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

Карпика А. Г.,
доцент кафедры
информационного обеспечения
ОВД, канд. тех. наук, доцент;
Петрищева Е. Н.,
преподаватель кафедры
информационного
обеспечения ОВД
(РЮИ МВД России)

Современные Интернет браузеры представляют собой комплексные программные решения, позволяющие пользователям решать широкий круг прикладных задач. Принцип модульной архитектуры, использующийся до этого в десктопных приложениях, в последние 10 лет стал нормой и для рассматриваемого круга приложений.

Несомненно, предоставление пользователю права конфигурирования программного продукта исходя из собственных целей и задач, является оправданным не только с технологической и коммерческой сторон, но и с точки зрения потребителей. При этом производитель программного продукта получает возможность создания сравнительно компактного и быстрого приложения, оптимально сконфигурированного для решения большинства задач, а реализация всех дополнительных функций, расширяющих возможности программы, отдается независимым производителям. Конечный пользователь, устанавливая дополнительные модули, действует самостоятельно, на свой «страх и риск».

Наименования модулей, расширяющих функционал браузеров, отличается в наиболее популярных программных продуктах, но механизм работы основных видов модулей схож.

Если задача модуля состоит в преобразовании результата обращения к ресурсу в альтернативный вид, модуль перехватывает обращение браузера, вносит изменения в отображение содержимого веб-страницы (например убирает рекламные баннеры) и возвращает веб-страницу пользователю.

При выполнении функции анонимайзера модуль подключается к удаленному прокси-серверу и направляет запрос браузера и ответ от посещенного ресурса через ресурс-посредник.

Независимо от того, какую задачу решает установленный модуль, его версия периодически обновляется. Таким образом, в обоих рассматриваемых случаях предполагается обмен данными между компьютером пользователя и производителем установленного модуля. Именно этот

факт делает их использование потенциально опасным для пользователя. Дополнительные модули в последнее время активно используются мошенниками как средство внедрения в компьютерную систему пользователя с целью реализации шпионских функций, либо рекламу продвижения информационных услуг третьих лиц, рассылки спама.

По информации компании Яндекс, примерами работы подобных модулей являются: агрессивная реклама, «всплывающая» на посещаемых веб страницах; подмена или добавление новых рекламных блоков на популярных веб-ресурсах (поисковые агрегаторы, социальные сети). При этом вредоносные модули могут демонстрировать откровенно мошенническую, или воздействующую на подсознание рекламу. Встречаются и другие действия, например, автоматическое открытие вкладки с определенным адресом ресурса, подмена поиска по умолчанию, сбор личных данных пользователя. Тенденция последних лет – майнингкриптовалют без ведома пользователей пораженных компьютеров.

Сложившаяся ситуация заставила разработчиков браузеров заняться вопросом безопасности пользователей, устанавливающих дополнительные модули. Пойти на это их заставило то, что большинство пользователей при первых признаках ухудшения работы компьютерной системы в глобальной сети отказывалось от использования текущего браузера, что влияло на его популярность и окупаемость инвестиций. Особенно этот вопрос актуален для браузеров, занимающих сравнительно небольшую нишу на этом рынке.

Анализ источников позволил обобщить методы, применяемые злоумышленниками, направленные на внедрение вредоносных модулей в браузеры и ответные действия разработчиков браузеров.

Так сложились обстоятельства, что лидирующей платформой для построения Интернет браузеров в настоящий момент является проект с открытым исходным кодом Chromium. На его базе разработано 27 браузеров, 22 из которых являются активными. Наиболее известными представителями в глобальном Интернете являются: GoogleChrome, Opera. В пространстве Рунета: Яндекс.Браузер. В Китайском Интернет пространстве – BaiduSpark. По данным ресурса www.netmarketshare.com в 2017 году большинство пользователей глобального пространства Интернет (почти 60 %) выбрало браузер Chrome (Таблица 1), что свидетельствует о существенном отрыве данного программного продукта от конкурентов.

Таблица 1.

Распространенность Интернет браузеров

Браузер	Мировой Интернет (%)	Рунет (%)
Chrome	**59,49**	**52,91**
MS Internet Explorer (MS Edge)	16,84 (5,65)	**1,94** (**1,64**)
Opera	**1,25**	**4,11**
Safari	3,72	14,17
Firefox	12,02	5,82
Яндекс Браузер	**1**	**15,45**
Другие	2	4

Несмотря на то, что оценки различных аналитических ресурсов несколько отличаются друг от друга, общая картина примерно схожа: браузеры, разработанные на платформе Chromium, занимают от 60 % до 76,05 % рынка. Учитывая эти обстоятельства, становится понятно, почему большинство модулей, расширяющих возможности браузеров, разрабатываются именно для этой платформы.

Одним из способов, которые злоумышленники теоретически могут использовать для внедрения вредоносного модуля в браузер является взлом аккаунтов ChromeWebStore, являющегося магазином приложений для браузера, созданного на этой платформе.

Реализация этой угрозы позволяет получить доступ к ресурсам конкретного разработчика, что может привести к подмене оригинальной версии версией модуля, содержащей вредоносный код. При этом опасность кроется не только для новых пользователей, но и для тех, кто установил модуль раньше, например, если вредоносная версия будет более новой, чем установленная.

Следующий способ внедрения заключается в том, что вредоносный модуль попадает в браузер не через штатную установку из магазина приложений, а вследствие «деятельности» сторонней программы, ранее внедренной в компьютер пользователя. Программа устанавливала в браузер модуль с идентификационным регистрационным номером идентичным оригиналу. Версия устанавливаемого модуля изначально искусственно завышена с целью избежать его замены оригинальным модулем при его обновлении.

Одним из наиболее используемых способов размещения вредоносных модулей в каталоге является эксплуатация злоумышленниками его открытости для WebStore свободного добавления модулей расширений. При этом для размещения модуля его премодерация не производится. Через определенное, достаточно короткое время, подобные модули

выявляются и помещаются в «черный список», но если злоумышленник разместил достаточно много копий, то у него есть шанс внедрить часть из них в компьютеры жертвы.

Достаточно опасным для пользователя и одновременно эффективным с точки зрения незаконной деятельности, является заявленная в проекте Chromium принципиальная возможность установки браузера и модулей расширения в «теневом» режиме. Для этого используются стандартные средства «групповых политик», применяемые для развертывания программного обеспечения в организации. Как известно, «теневой режим» предполагает установку, обновление и удаление программных продуктов без уведомления конечного пользователя, при этом теоретически возможна ситуация, когда в «групповых политиках» может быть прописан запрет на удаление программного обеспечения. В этом случае пользователь не сможет стандартными средствами операционной системы удалить установленные модули.

Помимо рассмотренного направления, злоумышленники активно пытаются внедрить вредоносные приложения в мобильные устройства пользователей. Известно, что наибольший интерес у них, в силу проводимой открытой политики разработчиков, вызывает операционная система Android.

Злоумышленники используют разнообразные способы, затрудняющих автоматическое, или полуавтоматическое исследования мобильных приложений. На этом фоне выделяют следующие наиболее распространенные способы маскировки вредоносных мобильных приложений: обфускация, шифрование символов, противодействие декомпилятору.

Обфускация – это искусственное усложнение кода программы. Применение этого способа позволяет злоумышленнику не изменяя функциональность программного продукта, сделать код «нечитаемым», непонятным для анализа.

Символы (символьные строки), содержащиеся в анализируемой программе, могут содержать важнейшую информацию об авторе, цели написания вредоносной программы (например, адрес удаленного сервера, номер криптокошелька, языка потенциальных жертв). Для шифрования строк злоумышленники используют широкий спектр алгоритмов, начиная с типовых, на основе XOR, Base64, ROT13, заканчивая алгоритмами на основе криптографических стандартов DES и AES.

Противодействие декомпилятору, как правило, осуществляется сочетанием «протекторов» с «обфускаторами». Протекторы не позволяют декомпилировать программу стандартным способом, поэтому время «жизни» подобной программы в магазине приложений и в устройстве пользователя может значительно возрасти.

Способы преодоления рассмотренных видов «защиты» злоумышленниками своих программных продуктов базируются на статическом и динамическом (поведенческом) видах анализа. Подробнее об их применении описано в [1] .

Таким образом, распространение вредоносных приложений в современном Интернет пространстве происходит всеми доступными злоумышленникам способами: через Интернет браузеры, приложения для мобильных устройств, посредством размещенных на веб ресурсах java скриптов, а также через зараженные документы Office и AdobeReader. Компания «Лаборатория Касперского» провела рейтинг способов внедрения вредоносного кода в компьютеры пользователей в 2017 г. [2] Результат представлен в таблице 2.

Таблица 2

Рейтинг способов внедрения вредоносных программ

Место в рейтинге	**Путь (способ)**	**Доля (%)**
1	Интернет браузер	38,63
2	Документы *Office*	26,15
3	Приложения для ОС *Android*	22,30
4	*Java*-скрипты	6,29
5	*Adobe Flash*	4,94
6	Документы «*pdf*»	1,68

Видно, что бесспорными «лидерами» в этой области выступают представители наиболее часто используемых пользователями информационных технологий: Интернет, офисных и мобильных. Это позволяет оптимизировать усилия, направленные на предупреждение и предотвращение киберпреступлений, связанных с распространением вредоносных программ.

_____

1. Скулкин О. Принципы обнаружения вредоносных приложений для Android [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/principles_detection_malicious_applications_Android (дата обращения: 2 апреля 2018 г.).

2. Развитие информационных угроз во втором квартале 2017 года. Статистика [Электронный ресурс]. URL: https://securelist.ru/it-threat-evolution-q2-2017-statistics/79226 (дата обращения: 2 апреля 2018 г.).

ОСНОВНЫЕ НАПРАВЛЕНИЯ И ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ДОРОЖНО-ТРАНСПОРТНЫХ ПРЕСТУПЛЕНИЙ

Матросова Л. Д.,
начальник кафедры ИТвДОВД,
канд. юрид. наук
(ОрЮИ МВД России
имени В. В. Лукьянова)

Состояние борьбы с преступностью в нашей стране настоятельно требует поиска принципиально новых подходов к раскрытию и расследованию преступлений, что непосредственным образом связано как с совершенствованием частных методик, так и с учетом возможностей использования компьютерных технологий, т. е. специализированных аппаратно-программных комплексов (АПК), построенных на основе законов логики, математического аппарата, теории информации, реализованных на базе компьютерной техники (КТ) в виде экспертных и автоматизированных информационно-поисковых систем (АИПС), интегрированных банков данных регионального и федерального уровней (АБД-Р, ИБД-Ф), автоматизированных рабочих мест (АРМ), а также возможностей как локальных, так и глобальных компьютерных сетей. Предназначение данных АПК – сбор, хранение и переработка служебной информации, используемой в процессе управления деятельностью ОВД и при раскрытии и расследовании преступлений. Такой подход позволяет коренным образом улучшить и ускорить процесс переработки оперативно-следственной информации, обусловливает значительное повышение эффективности проводимых мероприятий по розыску и изобличению преступников, установлению всех обстоятельств совершения преступления.

Эффективное расследование дорожно-транспортных преступлений предполагает оперативный анализ объемных информационных массивов, которые имеют тенденцию постоянно возрастать. Уровень нагрузки на следователей повышается, что приводит к их перегрузке и, как следствие, значительному увеличению сроков, сокращению объема и качества предварительного расследования, о чем свидетельствуют следующие цифры: в 2016 году в России зарегистрировано 173694 дорожно-транспортных происшествий; в суды направлено 89226 уголовных дел о нарушениях Правил безопасности дорожного движения и (или) эксплуатации транспортных средств, из которых 15,3 % возвращены на дополнительное расследование, а по некоторым регионам эта цифра доходит до 90 %. С 2011 по 2016 гг. нагрузка на следователей, специализирую-

щихся на расследовании ДТП, увеличилась с 21 до 37 уголовных дел, что не дает возможности всегда принимать оптимальные решения, повышает вероятность совершения ошибок при выдвижении следственных версий и их проверке, при подготовке и производстве отдельных следственных действий, например, осмотра места совершения дорожно-транспортного преступления.

Производство осмотра места совершения ДТП требует, чтобы все следователи правильно понимали его сущность, цели и задачи.

В ст. 176 УПК РФ сформулированы общие цели осмотра, как основания к его производству. Грамматический и семантический анализ позволяет толковать эту норму как допускающую разрешение двуединой задачи осмотра: во-первых, методами обнаружения, т. е. непосредственного восприятия явных, очевидных, материально фиксированных остаточных следов преступления; во-вторых, методами выяснения обстановки происшествия и иных обстоятельств, которые не явны, но требуется их установить в связи с осматриваемым местом, понять и зафиксировать.

Непосредственное восприятие следователем места совершения ДТП и фиксирование того, что очевидно, является важной, но лишь первоначальной задачей осмотра, не исчерпывающей всех целей криминалистического исследования обстановки места совершения ДТП. Восстановление механизма совершения ДТП и получение о нем фактических данных, прежде всего зависят от качества проведенного осмотра, полноты собранных следов и объектов, имеющих и могущих иметь отношение к дорожному событию. Соблюдение данных требований позволит обойти стороной необходимость назначения повторного осмотра места совершения ДТП.

Полагаем, что главной задачей осмотра места совершения ДТП является выяснение обстановки места совершения ДТП и механизма его совершения. В процессе осмотра следователю необходимо перейти от решения первоначальной задачи восприятия и описания непосредственно наблюдаемых объектов и фиксирования последствий ДТП к установлению породивших их причин и объяснению внутреннего взаимодействия элементов обстановки места ДТП и развития механизма дорожного события.

Криминалистическое исследование обстановки места ДТП предполагает выяснение вида (наезд, столкновение и т. д.) и механизма развития ДТП. Выяснение механизма дорожного события конкретизируется в виде подзадач, в процессе решения которых устанавливаются фазы развития ДТП на основе фактических данных, обнаруживаемых при следственном осмотре.

Традиционно сложившееся понимание криминалистического исследования при осмотре места преступления, сводившее это сложное

следственное действие лишь к непосредственному восприятию очевидной обстановки, следов и объектов, могущих иметь доказательственное значение, не способствует повышению эффективности расследования преступлений, особенно при расследовании преступлений, связанных с нарушением Правил дорожного движения и (или) эксплуатации транспортных средств.

Многие элементы обстановки места ДТП и его механизма могут не отражаться в каких-то специфических следах, а значит, их нельзя обнаружить непосредственным восприятием. Например, для установления объективной возможности увидеть с места водителя возникшую опасность нередко требуется моделирование в пространстве дороги границ аварийной фазы развития события, а также установление расчетного положения транспортного средства на дороге в момент появления опасности для движения и расстояния, на котором находилось транспортное средство от препятствия во время его обнаружения водителем. Все эти факторы объективны и материальны. Однако их установление при осмотре места ДТП возможно не по следам, так как таковых может и не быть, а посредством опросов очевидцев, соответствующих расчетов на основе закономерностей движения, опытных действий в обстановке места ДТП для проверки их реальности.

Представляется, что следователь на месте ДТП обязан не просто фиксировать то, что попадается на глаза, а сопоставлять с картиной происшедшего, анализировать и на основе этого приходить к каким-либо умозаключениям. Имеется острая необходимость разработки рекомендаций по использованию опосредствованных технических приемов и методов криминалистического исследования места совершения ДТП.

Сказанное позволяет интерпретировать криминалистическое понятие осмотра места совершения ДТП несколько шире, чем непосредственное восприятие следователем очевидной обстановки и следов.

На наш взгляд, осмотр места совершения ДТП представляет собой следственное действие, производимое в соответствии с уголовно-процессуальным законом следователями и другими, указанными в законе лицами, посредством применения криминалистических методов и приемов для исследования материальной дорожной обстановки (дорожного полотна, транспортного средства, трупа, механизма совершения ДТП и других объектов, имеющих отношение к расследуемому событию) в целях обнаружения, фиксации и изъятия фактических данных, необходимых для установления обстоятельств совершения дорожно-транспортного преступления и лиц, виновных в его совершении.

В обобщенном виде можно говорить о наиболее типичных задачах осмотра, характерных для всех видов ДТП, которые, на наш взгляд, можно разделить на следующие категории:

– задачи, решаемые после получения сообщения о совершении ДТП;

– задачи, решаемые по приезду СОГ на место совершения ДТП;

– задачи, решаемые непосредственно в процессе осмотра места совершения ДТП.

К первой категории задач мы относим:

– обеспеченность СОГ лицами, проводящими осмотр места совершения ДТП, а также необходимыми для этого техническими средствами;

– обеспечение своевременного выезда СОГ на место совершения ДТП.

– Вторую категорию задач составляют:

– оказание помощи пострадавшим, если она им еще не оказана;

– удаление с места ДТП посторонних лиц;

– установление очевидцев ДТП, а также лиц, управлявших транспортными средствами, причастных к ДТП;

– выяснение у очевидцев, участников ДТП и работника ГИБДД, первым прибывшего на место ДТП:

– времени, характера и обстоятельств совершения ДТП;

– не подвергалась ли дорожная обстановка на месте совершения ДТП изменениям, если да, то – характер изменений, кем и в связи с чем они были произведены;

– в каком направлении скрылось лицо, управлявшее транспортным средством, причастным к ДТП, его приметы. Вид, номерной знак и характерные приметы транспортного средства. Организация его преследования «по горячим следам»;

– принятие мер к сохранности обстановки места совершения ДТП до окончания следственного осмотра;

– ознакомление с общей дорожной обстановкой на месте совершения ДТП;

– определение границ и объектов осмотра места совершения ДТП;

– определение порядка и тактики производства осмотра места совершения ДТП;

– приглашение для участия в осмотре понятых и разъяснение им их прав и обязанностей.

Последнюю категорию задач представляют:

– непосредственное восприятие следователем обстановки места совершения ДТП и фиксирование в протоколе всего того, что очевидно;

– выяснение вида и механизма развития ДТП;

– обнаружение, фиксирование и изъятие с предварительным исследованием следов и объектов, могущих иметь доказательственное значение;

– определение технического состояния транспортных средств, причастных к совершению ДТП;

– изучение, анализ, оценка полученной информации с целью выдвижения следственных версий об обстоятельствах совершения ДТП;

– установление наличия причинных связей между нарушениями Правил дорожного движения и (или) эксплуатации транспортного средства и наступившими общественно опасными последствиями;

– установление причин и условий, способствовавших совершению ДТП.

Приведенный перечень задач является типичным, характерным для исследования обстановки места ДТП лишь в общем случае. Он может быть уточнен и дополнен в зависимости от вида ДТП и вызванных им последствий. Например, в случае опрокидывания транспортного средства, необходимо дополнительно зафиксировать состояние дорожного полотна (наличие горюче-смазочных материалов, гололеда и т. д.), техническое состояние тормозной системы, рулевого управления, шин колес ТС и т. д.

Полагаем целесообразным несколько подробнее остановиться на ситуации, касающейся розыска лица, скрывшегося с места совершения им ДТП.

Производство оперативно-розыскных мер требует применения специальных средств и методов:

– производство оперативных осмотров помещений, зданий, сооружений, например, по месту жительства и работы разыскиваемого лица, а также участков местности и транспортных средств, связанное с визуальным, слуховым и иным изучением (исследованием) данных объектов, в том числе с использованием специальных технических средств и иных средств, с целью получения информации, имеющей значение для решения задач оперативно-розыскной деятельности;

– опрос граждан, которые осведомлены или могут знать о местонахождении скрывшегося лица;

– изучение различных документов (в том числе архивных), направление запросов в государственные органы, предприятия, учреждения и организации, а также использование возможностей криминалистических и оперативно-розыскных учетов ОВД.

В период первоначальной проверки с целью выявления разыскиваемого ТС, подразделениями ОВД, задействованными в розыске, осуществляется:

– получение по учетам ГИБДД установочных данных на транспортные средства и их владельцев, предположительно участвовавших в совершении ДТП, оперативная отработка данной информации:

– проверка возможных мест ремонта транспортных средств, обращений для получения страхового возмещения;

– установление лиц, эксплуатирующих по доверенности выявленное по учетам транспортное средство;

– направление розыскных заданий, ориентировок в близлежащие ОВД, внештатным сотрудникам полиции, работникам жилищно-коммунальных органов, представителям общественных правоохранительных организаций на установление разыскиваемого транспортного средства и лица, управлявшего им во время совершения ДТП.

Необходимо отметить, что в отличие от мест совершения других преступлений, место совершения ДТП имеет ряд особенностей, а именно: как правило, ДТП имеют место на проезжей части дороги с интенсивным движением транспортных средств и пешеходов, что иногда приводит к изменению обстановки их совершения с необратимой утратой многих следов преступления. Это происходит по различным объективным и субъективным причинам: по вине водителя, заинтересованного в благоприятном для него исходе дела; вследствие воздействия других транспортных средств, пешеходов или атмосферных осадков на следы и иные объекты, могущие иметь доказательственное значение. В связи с этим, возникает необходимость приступать к осмотру места ДТП незамедлительно, вслед за получением сообщения о нем. По данной категории преступлений, особое значение при их расследовании имеют оперативность и быстрота проведения неотложных следственных действий.

Общественно опасные последствия ДТП возникают вследствие взаимодействия следующих элементов системы дорожного движения: дорожной обстановки, транспортного средства, водителя и пешеходов. Каждый из этих элементов до момента наступления опасной для дорожного движения ситуации действует самостоятельно, но в условиях ее наступления их действия часто «переплетаются». Механизм действий вышеназванных элементов до наступления опасной ситуации и их взаимодействия в ее период, продолжающийся обычно незначительное время (доли секунд), требует от участников осмотра места ДТП весьма тщательного и всестороннего подхода к его реконструкции.

Программистами предприятия «МАК» г. Волгограда разработана специализированная программа «Расследование дорожно-транспортных преступлений», которая по своим функциональным возможностям позволяет составлять план расследования, по результатам выполнения которого формируется база данных с последующим использованием ее записей; подготавливать и выводить на печать процессуальные документы по уголовному делу.

Кроме того, в органах предварительного расследования активно эксплуатируется модульная и сетевая версии Специальной Информационной Системы (СИС), функциями которой являются формирование до-

кументов по уголовным делам, контроль сроков предварительного расследования, архивирование материалов уголовных дел, учет уголовных дел, учет лиц, обвиняемых (подозреваемых) в совершении преступления, потерпевших и свидетелей, формирование статистических документов. Однако, главный недостаток этой системы видится в том, что по своему назначению она охватывает не все стороны процесса расследования преступления, а только лишь уголовно-процессуальную и организационно-управленческую, а ведь не менее важна и аналитическая сторона данного процесса.

В целях восполнения этого пробела была создана автоматизированная информационная система (АИС) службы расследования «РАКУРС» (Расследование, Анализ, Контроль, Учет Работы, Статистика), предназначенная для функционирования как в сетевом, так и в модульном режиме в целях информационного обеспечения деятельности следователей по раскрытию и расследованию отдельных видов преступлений (в том числе дорожно-транспортных), рационализации их труда при подготовке и оформлении процессуальных документов, анализа доказательств по уголовным делам, учета работы и составления статистических и иных отчетов о деятельности следователей.

Одной из основных подсистем, с которой чаще всего приходится работать пользователю АИС «РАКУРС», является подсистема «Задачи», содержащая следующие группы задач:

- планирование расследования.

Информационное обеспечение процесса планирования расследования преступления и производства отдельных следственных действий. На основе анализа первичной информации о совершенном преступлении система предлагает версии, для каждой из которой предусмотрена база данных, содержащая информацию об обстоятельствах, подлежащих выяснению, и средствах их установления (следственные действия, оперативно-розыскные и иные мероприятия);

- процессуальные документы по уголовному делу.

Информационное обеспечение процесса принятия следователем отдельных процессуальных решений на первоначальном и последующем этапах расследования преступления, а также для процессуального оформления этих решений с использованием компьютера для последующего их использования. Система имеет следующие формы ввода (бланки процессуальных документов): постановления (о возбуждении уголовного дела, о назначении различных видов судебных экспертиз, о признании потерпевшим и т. д.), протоколы (допросов, очной ставки и т. д.), различные виды запросов, писем, сообщений, требований.

На завершающем этапе расследования преступления пользователь (следователь) имеет возможность подготовить постановление о продлении сроков предварительного расследования и содержания обвиняемых

под стражей, постановление о прекращении или приостановлении уголовного дела, обвинительное заключение, а также ряд других процессуальных документов.

По окончании формирования, указанные документы могут быть выведены на принтер или в текстовый файл. По желанию пользователя они либо сохраняются в базе данных с целью дальнейшего их использования, либо удаляются.

Анализ и оценка доказательств

В данном блоке пользователю представлена возможность провести всесторонний анализ и дать оценку доказательствам, собранным в ходе проведения тех или иных следственных действий.

Кодексы, другие нормативные акты, юридическая литература содержит нормативно-правовую информацию, регламентирующую производство предварительного следствия.

Выход в другие программы

Данный блок предусматривает выход в другие программные оболочки (например, текстовые редакторы, электронные таблицы, графические редакторы) с целью формирования в них процессуальных документов по уголовному делу.

Полагаем, что именно такого направления следует придерживаться при разработках специализированного программного обеспечения процесса раскрытия и расследования той или иной категории преступлений.

Помимо вышеуказанных, существуют и другие компьютерные системы оперативно-следственного назначения.

Представляется, что такое разнообразие автоматизированных систем одного и того же назначения, но с различными по сути подходами к их разработке не позволит, на наш взгляд, обеспечить в полном объеме все аспекты деятельности как отдельного сотрудника ОВД, так и подразделения в целом (кроме АИС «РАКУРС»). В связи с этим считаем, что созрела острая необходимость в определении единых требований к построению и функционированию специализированных компьютерных систем оперативно-следственного назначения для сотрудников ОВД (в том числе, для следователей, специализирующихся на раскрытии и расследовании ДТП).

На наш взгляд, программный комплекс вышеуказанных систем должен содержать подсистемы, которые по назначению можно разделить на вспомогательные и экспертные.

Вспомогательные подсистемы предназначены оптимизировать функциональные потребности пользователя (следователя, работника дознания) и могут быть представлены:

– программными средствами обработки текстовых и графических документов (текстовые и графические редакторы, программы проверки

правописания, сканирования и распознавания текстов и изображений, перевода текста с иностранного языка на русский и наоборот);

– системами управления базами данных, предназначение которых – поиск, обработка и хранение информации оперативно-следственного характера;

– системами, позволяющими осуществлять математическую обработку данных и хранение цифровой информации (электронные таблицы).

В настоящее время принято различать три типа опасностей, которым подвержена информация, обрабатываемая с помощью ПЭВМ:

– ошибки, допускаемые при сборе, передаче и использовании данных;

– искажение информации в результате саботажа, изменений данных и программ, а также смены персонала;

– потеря информации вследствие стихийных бедствий и несчастных случаев (наводнения, пожары, взрывы и т. д.), связанная с повреждением аппаратных средств компьютерной техники или утратой ее программного обеспечения.

В связи с этим, под мерами защиты информации мы понимаем комплекс средств, методов и мероприятий, направленных на исключение или существенное затруднение искажения, уничтожения или несанкционированного использования защищаемой информации. Данный комплекс должен предусматривать:

Организационные меры защиты:

– увеличение размеров контролируемой (проверяемой) зоны объекта компьютерной техники;

– ограничение доступа к промежуточным носителям информации и в помещения, где проводится обработка информации с использованием программно-аппаратных средств компьютерной техники;

– демонтаж незадействованных кабелей, телефонных и иных линий связи, имеющих выход за пределы контролируемой зоны объекта.

Технические меры защиты:

– применение систем активной защиты;

– экранирование помещений, отдельных аппаратных средств компьютерной техники;

– установка помехоподавляющих фильтров;

– использование в специальном (защищенном) исполнении основных и вспомогательных аппаратных средств КТ.

К первым могут относиться: системы телеобработки и подготовки данных, повышения достоверности и другие устройства обработки информации. Ко вторым – системы заземления и электропитания; средства и системы сигнализации (пожарной, охранной и т. д.), кондиционирова-

ния, звукозаписи и звуковоспроизведения речевой информации; контрольно-измерительная аппаратура.

Программные меры защиты – совокупность специальных программ, с помощью которых осуществляется:

– идентификация пользователя;

– разграничение доступа пользователей к обрабатываемым массивам служебной информации;

– предотвращение несанкционированного доступа с автоматической регистрацией его фактов и попыток;

– регистрация санкционированных обращений;

– коррекция защиты (изменение паролей, идентификаторов);

– автоматическое уничтожение остаточной информации на промежуточных носителях;

– защита от восстановления или попыток восстановления уничтоженной информации;

– защита от копирования обрабатываемой информации и копирования самих программ защиты;

– криптографическое преобразование информации по определенному алгоритму с целью ее хранения или передачи по каналам связи за пределы контролируемой зоны объекта компьютерной техники.

Аппаратные меры защиты, направленные на криптографическое преобразование информации, передаваемой по каналам связи за пределы контролируемой зоны объекта компьютерной техники, осуществляемое аппаратными средствами.

5. Программно-аппаратные меры защиты, к которым относится комплексное использование программных мер (специальных программ) и аппаратных средств, позволяющее осуществлять криптографическое преобразование отдельных файлов и групп файлов, передавать по каналам связи зашифрованную информацию. Данные меры позволяют обеспечить более высокий уровень защиты по отношению к программным мерам и меньшую трудоемкость по отношению к аппаратным.

Следует особо выделить меры защиты информации в локальных и распределенных компьютерных сетях, организация которых приводит к расширению круга лиц, участвующих в обработке служебной информации, что повышает вероятность ее утечки по техническим каналам, уничтожения либо искажения. К таковым, на наш взгляд, относится:

– ограничение доступа к обрабатываемой информации, а также к аппаратным и программным средствам КТ лиц, не имеющих непосредственного отношения к данной информации;

– исключение наводок опасного сигнала с информационных линий связи на провода и кабели, уходящие за пределы контролируемой зоны объекта КТ;

– внедрение систем криптографической защиты данных, записываемых на магнитные носители общей информационной базы и передаваемых по линиям связи между центральной ПЭВМ (сервером) и периферийными вычислительными комплексами;

– внедрение автоматизированных систем защиты от несанкционированного доступа к данным общей информационной базы центрального вычислительного комплекса, а также от компьютерных вирусов.

Безусловно, все применяемые программно-аппаратные средства защиты информации должны соответствовать определенным требованиям по защите от несанкционированного доступа к информации, и пройти на этот предмет специальные исследования.

Для всех сотрудников ОВД, и в первую очередь следователей и работников дознания, необходимы навыки принятия решений в сложных ситуациях, которые в настоящее время, приобретаются ими в основном уже в ходе служебной деятельности, хотя это должно происходить еще при обучении в вузах или на курсах повышения квалификации следственных работников.

Наиболее приемлемой и эффективной представляется компьютеризированная (в виде обучающих программ описательного типа, контрольно-обучающих программ текстового типа, имитационных контрольно-обучающих программ типа деловых игр, комбинированных программ, сочетающих в себе черты всех вышеперечисленных типов программ) форма получения таких навыков во время подготовки будущих сотрудников ОВД. На это же указывает Приказ МВД России от 29 марта 2005 г. № 215 «Об утверждении Инструкции о порядке проведения проверок образовательных учреждений высшего профессионального образования внутренних войск Министерства внутренних дел Российской Федерации» «... необходимо совершенствовать методики обучения, внедрять в учебный процесс новые эффективных методы и средства обучения»

Компьютерный курс обучения предусматривает следующие важные разделы:

– фаза создания такого курса, которая предполагает объединение разрозненных компьютерных программ для обеспечения освоения различных разделов изучаемой дисциплины;

– фаза выбора базовых подразделений, участвующих в создании автоматизированной системы обучения;

– фаза создания банка данных, служащих для наполнения курса модельными примерами.

С учетом данного алгоритма была разработана имитационно-обучающая программа «Расследование дорожно-транспортных преступлений», функционирование которой построено так, чтобы максимально учесть как можно больше реалий практической деятельности следовате-

лей и работников органов дознания по раскрытию и расследованию дорожно-транспортных преступлений.

Программа акцентирует внимание на следственных ситуациях и исследуемых версиях; предусматривает постановку вопросов о целях и задачах, на достижение которых направлено принимаемое по делу решение, а также об обстоятельствах, которые следует выяснить при расследовании ДТП и производстве определенного следственного действия или иного мероприятия. Таким образом, работающий с программой пользователь не сможет случайно получить неожиданный для себя результат, не имея представления о том, на получение какой информации в ходе следствия по делу ориентировано то или иное следственное действие.

Данная программа позволяет проводить новое расследование; продолжать ранее начатое расследование; формировать список целей, задач и проверяемых обстоятельств для дальнейшей конкретизации в зависимости от следственных ситуаций и версий, выбранных пользователем; осуществлять просмотр полученной в ходе следствия информации, а также списка известных лиц и предметов; выдавать советы по дальнейшему ведению расследования; вести пользователю «Записную книжку»; сохранять результаты расследования в файле; предоставляет список рекомендуемых для изучения законодательных и иных нормативных актов, а также специальной литературы по методике расследования преступлений данного вида.

Данная программа, на наш взгляд, может служить средством компьютеризированного обучения и контроля уровня профессиональной подготовки курсантов и слушателей образовательных организаций системы МВД России, а также практических работников следственных подразделений.

Полагаем, что именно компьютеризированная форма процесса обучения методике раскрытия и расследования ДТП позволит курсантам и слушателям образовательных организаций системы МВД приобрести те знания и навыки, которые столь необходимы им будут на практике в условиях роста количества совершения данного вида преступлений.

На наш взгляд, активное использование автоматизированных оперативно- справочных, розыскных и криминалистических учетов, а также разработка и внедрение в деятельность следственного аппарата специализированных компьютерных систем, построенных на основе общих требований, предъявляемым к ним, и содержащих нормативно-правовую и методическую информацию, непременно обусловит эффективность системы информационного обеспечения всех стадий процесса расследования дорожно-транспортных преступлений и его оперативно-розыскного сопровождения.

АКТУАЛЬНЫЕ ВОПРОСЫ ПОСТРОЕНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ПОРТАЛА

Мишин Д. С.,
доцент кафедры ИТвДОВД,
канд. юрид. наук,
Паньков С. Л.,
начальник НИиРИО
(ОрЮИ МВД России
имени В. В. Лукьянова)

Создание и совершенствование элементной базы привело к развитию и повсеместному внедрению средств вычислительной техники. В дальнейшем, благодаря научно-техническому прогрессу, подобная тенденция позволила разработать и приступить к эксплуатации вычислительных сетей, что повысило оперативность обмена данными между сотрудниками, при решении сходных или взаимосвязанных задач, посредством обмена данными на локальном уровне в режиме реального времени. Развитие систем передачи данных способствовало развитию глобальных вычислительных сетей, позволяющих обеспечивать виртуальное взаимодействие между удаленными на значительное расстояние рабочими станциями и хранилищами информационных массивов. Повышение эффективности работы и качества принимаемых управленческих решений стало возможным благодаря использованию, посредством Интернет-технологий, систем распределенной обработки информации.

Требования, предъявляемые к вычислительным сетям, достаточно многогранны, но требуют обязательного соблюдения ряда условий. В первую очередь необходимо обеспечить совместную работу с информационными ресурсами всех зарегистрированных в вычислительной сети пользователей с обязательной централизацией систем управления доступом. При этом, в используемой телекоммуникационной системе, с целью снижения возможных рисков необходимо перманентное принятие мер направленных на повышение живучести, обеспечение адекватного реагирования на возникающие инциденты, а также соблюдение пользователями установленных правил работы.

Соблюдение указанных условий значительно упрощается после разработки и последующего внедрения в эксплуатацию корпоративного портала, структура и содержание которого формируются в соответствии с настоящим и перспективным содержанием информационных массивов. Кроме того, порталу необходимо обеспечить, в соответствии с потребностями пользователя, динамичное отображение данных для решения поставленных оперативно-тактических и стратегических задач [1].

Современное программное обеспечение, используемое в телекоммуникационных системах, позволяет реализовать поставленные задачи посредством продуктов с элементами искусственного интеллекта, а также реализации управления информационными ресурсами самим владельцем. В рассматриваемой архитектуре корпоративного портала связь между программным обеспечением и информационным массивом предоставляет пользователю помощь в процессе построения запроса и предоставляет исчерпывающий ответ.

В целом, для создания корпоративного портала необходима реализация целого ряда требований. В первую очередь, для повышения целесообразности решаемых задач и проектов, необходимо определение требований, как к самому порталу, так и к коммуникационной среде. На следующем этапе обеспечивается опытная эксплуатация продукта, а с целью исследования возможности его совместного использования в ней участвует максимальное число сотрудников. Еще одним существенным требованием, необходимым для повышения результативности использования портала, является наличие комплекта документов, определяющих особенности эксплуатации, ответственных лиц и основные принципы работы. Кроме того, целесообразно определить методику, предназначенную для проведения оценки используемого программного продукта.

Корпоративный портал предназначен для повышения оперативности сбора и обработки данных посредством использования автоматизированных систем управления. К основным задачам системы можно отнести повышение эффективности управления с одновременной реализацией в используемых массивах данных вопросов доступности, полноты и достоверности. Таким образом, создаваемая среда может стать базисом для наполнения и управления информационными массивами, а также позволит создать динамический потенциал и разработать стратегию дальнейшего использования. Обеспечение взаимодействия между находящимися на значительном удалении рабочими станциями возможно вследствие как развития собственной телекоммуникационной сети [2], так и использовании глобальной вычислительной сети с обязательным обеспечением шифрования каналов связи.

Распределенные системы управления, используемые корпоративными порталами, можно рассматривать в качестве созвездия взаимосвязанных единиц, что предоставляет пользователям возможность наполнения информационных массивов. К основным принципам рассматриваемой стратегии можно отнести:

1. Принцип автономности, позволяющий обеспечивать самостоятельное управление информационными массивами портала;

2. Принцип координации, позволяющий обеспечивать обмен данными между информационными массивами, а также отражать информацию по осуществляемому запросу.

Задача корпоративного портала, используемого организацией, должна заключаться в отображении информации о достижениях, предоставлении форм необходимых документов и отчетов о выполненных работах, а также предоставлении возможности как служебного, так и неформального общения.

Предоставление запрашиваемых пользователем данных обеспечивается информационным массивом, за управление которым с концептуальной и технологической точек зрения отвечает конкретное должностное лицо. Используемое в предлагаемой архитектуре программное обеспечение-агент имеет четкое знание о содержании конкретного информационного массива, а также связанных с ним хранилищах. Основными функциями данных программных продуктов являются оказание помощи пользователю в создании информационного запроса и ответ на запросы, поступающие от других узлов.

Программно-аппаратное обеспечение корпоративного портала предоставляет возможность определять оптимальные комплексные решения, преследующие цель повышения эффективности взаимодействия пользователей. В тоже время, от корпоративных порталов кроме процессов консолидации требуется наличие возможности обеспечения управления информационными массивами отдельными пользователями. То есть, портал с одной стороны обеспечивает инфраструктуру управления информационными массивами, а с другой, стороны это не является определяющим фактором в процессе эксплуатации.

В настоящее время в процессе использования корпоративных порталах достаточно острот стоит проблема обеспечения информационной безопасности. К наиболее оптимальным средствам, применяемым для обеспечения безопасности информации, можно отнести уже достаточно популярные системы обнаружения атак, включающие в свой состав различные элементы и модули. Один из наиболее важных модулей, от которого напрямую зависит эффективность функционирования системы, является обеспечение распознавания атак.

Методы анализа, применяемые в работе системы обнаружения атак, оказывают значительное влияние на эффективность ее работы. Если на момент введения в эксплуатацию подобных систем применялись статистические методы, то в настоящее время разработаны новые методики широко использующие не только нечеткую логику, но и нейронные сети.

Своевременное определение аномалий в процессе функционирования сети, связанное с возникновением неисправностей аппаратно-программных средств или деятельность хакеров является достаточно сложной задачей. Применяемые в настоящее время системы, реализующие анализ потоков, обеспечивают выявление уже известных аномалий на основании хранящихся в базе сценариев возможных атак, а вновь

разработанные процедуры остаются без внимания. Причина этого кроется в ограниченности используемых характеристик потоков данных и методов их анализа [3].

На основании этого представляется целесообразным построение системы обнаружения атак на основе использования нейросетевых методов анализа, одним из основных элементов которого является нейросетевой анализатор. Для обеспечения его эффективной работы необходимо в процессе обработки сетевых протоколов обеспечить выборку характеристик протекающих сессий, а также IP-адресов пользователей. Полученная в результате анализа действующих сетевых потоков и имитации по различным сценариям атак на сеть обучающая выборка может быть использована в процессах обучения и самообучении нейронных сетей.

Процесс обнаружения аномалий, используемый в нейронной сети, основан на обязательном создании профиля авторизованного пользователя, содержащего, в том числе, распределение выполняемых команд. Подобное требование связано с отличающейся у каждого пользователя тенденцией использования режимов работы в процессе выполнения служебных задач. При нейросетевом анализе потоков данных проводится классификация в процессе которой проводится сравнение текущей активности пользователя с различными сценариями сетевых атак, неопознанными или аномальными ситуациями.

Используемая архитектура нейронной разделяется на два основных уровня обработки данных. На первом уровне обеспечивается обработка различных одиночных сессий (IP-адресов отправителей и получателей пакетов), анализируются потоки с аномальными характеристиками и обеспечивается их обобщение данных для принятия решения на втором уровне.

В заключение следует сказать, что использование, созданного для решения возникающих задач, корпоративного портала дает возможность повысить оперативность управления с последующим повышением эффективности выполнения поставленных задач. Использование систем обнаружения атак для обеспечения безопасности информации в корпоративных порталах позволяет дать объективную оценку текущего уровня защищенности информационных активов. Выполнение выработанных рекомендаций будет способствовать повышению уровня обеспечения информационной безопасности и снижению потенциальных потерь благодаря повышению устойчивости функционирования телекоммуникационной среды, в целом, и корпоративного портала, в частности.

---

1. Мишин Д. С. Проблемы автоматизации процессов сбора и обработки данных в корпоративном портале // Наука и практика. 2016. № 2 (67). С. 136–138.

2. Мишин Д. С., Масалыгин К. К., Ставцева А. Г. Автоматизация сбора и обработки данных в корпоративном портале промышленного предприятия // Информационные системы и технологии. 2015. № 3 (89). С. 71–77.
3. Теоретические и прикладные аспекты защиты объектов информатизации / Под ред. Е. М. Сухарева. Кн. 5. М.: Радиотехника, 2007. 208 с. (Сер. Защита информации. Редактор Е. М. Сухарев.)

ОПИСАНИЕ ВОЗМОЖНОСТИ СОЗДАНИЯ СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В ГИБДД МВД РФ ПРИ ИСПОЛЬЗОВАНИИ СТАТИСТИЧЕСКИХ ДАННЫХ Д

Кузнецов А. С.,
преподаватель кафедры
ИТвДОВД, канд. тех. наук
(ОрЮИ МВД России
имени В. В. Лукьянова)

Одной из наиболее острых проблем безопасности человека в современном обществе является безопасность дорожного движения. Ввиду этого актуальность задачи снижения общего количества и тяжести последствий дорожно-транспортных происшествий в России и мире находится на высоком уровне. Внедрение и использование современных информационных технологий в повседневной деятельности органов отвечающих за решение задач в области безопасности дорожного движения позволяет более эффективно и качественно построить их работу.

Важной задачей статистики является разработка методики статистической оценки социальных явлений, которая осложняется тем, что многие социальные явления не имеют количественной оценки. Но, исследуя явления в самых различных областях, статистика сталкивается с зависимостями как между количественными, так и между качественными показателями, признаками. Так, существует сильная взаимосвязь между параметрами и характеристиками движения автотранспорта, технической исправности транспортных средств, состояния дорожной сети, технических средств организации дорожного движения, состояния подъездных путей, пешеходных переходов, погодных условий, культуры водителей и других данных [1].

Оперативность принятия управленческих решений порой является ключевым фактором успешного выполнения поставленной задачи. Внедрение многопараметрической информационно-аналитической системы моделирования прогнозирования ситуации в области обеспечения безо-

пасности дорожного движения (МИАС) позволило более эффективно решать следующие задачи [2]:

проводить мониторинг сложившейся ситуации в области безопасности дорожного движения в субъектах Российской Федерации и в России в целом;

анализировать динамику показателей административной практики, количества транспортных средств и других показателей сферы безопасности дорожного движения;

анализировать комплексную информацию по основным характеристикам (условиям, причинам, факторам, участникам и т. д.) дорожно-транспортных происшествий;

осуществлять анализ и формирование перечня наиболее проблемных направлений аварийности на автотранспорте;

выполнять мониторинг и анализ мест концентрации ДТП на федеральных автодорогах, а также определять перечень причин концентрации происшествий, в том числе неудовлетворительных дорожных условий на выбранном отрезке дороги.

Расчет аналитических показателей, характеризующих аварийность в конкретном регионе за различные периоды времени позволяет руководителю оценить и скорректировать работу подчиненных. Однако, на сегодняшний день не существует автоматизированной системы принятия управленческих решений. Руководитель должен самостоятельно оценить работу подчиненных исходя из ряда аналитических показателей, учитывая ряд внешних факторов.

Система интеллектуальной поддержки принятия управленческих решений может осуществлять формулировку выводов на основе полученных аналитических показателей и анализа внешних факторов без участия руководителя.

Одной из наиболее ответственных задач, возлагаемых на ГИБДД, является контроль за строительством и реконструкцией дорог и улиц, дорожных сооружений, железнодорожных переездов, линий городского электрического транспорта. При использовании МИАС оператор может получать данные о состоянии аварийности на различных участках федеральных автодороги, а также количество денежных средств, потраченных на ремонт или создание каждого такого участка. Часто приходится вычислять какой из участков дороги наиболее сильно нуждается в ремонте или установке дополнительных знаков и на каком из них проведение данных работ наиболее целесообразно с экономической точки зрение. Подготовка такого решения исходя из личных убеждений соответствующего руководителя не всегда является оптимальной.

Нахождение оптимального решения описанной выше задачи может выполняться системой интеллектуальной поддержки управленче-

ских решений в автоматическом режиме, при этом необходимо учитывать следующие факторы:

средняя цена ремонта участка дороги;

относительный показатель аварийности на данном участке дороги.

Среднюю цену ремонта можно вычислить как нахождение простого среднего по предыдущим показаниям.

Относительный показатель аварийности необходимо рассчитать, как отношение ДТП на конкретном участке дороги к сумме ДТП по всем участкам одной дороги в зоне ответственности конкретного субъекта управления (рисунок 1).

Рисунок 1. Схема автодороги.

Требуемым результатом является нахождение участка с наиболее высоким показателем аварийности и наиболее приемлемой ценой реконструкции.

Решение этой задачи можно выполнить путем применения метода неопределенных множителей Лагранжа для нахождения условного оптимума, который и будет являться искомым участком дороги.

Система интеллектуальной поддержки должна включать в себя ряд модулей ответственных за расчет и формулировку выводов в конкретной области управления. Представленная выше задача является только одним примером области, в которой использование автоматизированных систем анализа нескольких показателей позволяет наиболее оптимально выработать управленческое решение.

1. Матросова Л. Д. Вопросы использования статистических взаимосвязей в целях оптимизации деятельности Госавтоинспекции // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2017. № 1 (70). С. 124–127.

2. Семенов Е. Ю. Перспективы использования новых возможностей МИАС ГИБДД // Научно-аналитический журнал Наука и практика Российского экономического университета им. Г. В. Плеханова. 2016. № 1. С. 95.

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ АВТОМАТИЗАЦИИ ПРОЦЕССОВПЕРЕДАЧИ И ОБРАБОТКИ ВИДЕОИЗОБРАЖЕНИЙ В СИСТЕМЕКОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Орешин Н. А.,
канд. тех. наук, профессор,
Черепков С. А.,
канд. тех. наук,
Лазарев С. Н.,
доцент,
Евсеев Т. С.
(Академия ФСО России)

Сложная и динамично изменяющаяся социально-политическая, экономическая и военная обстановка в современном мире обуславливает необходимость резкого повышения уровня безопасного функционирования силовых структур России. Очевидно, что одним из возможных направлений решения данной проблемы является модернизация их автоматизированных систем управления (АСУ). Обобщенная модель АСУ силовых структур России показана на рисунке 1.

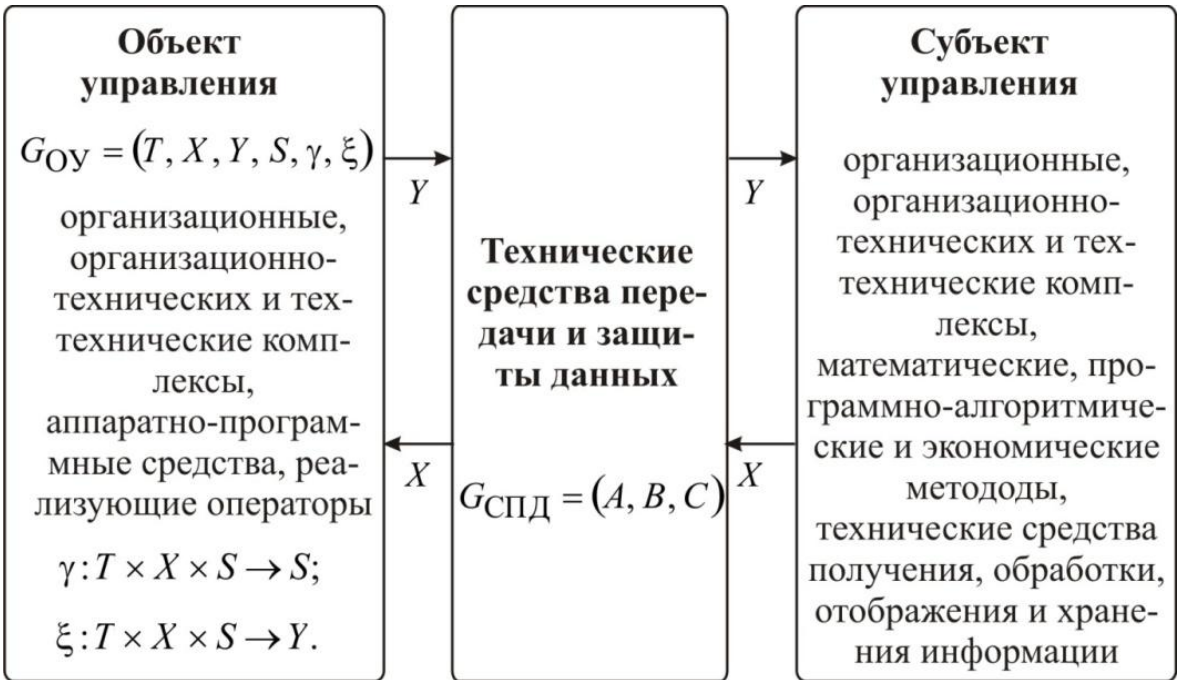

Рисунок 1. Обобщенная модель АСУ силовых структур России.

Основным предназначением АСУ силовых структур России является выработка субъектом управления (по результатам анализа выход-

ных сигналов $y_i \in Y$ объекта управления) необходимых воздействий $x_i \in X$ на объекты управления (ОУ) с целью получения максимального эффекта от их использования по назначению.

При решении рассматриваемой задачи в работе для объекта управления АСУ использована модель, предложенная отечественными учеными Р. М. Юсуповым и А. К. Дмитриевым, в виде упорядоченного множества [1]

$$G_{\text{îÓ}} = (T, X, Y, S, \gamma, \xi), \tag{1}$$

где T – множество моментов времени, в которые субъектом управления наблюдается объект управления;

X – множество входных сигналов, поступающих по техническим средствам передачи данных от субъекта управления к объекту управления и характеризующих воздействие субъекта управления на объект управления;

Y – множество выходных сигналов объекта управления, предназначенных для передачи их по цифровой сети к субъекту управления и отражающих реакцию объекта управления на входные воздействия;

S – множество состояний объекта управления;

γ – оператор переходов, отражающий механизм изменения состояния объекта управления под действием внутренних (состояний объекта управления S) и внешних возмущений X;

ξ – оператор выходов, описывающий механизм формирования выходного сигнала Y объекта управления как реакции его на внутренние (состояния объекта управления S) и внешние возмущения X.

Оператор переходов γ и оператор выходов ξ реализуют соответственно отображения

$$\gamma : T \times X \times S \to S; \tag{2}$$

$$\xi : T \times X \times S \to Y. \tag{3}$$

Анализ, проведенный в данной работе, показывает, что используемые в настоящее время современные АСУ силовых структур России признаны решать целый класс задач, связанных с автоматизацией следующих функций:

- управление служебной и оперативной деятельностью;
- кадровый учет;
- многоуровневый учет рабочего времени;

− расчет и оптимизация бюджета заработных плат;

− автоматизация документооборота и управление лицевыми счетами;

− управление задачами и поручениями;

− централизованное управление интегрированной системой охраны, включающей в себя подсистему контроля и ограничения доступа;

− видеонаблюдение и аудио контроль помещений;

− мониторинг использования персональных компьютеров;

− контроль телефонных соединений;

− запись телефонных разговоров и т. д.

Как показывает практика современные АСУ это территориально-распределенные системы. Они, наряду с управленческими аспектами, признаны решать целый класс задач, связанный с автоматизацией процессов, обеспечивающих необходимый уровень контроля и управления доступом персонала при тенденции удаления наблюдаемых объектов от центров управления и существенном увеличения их числа. Поэтому в АСУ силовых структур России можно выделить подсистему контроля и управления доступом, которую в дальнейшем будем исследовать как систему контроля и управления доступом (СКУД).

Как показывают исследования, функционирование СКУД силовых структур России направлено на выполнение следующих задач:

− мониторинг присутствия персонала и посетителей;

− автоматический вход-выход сотрудников подразделения через проходные по электронным картам в соответствии с графиками работы;

− вход посетителей и гостей по разовым картам под контролем оператора проходной с автоматическим возвратом разовой карты при выходе;

− проезд автотранспорта через контрольно-пропускные пункты (КПП) с обеспечением досмотра при въезде и выезде;

− автоматическое управление шлагбаумами и дорожными блокираторами на границах зоны досмотра;

− автоматический вывод на мониторы операторов информации о предъявителе электронной карты при входе или въезде на территорию;

− ручное управление проходными и КПП в нештатных ситуациях с фиксацией всех действий операторов в протоколе системы;

− автоматических контроль доступа в помещения предприятия, а также в отдельные помещения зданий и цехов;

− выдача, возврат и учет постоянных, временных и разовых карт доступа в бюро пропусков предприятия;

− автоматический учет рабочего времени для сотрудников предприятия, формирование отчетов по отработанному времени по стандартным формам;

− охрану территорий, зданий, оборудования и инженерных коммуникаций строительных объектов, объектов социальной инфраструктуры, а также контроль исполняемых функций;

− классификацию и распознавание людей, транспортных средств и предметов;

− автоматическое выявление нештатных ситуаций и событий при выполнении функций охраны и контроля;

− обеспечение оперативного принятия решений при обнаружении событий нарушения функционирования, попыток хищения материально-технических ценностей, выявлении подозрительных предметов или возникновении нештатных ситуаций и угроз.

Современные автоматизированные СКУД силовых структур России представляют собой организационно-технические системы (рисунок 2).

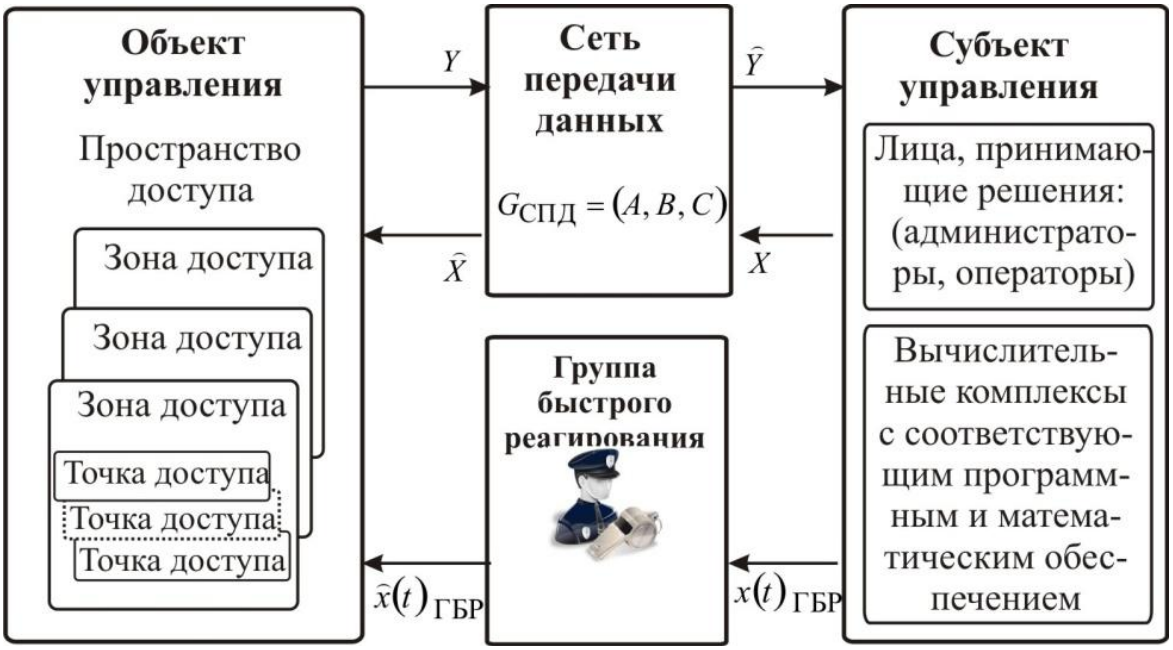

Рисунок 2. Обобщенная модель территориально-распределенной Автоматизированной системы контроля и управления доступом.

Основными элементами СКУД являются[2]:

− субъект управления: лица, принимающее решение (администраторы, операторы) и вычислительные комплексы с соответствующим программным и математическим обеспечением;

− объект управления (точки доступа, зоны доступа, пространство доступа);

− цифровая сеть, обеспечивающая передачу данных между объектами и субъектами управления;

− группа быстрого реагирования (ГБР).

Эта организованная совокупность людей и материальных средств преследует главную цель – наилучшим образом обеспечить контроль и управление доступом, под которым понимается комплекс мероприятий, направленных на ограничение и санкционирование доступа людей, транспорта и других объектов (далее объектов доступа) в (из) помещения, здания, зоны и территории.

В работе контроль и управление доступом рассматривается как процесс, реализуемый АСКУД и осуществляемый для выработки (по результатам наблюдений состояний точек доступа) необходимых воздействий на исполнительные устройства и группу быстрого реагирования с целью ограничения, и санкционирования перемещения объектов доступа через управляемые преграждающие устройства.

В работе в соответствии со стандартами приняты термины, имеющие следующие толкования [3].

Доступ – это перемещение людей, транспорта, дронов и других объектов в (из) помещения, здания, зоны и территории. При этом в работе будем различать как санкционированный, так и несанкционированный доступы.

Здесь под санкционированным доступом понимается доступ людей или объектов, имеющих права на это право, а под несанкционированный – доступ людей или объектов, не имеющих такого права.

Точка доступа (ТД) – место, где непосредственно осуществляется контроль доступа. Такими местами являются дверь (например, сейфа или кабинета), турникет, кабина прохода и другие средства, оборудованные считывателем, исполнительным механизмом, электромеханическим замком, электронными фотоаппаратами и видеокамерами.

Зона доступа (ЗД) – совокупность точек доступа, находящихся на территории, которая оборудуется средствами видеонаблюдения, электронным фотоаппаратом, считывателем, управляемым преграждающим устройством, исполнительным механизмом, электромеханическим замком, базой данных. Данная совокупность средств обладает технической, информационной, программной и эксплуатационной совместимостью.

Совокупность зон доступа, находящихся в сфере влияния СКУД будем называть пространством доступа (ПД). Для осуществления доступа на территорию ПД, а также для мониторинга состояния его территории, как и зона доступа, оно оборудуется средствами видеонаблюдения, электронным фотоаппаратом, считывателем, управляемым преграждающим устройством, исполнительным механизмом, электромеханическим замком, базой данных.

Здесь под средствами контроля и управления доступом понимаются любые механические, электромеханические, электрические, элек-

тронные устройства, конструкции и программные средства, обеспечивающие реализацию процессов контроля и управления доступом.

Основным предназначением АСКУД силовых структур является постоянный многоуровневый мониторинг состояния пространства доступа и выработка необходимых воздействий на исполнительные устройства и группу быстрого реагирования с целью ограничения, и санкционирования перемещения объектов доступа в пределах контролируемой территории (рисунок 2).

Как показано в работе, широкое внедрение в системы контроля и управления доступом средств видеонаблюдения (датчиков, регистраторов, серверов и т.п.) позволяет повысить эффективность и безопасность функционирования силовых структур России. Однако такой подход к модернизации систем контроля и управления обладает тремя основными недостатками.

Во-первых, на операторов налагается высокая нагрузка, и на практике её можно выдержать только в течение 2−3 часов, даже если камера наблюдения всего одна.

Во-вторых, необходимый поиск события в видеоархиве может быть проведён лишь при помощи длительного просмотра архива целиком.

В-третьих, увеличение числа наблюдаемых объектов и, следовательно, числа видеокамер, обуславливает необходимость передачи огромного объема потока видеоданных.

Поскольку объем передаваемой видеоинформации, необходимой для видеонаблюдения в режиме реального времени, весьма велик и по известным причинам постоянно возрастает, то вполне очевидно, что сегодня возникает проблема повышения эффективности функционирования СКУД при минимизации числа операторов с учетом потенциальных психофизиологических их особенностей.

Для решения задачи повышения качества контроля и управления доступом была произведена её формализация:

По заданной автоматизированной системе контроля и управления доступом в виде множества

$$Q_{\text{АСКУД}} = \left\{ S_{\text{ПД}}(t),\ X_{\text{ПД}}(t),\ Y_{\text{ПД}}(t), F_1,\ F_2,\ Q_{\text{ПД}},\right.$$

$$\left. Q_{\text{ОПП}},\ N_m^{N^m},\ N^m,\ \text{K}_{\text{ВП}}(t) \right\}, \tag{4}$$

элементами которого являются подмножества, характеризующие в момент времени $t \in T$:

– состояния пространства доступа $S_{\text{ÏÄ}}(t)$;

– входные воздействия $X(t)$ на пространство доступа;

– реакции пространства доступа $Y(t)$ на входные воздействия $X(t)$;

– структуру пространства доступа $Q_{\text{ÏÄ}}$;

– цветовое пространство пикселя $Q_{\text{ÖÏÏ}}$;

– поток видеокадров $\text{K}_{\text{ÂÏ}}(t)$;

– механизм изменения состояний точек доступа по входным воздействиям (оператор F_1);

– механизм формирования выходного сигнала (оператор F_2),

– а также величины, характеризующие количество точек $N_m^{N^m}$ в каждой m-ой зоны и количество зон N^m доступа в пространстве доступа,

– требуется реализовать алгоритмы:

– формирования мультимедийного потока F_3;

– выделения кадров-вставок F_4;

– восстановление видеопотока F_5,

– обеспечивающие автоматизацию контроля и управления доступом при минимальном числе операторов

$$O_{\min} = \sum_{m=1}^{N^m} \sum_{n=1}^{N_n^m} O_{n,m} \Rightarrow \min \tag{5}$$

при ограничениях, отражающих предельно допустимые психофизиологические нагрузки $\eta_{\text{Î ïðåä}}$ операторов

$$\eta_{\text{Î ôàêò}} \le \eta_{\text{Î ïðåä}} \tag{6}$$

По результатам анализа современного состояния и перспектив развития автоматизированных систем управления и систем контроля и управления доступом силовых структур России получены следующие результаты.

Выявлено, что поскольку объем передаваемой видеоинформации, необходимой для видеонаблюдения в режиме реального времени, весьма велик и по известным причинам постоянно возрастает, то сегодня возникает проблема повышения эффективности функционирования СКУД

при минимизации числа операторов с учетом потенциальных психофизиологических их особенностей.

Сделан вывод о том, что одним из путей повышения эффективности функционирования СКУД является разработка и внедрение в автоматизированные СКУД эксклюзивных методов формирования мультимедийного потока, содержащего как видеокадры, так и кадры-вставки на передачи, и цифровых методов обработки видеоизображений (выделение кадров-вставок, фильтрацию и восстановление потока видеоданных) на приеме.

Повышение роли СКУД, усложнение архитектуры ее объектов, рост числа и диапазонов параметров, измеряемых электронных и механических устройств, ужесточение требований к точности измерений и их быстродействию приводят к необходимости автоматизации измерений в рамках автоматизированных систем контроля технического состояния.

Произведена постановка задачи повышения эффективности контроля и управления доступом персонала в силовых структурах России.

---

1. Орешин Н. А., Смирных В. А., Орешин А. Н., Лазарев С. Н. Автоматизация процесса организации контроля технического состояния объектов системы контроля и управления доступом на основе технологии виртуальных приборов [Электронный ресурс] // Научно-технический сборник АО «Концерн "Системпром"» / Под ред. канд. техн. наук А. П. Мурзина. М.: Издательство АО «Концерн "Системпром"», 2017. № 1. Инв. № Д-2030. С. 361–367.

2. Орешин Н. А., Смирных В. А., Лазарев С. Н., Черепков С. А. Анализ современного состояния и перспективы развития автоматизированных систем управления предприятий оборонно-промышленного комплекса России // Материалы XXV военно-научн. конф., 25–26 мая 2017 г. В 2 ч. Смоленск: Изд-во Военной академии войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А. М. Василевского, 2017. Ч. 2. С. 210–216.

3. ГОСТ Р. 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. М.: Изд-во стандартов, 1998. 24 с.

МАТЕМАТИЧЕСКИЕ АСПЕКТЫ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ПЕРЕДАЧИ И ОБРАБОТКИ ВИДЕОИЗОБРАЖЕНИЙ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Лазарев С. Н.,
доцент,
Орешин Н. А.,
канд. тех. наук, профессор,
Матвеев А. М.,
Закиров И. И.
(Академия ФСО России)

Для решения научной задачи, направленной на повышение качества контроля и управления доступом, предложена математическая модель, отражающие процессы формирования потока фотографических кадров, мультимедийного потока, идентификации кадров-вставок в потоке видеоданных и восстановления потока. Данная модель базируется на обобщенной модели территориально-распределенной автоматизированной системы контроля и управления доступом (АСКУД), показанной на рисунке 1.На данной модели применяются следующие обозначения:

– $ÒÄ_1^1$, $ÒÄ_n^1$, $ÒÄ_{N^1}^1$, $ÒÄ_1^m$, $ÒÄ_n^m$, $ÒÄ_{N^m}^m$, $ÒÄ_1^M$, $ÒÄ_n^M$, $ÒÄ_{N^M}^M$ – соответственно первая, текущая *n*-ая и последняя N^m-ая точки доступа первой $ÇÄ_1$, текущей *m*-ой $ÇÄ_m$ и последней *M*-ой $ÇÄ_M$ зон доступа;

– $K_{ÂÏ\,1\,1}$, $K_{ÂÏ\,1\,n}$, $K_{ÂÏ\,1\,N^1}$, $K_{ÂÏ\,m\,1}$, $K_{ÂÏ\,m\,n}$, $K_{ÂÏ\,m\,N^m}$, $K_{ÂÏ\,M\,1}$, $K_{ÂÏ\,M\,n}$, $K_{ÂÏ\,M\,N^M}$ – видеопотоки, поступающие от камер видеонаблюдения соответственно первой, текущей *n*-ой и последней N^m-ой точки доступа первой, текущей *m*-ой и последней *M*-ой зоны доступа, и поступающие на вход сети передачи данных;

– $K_{ÂÏ\,1}$, $K_{ÂÏ\,m}$, $K_{ÂÏ\,M}$ – видеопотоки, поступающие от камер видеонаблюдения соответственно первой, текущей *m*-ой и последней *M*-ой зоны доступа, и поступающие на вход сети передачи данных;

– $\widehat{K}_{ÂÏ\,1\,1}$, $\widehat{K}_{ÂÏ\,1\,n}$, $\widehat{K}_{ÂÏ\,1\,N^1}$, $\widehat{K}_{ÂÏ\,m\,1}$, $\widehat{K}_{ÂÏ\,m\,n}$, $\widehat{K}_{ÂÏ\,m\,N^m}$, $\widehat{K}_{ÂÏ\,M\,1}$, $\widehat{K}_{ÂÏ\,M\,n}$, $\widehat{K}_{ÂÏ\,M\,N^m}$, $\widehat{K}_{ÂÏ\,m}$, $\widehat{K}_{ÂÏ\,m}$, $\widehat{K}_{ÂÏ\,M}$ – видеопотоки, поступающие из сети передачи данных и соответствующие потокам $K_{ÂÏ\,1\,1}$, $K_{ÂÏ\,1\,n}$, $K_{ÂÏ\,1\,N^1}$, $K_{ÂÏ\,m\,1}$, $K_{ÂÏ\,m\,n}$, $K_{ÂÏ\,m\,N^m}$, $K_{ÂÏ\,M\,1}$, $K_{ÂÏ\,M\,n}$, $K_{ÂÏ\,M\,N^M}$, $K_{ÂÏ\,1}$, $K_{ÂÏ\,m}$, $K_{ÂÏ\,M}$;

– $K_{\text{ÏÏ}\,{}^{1}_{1}}$, $K_{\text{ÏÏ}\,{}^{1}_{n}}$, $K_{\text{ÏÏ}\,{}^{1}_{N^1}}$, $K_{\text{ÏÏ}\,{}^{m}_{1}}$, $K_{\text{ÏÏ}\,{}^{m}_{n}}$, $K_{\text{ÏÏ}\,{}^{m}_{N^m}}$, $K_{\text{ÏÏ}\,{}^{M}_{1}}$, $K_{\text{ÏÏ}\,{}^{M}_{n}}$, $K_{\text{ÏÏ}\,{}^{M}_{N^M}}$ – мультимедийные потоки, поступающие от устройств видеонаблюдения соответственно первой, текущей *n*-ой и последней *N*-ой точки доступа первой, текущей *m*-ой и последней *M*-ой зоны доступа, и поступающие на вход сети передачи данных;

– $K_{\text{ÏÏ}\,1}$, $K_{\text{ÏÏ}\,m}$, $K_{\text{ÏÏ}\,M}$ – мультимедийные потоки, поступающие от устройств видеонаблюдения соответственно первой, текущей *m*-ой и последней *M*-ой зоны доступа, и поступающие на вход сети передачи данных.

– $\widehat{K}_{\text{ÏÏ}\,{}^{1}_{1}}$, $\widehat{K}_{\text{ÏÏ}\,{}^{1}_{n}}$, $\widehat{K}_{\text{ÏÏ}\,{}^{1}_{N^1}}$, $\widehat{K}_{\text{ÏÏ}\,{}^{m}_{1}}$, $\widehat{K}_{\text{ÏÏ}\,{}^{m}_{n}}$, $\widehat{K}_{\text{ÏÏ}\,{}^{m}_{N^m}}$, $\widehat{K}_{\text{ÏÏ}\,{}^{M}_{1}}$, $\widehat{K}_{\text{ÏÏ}\,{}^{M}_{n}}$, $\widehat{K}_{\text{ÏÏ}\,{}^{M}_{N^M}}$, $\widehat{K}_{\text{ÏÏ}\,1}$, $\widehat{K}_{\text{ÏÏ}\,m}$, $\widehat{K}_{\text{ÏÏ}\,M}$ – мультимедийные потоки, поступающие из сети передачи данных и соответствующие потокам $K_{\text{ÏÏ}\,{}^{1}_{1}}$, $K_{\text{ÏÏ}\,{}^{1}_{n}}$, $K_{\text{ÏÏ}\,{}^{1}_{N^1}}$, $K_{\text{ÏÏ}\,{}^{m}_{1}}$, $K_{\text{ÏÏ}\,{}^{m}_{n}}$, $K_{\text{ÏÏ}\,{}^{m}_{N^m}}$, $K_{\text{ÏÏ}\,{}^{M}_{1}}$, $K_{\text{ÏÏ}\,{}^{M}_{n}}$, $K_{\text{ÏÏ}\,{}^{M}_{N^M}}$, $K_{\text{ÏÏ}\,1}$, $K_{\text{ÏÏ}\,m}$, $K_{\text{ÏÏ}\,M}$.

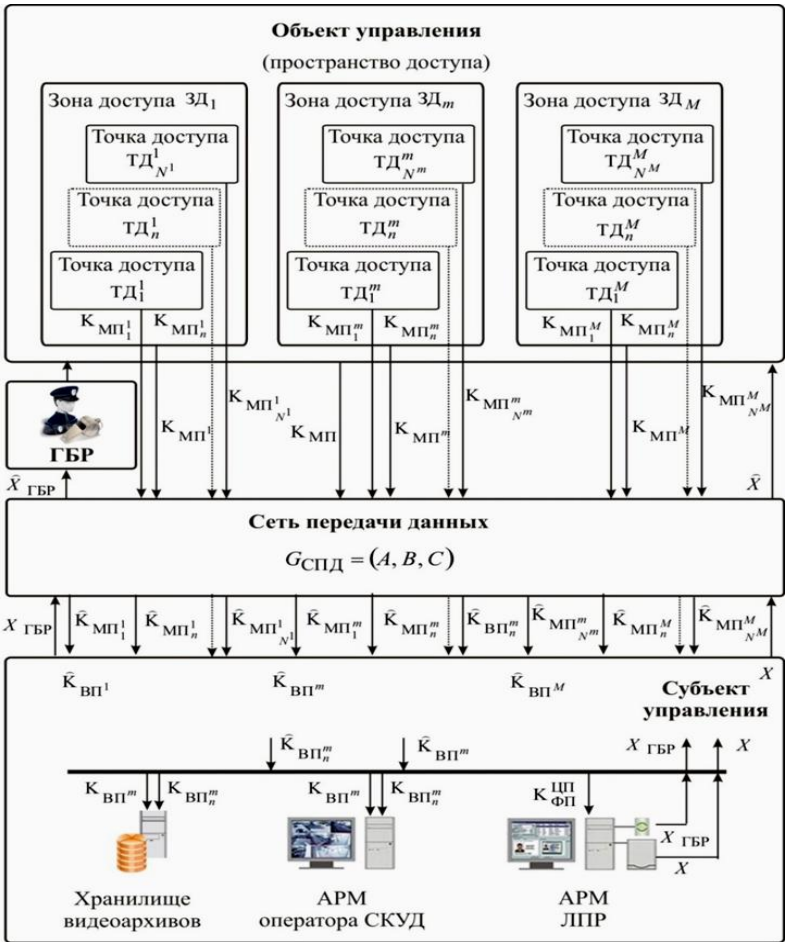

Рисунок 1. Модель территориально-распределенной АСКУД.

В отличие от известных моделей она отражает направленные на рациональную (оптимальную) организацию санкционированного доступа следующие процессы [1]:

− ввода идентификационных признаков;

− идентификации субъектов и объектов доступа по идентификационным признакам;

− аутентификации субъекта доступа;

− отображения фотографических данных субъекта доступа оператору;

− визуальной идентификации субъекта доступа;

− передачи, сбора, хранения и обработки информации о состояниях точек, зон и пространства доступа;

− формирования и обработки мультимедийного потока видеоданных;

− изменения состояний точек доступа по входным воздействиям;

− формирования видеопотока, потока фотографических кадров, потока кадров-вставок и мультимедийного потока;

− выделения кадров-вставок;

− восстановление видеопотока,

а также следующие свойства:

− состояния точек, зон и пространства доступа;

− входные воздействия на точку, зону и пространство доступа;

− реакции точек, зон и пространства доступа на входные воздействия;

− территориально-распределенную структуру пространства доступа;

− цветовое пространство пикселя.

В работе эта математическая модель в формализованном виде представлена множеством

$$Q_{\text{ÀÑÊÓÄ}} = \left\{ T, S_{\text{ÏÄ}}(t), X_{\text{ÏÄ}}(t), Y_{\text{ÏÄ}}(t), Q_{\text{ÏÄ}}, Q_{\text{ÖÏÏ}} , \right.$$

$$\left. F_1 , F_2 , F_3 , F_4 , F_5 , F_6 , F_7 , F_8 , F_9 , F_{10}, F_{11} \right\}, \tag{1}$$

где T – подмножество моментов времени $t \in T$, в которые наблюдается точка доступа;

$S_{\text{ÏÄ}}(t)$ − подмножество состояний пространства доступа в момент времени $t \in T$;

$X(t)$ − подмножество входных воздействий $x(t) \in X(t)$ на пространство доступа;

$Y(t)$ − подмножество реакции $y(t) \in Y(t)$ пространства доступа на входные воздействия $X(t)$;

$Q_{\text{ПД}}$ − подмножество, отражающее структуру пространства доступа;

$Q_{\text{ЦП}}$ − подмножество, характеризующее цветовое пространство пикселя видеоизображения;

$F_1 : \text{К}_{\text{ФП}}(t) \to \text{К}^{\text{Д}}_{\text{ФП}}(t)$ − оператор, описывающий механизм включения в поток фотографических кадров $\text{К}_{\text{ФП}}(t)$ дату появления события, требуемого для анализа и принятия решения о допуске субъектов к точке доступа;

$F_2 : \text{К}_{\text{ФП}}(t) \to \text{К}^{\text{ЦП}}_{\text{ФП}}(t)$ − оператор, описывающий механизм включения в поток фотографических кадров $\text{К}_{\text{ФП}}(t)$ цифровой подписи, для определения точки доступа в которой появилось событие, требуемое для анализа и принятия решения о допуске субъектов;

$F_3 : \text{К}^{\text{Д}}_{\text{ФП}}(t),\ \text{К}^{\text{ЦП}}_{\text{ФП}}(t) \to \text{К}_{\text{ПКВ}}(t)$ − оператор, описывающий механизм формирования потока кадров-вставок $\text{К}_{\text{ПКВ}}(t)$ из потоков фотографических кадров $\text{К}^{\text{Д}}_{\text{ФП}}(t)$ и $\text{К}^{\text{ЦП}}_{\text{ФП}}(t)$;

$F_4 : \text{К}_{\text{ВП}}(t), \text{К}_{\text{ПКВ}}(t) \to \text{К}_{\text{МП}}(t)$ − оператор, описывающий механизм формирования мультимедийного потока $\text{К}_{\text{МП}}(t)$ из видеопотока $\text{К}_{\text{ВП}}(t)$ и потока кадров-вставок $\text{К}_{\text{ПКВ}}(t)$;

$F_5 : \text{К}_{\text{МП}}(t) \to \text{К}^{\text{З}}_{\text{МП}}(t)$ − оператор, описывающий механизм формирования защищенного мультимедийного потока $\text{К}^{\text{З}}_{\text{МП}}(t)$;

$F_6 : \text{К}^{\text{З}}_{\text{МП}}(t) \to \text{К}_{\text{МП}}(t)$ − оператор, описывающий механизм восстановления на приеме мультимедийного потока $\text{К}_{\text{МП}}(t)$;

$F_7 : \text{К}_{\text{МП}}(t) \to \text{К}_{\text{ВП}}(t)$ − оператор, описывающий механизм выделения и восстановления видеопотока $\text{К}_{\text{ВП}}(t)$;

$F_8 : \text{К}_{\text{МП}}(t) \to \text{К}_{\text{ПКВ}}(t)$ − оператор, описывающий механизм выделения потока кадров-вставок $\text{К}_{\text{ПКВ}}(t)$ из мультимедийного потока $\text{К}_{\text{МП}}(t)$;

$F_9 : \text{К}_{\text{ПКВ}}(t) \to X_{\text{ПД}}(t)$ − оператор, описывающий механизм формирования входных воздействий $x(t) \in X(t)$ на точки и зону доступа;

$F_{10} : T \times X_{\text{ПД}}(t) \times S_{\text{ПД}}(t) \to S_{\text{ПД}}(t)$ − оператор, описывающий механизм изменения состояния пространства доступа $S_{\text{ПД}}(t)$ в момент времени $t \in T$ при поступлении входного воздействия $x(t) \in X(t)$;

$F_{11}: T \times X_{\text{ПД}}(t) \times S_{\text{ПД}}(t) \to Y_{\text{ПД}}(t)$ – оператор, описывающий механизм реакции пространства доступа $Y_{\text{ПД}}(t)$ в момент времени $t \in T$ при поступлении входного воздействия $x(t) \in X(t)$.

Поскольку основой построения и развития автоматизированной СКУД является ее территориально-распределенная архитектура, позволяющая отразить взаимодействие открытых систем на трех уровнях[2]:

– точки доступа;

– зоны доступа;

– пространства доступа,

то состояния пространства доступа будем выражать множеством $S_{\text{ПД}}(t) = \left\{ S_{\text{ЗД}_m}(t), m = \overline{1, M} \right\}$, элементами которого являются M множеств состояний в момент времени t зон доступа $S_{\text{ЗД}_m}(t)$, образующих пространство доступа.

По аналогии с вышеизложенным, состояние m-ой зоны доступа в момент времени t будем характеризовать множеством $S_{\text{ЗД}_m}(t) = \left\{ S_{\text{ТД}_n^m}(t), n = \overline{1, N^m} \right\}$, элементами которого являются N^m состояний точек доступа $S_{\text{ТД}_n^m}(t)$ в m-ой зоне доступа в момент времени t;

Состояние $S_{\text{ТД}_n^m}(t)$ n-ой точки доступа m-ой зоны доступа определяется санкционированным или несанкционированным доступом субъектов $s_{\text{СД}_n^m}$ и объектов доступа $s_{\text{ОД}_n^m}$, наличием (или отсутствием) группы быстрого реагирования $s_{\text{ГБР}_n^m}$, состояниями управляемых преграждающих устройств $s_{\text{УПУ}_n^m}$ и системы сигнализации $s_{\text{СС}_n^m}$.

С учетом сказанного состояние $S_{\text{ТД}_n^m}(t)$ отобразим множеством $S_{\text{ТД}_n^m}(t) = \left\{ s_{\text{СД}_n^m}, s_{\text{ОД}_n^m}, s_{\text{ГБР}_n^m}, s_{\text{УПУ}_n^m} \right\}$.

Состояние точки доступа $S_{\text{ТД}_n^m}(t)$ по элементам $s_{\text{СД}_n^m}$ и $s_{\text{ОД}_n^m}$ определяется исходя из следующих факторов:

– по наличию или отсутствию в наблюдаемой точке субъекта или объекта доступа в момент времени t;

– по наличию или отсутствию у субъекта и объекта доступа, находящегося в наблюдаемой точке в момент времени t, кодового признака (КП), используемого для их идентификации;

– по наличию или отсутствию у субъекта доступа, находящегося в наблюдаемой точке в момент времени t, биометрического признака (БП), используемого для его идентификации.

В рамках проведенного исследования авторы работы рассматривают четыре состояния $s_{\text{ÓÏÓ}\ n}^{m}$ управляемых преграждающих устройств, расположенных в n-ой точки доступа m-ой зоны доступа:

− работоспособное открытое состояние, при котором обеспечивается допуск субъекта и (или) объекта доступа через УПУ;

− неработоспособное открытое состояние, при котором обеспечивается допуск субъекта и (или) объекта доступа через управляемые преграждающие устройства;

− работоспособное закрытое состояние, при котором запрещается допуск субъекта и (или) объекта доступа через УПУ.

− неработоспособное закрытое состояние, при котором запрещается допуск субъекта и (или) объекта доступа через УПУ.

Состояние точки доступа $S_{\text{ÒÄ}_n^m}(t)$ по элементу $s_{\text{ÃÁÐ}_n^m}(t)$ будем характеризовать по наличию или отсутствию в n-ой точки доступа m-ой зоны доступа группы быстрого реагирования в момент времени t;

Состояние точки доступа $S_{\text{ÒÄ}_n^m}(t)$ по элементу $s_{\text{ÑÑ}_n^m}(t)$ будем описывать состояниями датчиков системы сигнализации в момент времени t.

Заметим, что из-за несовершенства современных алгоритмов обработки идентификационных признаков даже при работоспособном открытом или закрытом состоянии УПУ возможны ошибки 1-го рода (вероятность ошибочного отклонения законного пользователя) и ошибки 2-го рода (вероятность ошибочного предоставления доступа незаконному пользователю).

Для принятия решения субъектом управления о выработки необходимого воздействия на объект управления (точку доступа) предлагается в модели автоматизированной территориально-распределенной системы контроля и управления доступом использовать следующие технологии:

− формирования потока видеопотока $\text{K}_{\text{ÂÏ}}(t)$, фотографических кадров $\text{K}_{\text{ÔÏ}}(t)$, потока кадров-вставок $\text{K}_{\text{ÏÊÂ}}(t)$, мультимедийного потока $\text{K}_{\text{ÌÏ}}(t)$;

− выделения из мультимедийного потока кадров-вставок;

− восстановления видеопотока.

Видеопоток $\text{K}_{\text{ÂÏ}}(t) = \left(\kappa_{\text{âèä}\ 1}, \kappa_{\text{âèä}\ 2}, \cdots, \kappa_{\text{âèä}\ k}, \cdots\right)$ формируется в каждой точки, зоны и в пространстве доступа камерами видеонаблюдения. Основное предназначение видеопотока – нести информацию о текущих состояниях наблюдаемых объектов. В данном потоке число кадров в секунду определяется техническими особенностями используемых видеокамер. В зависимости от принятых организационно-технических мер

данный поток может быть записан в базу данных объектов (точки, зоны и пространства доступа), где расположены камеры видеонаблюдения. При необходимости (при анализе состояний наблюдаемых объектов и принятии решения) данный поток передается в субъект управления по каналам сети передачи данных.

Заметим, что поскольку видеопоток $K_{ВП}(t)$ передается в субъект управления только при необходимости (например, при мониторинге нарушения санкционированного доступа), то требования к пропускной способности сети передачи данных, к количеству видеомониторов и к операторам, обслуживающих их, резко уменьшаются. Вполне очевидно, что при этом существенно повышается качество контроля и управления доступом при минимальном числе обслуживающих операторов с учетом ограничений на их психофизиологические потенциальные возможности.

Поток $K_{ФП}(t) = \left(\kappa_{фото\,1}, \kappa_{фото\,2}, \cdots, \kappa_{фото\,k}, \cdots\right)$ фотографических кадров формируется электронными фотоаппаратами. Основное предназначение потока фотографических кадров – обеспечить при вводе идентификационных признаков в УПУ графической информацией устройство управления для установления заданного режима доступа, а также для отображения и регистрации информации. В автоматизированных территориально-распределенных системах информация потока фотографических кадров является необходимой не только для устройств управления точек, зон и пространства доступа, но и субъекта управления. Поэтому она передается по сети передачи данных.

---

1. Орешин Н. А., Смирных В. А., Орешин А. Н., Демин А. Ю. Модель автоматизированной системы контроля технического состояния объектов доступа, как системы массового обслуживания доступом // Информационные системы и технологии. 2017. № 6. С. 103–112.

2. Орешин Н. А., Смирных В. А., Орешин А. Н., Лазарев С. Н. Автоматизация процесса организации контроля технического состояния объектов системы контроля и управления доступом на основе технологии виртуальных приборов [Электронный ресурс] // Научно-технический сборник АО «Концерн "Системпром"» / Под ред. канд. техн. наук А. П. Мурзина. М.: Издательство АО «Концерн "Системпром"», 2017. № 1. Инв. № Д-2030. С. 361–367.

ПРЕДЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ НАДЕЖНОСТИ ЭЛЕКТРОСНАБЖЕНИЯ МАЛОГАБАРИТНЫХ ИНДИВИДУАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ МОБИЛЬНЫХ ОБЪЕКТОВ ТЕЛЕКОММУНИКАЦИЙ СИЛОВЫХ ВЕДОМСТВ

Костин С. В.,
канд. тех. наук,
Ванюков Р. Ю.
(Академия ФСО России)

В настоящее время существует множество объектов телекоммуникаций (ОТ) различного назначения. Среди них различают стационарные и подвижные ОТ. В состав любого ОТ входит система электроснабжения, представляющая собой совокупность установок, обеспечивающих потребителей ОТ электроэнергией [1; 2]. Одним из важных вопросов функционирования системы электроснабжения является обеспечение качества электропитания потребителей, характеризующееся следующими показателями качества энергии (ПКЭ): качеством электроэнергии (качеством напряжения), снабжаемой системой электроснабжения, и надежностью электроснабжения (надежностью работы системы электроснабжения). Качество электроэнергии определяется воздействием электроэнергии на электрооборудование ОТ, подключенное к электрической сети, оцениваемое по соответствию, например, качества напряжения установленным требованиям. Надежность же электроснабжения характеризуется надежностью функционирования системы электроснабжения, т. е. способностью системы электроснабжения обеспечивать электропотребителей на ОТ электрической энергией, сохраняя во времени значения показателей качества электрической энергии (при определенных условиях эксплуатации) в установленных пределах. Первый показатель качества энергии определен выбором как энергосбытовой компании, так и оборудованием на ОТ, которое располагается на электрических вводах [3]. Во втором случае уместно вести разговор о категорировании ОТ в целях обеспечения надежности его электроснабжения. Практически все ОТ силовых ведомств относятся к особой группе первой категории электроприемников по надежности электроснабжения. Это значит необходимо обеспечить наличие не только двух независимых источников электрической энергии, а также третьего источника электроэнергии в виде агрегата бесперебойного питания, аккумуляторные батареи и т. п.

При строительстве и эксплуатации стационарных ОТ силовых ведомств данные требования учитываются и выполняются. На подвижных ОТ (ПОТ) силовых ведомств также при их разработке и вводе в эксплуатацию предусмотрены два источника электрической энергии в виде ос-

новного (промышленная сеть) и резервного (электроагрегат). Кроме того, в состав системы электроснабжения (СЭС) ПОТ вводятся: второй электроагрегат, АКБ, ИБП и т. д. Какой тип устройства включается в СЭС ПОТ определяет заказчик, исходя из предназначения конкретного ОТ, однако включение каждого нового элемента СЭС приводит к увеличению количества средств доставки.

Следует отметить, что для некоторых задач необходимы малые ПОТ – мобильные ОТ, состоящие из одной единицы транспортного средства. Выполнение своих задач этими мобильными ОТ (МОТ) не требует больших энергозатрат, однако эти ОТ также относятся к особой группе первой категории электроприемников по надежности электроснабжения. Таким образом, необходимо ввести в СЭС устройства, которые могут быть применены для резервирования электропитания МОТ с малогабаритными индивидуальными телекоммуникационными системами. В силу выполнения специфических задач данной категорией МОТ не могут быть использованы следующие источники электропитания:

1. Стационарная сеть, так как МОТ может быть развернут и свернут скрытно, а также количество мест развертывания не ограничено.

2. Электроагрегаты – производят шум, снижают скрытность, кроме того, требуется время на их развертывание и свертывание.

3. Мощные АКБ – требуют достаточно места в транспортном средстве.

В данных условиях представляется целесообразным использование источников электропитания для малогабаритных индивидуальных телекоммуникационных систем, состоящих из химических источников тока, источников тока на основе возобновляемых источников энергии и источников отбора мощности от двигателя транспортного средства.

В качестве основного источника электроэнергии предлагается использовать источник отбора мощности от двигателя транспортного средства в виде автомобильного преобразователя (инвертора) или химический источник тока в виде АКБ на основе gel-технологий при скрытном расположении МОТ. АКБ банной технологии имеют следующие преимущества:

1. Значительный срок эксплуатации (около 10 лет).
2. Большое количество циклов зарядов-разрядов.
3. При глубоком разряде не требуется срочный заряд.
4. Потери ёмкости в случае простоя АКБ небольшие (около 20 %).
5. Обладает высокой эффективностью, т.к. имеет малое внутреннее сопротивление.
6. Не требуют обслуживания и отличаются безопасностью эксплуатации за счёт непроницаемости корпуса.

В качестве резервного источника электроэнергии предлагается использовать АКБ или источников тока на основе возобновляемых ис-

точников энергии в виде комплектов на основе ветрогенераторов или солнечных батарей [4].

Кроме этого в составе большинства малогабаритных индивидуальных телекоммуникационных систем МОТ имеются средства ЭВМ, которые снабжены собственными источниками электропитания (внутренними АКБ) и дополнительными накопителями – химическими источниками тока. В качестве последних могут быть использованы малогабаритные зарядные устройства на солнечных батареях, но они имеют существенный недостаток – в ненастную погоду или при отсутствии солнца они применимы. В последнее время появились новые источники тока, так же использующие электро-химические процессы. Такими источниками являются топливные элементы, использующее богатое водородом топливо [4–6].

В заключении хотелось бы сделать вывод, что современные технологии уже разработать и внедрить СЭС на МОТ силовых ведомств с высокими требованиями по надежности электроснабжения с учетом специфики выполняемых задач. В настоящее время в России имеются разработки в области электроэнергетики на основе возобновляемых источников энергии, которые уже внедряются.

---

1. Правила электроустановок: Приказ Минэнерго России от 8 июля 2002 г. № 204.

2. Иванов В. Н.; Орешин Н. А.; Орешин А. Н. и др. Электропитание устройств и систем телекоммуникаций: учебное пособие / под общ. ред. Н. А. Орешина. Орёл: Академия ФСО России, 2015. 535 с.: ил.

3. О функционировании розничных рынков электрической энергии, полном и (или) частичном ограничении режима потребления электрической энергии: Постановление Правительства Рос. Федерации от 4 мая 2012 г. № 442: с изменениями и дополнениями.

4. Удалов С. Возобновляемая энергетика: учебное пособие. Новосибирск: Изд-во НГТУ, 2016.

5. Проблемы и перспективы использования возобновляемых источников энергии / В. К. Федоров, А. С. Татевосян, М. М. Сангов, Р. Т. Тажиев. Омский ГТУ.

6. Ермоленко Г. В., Фетисова Ю. А. Карта отрасли ВИЭ в России. Оптовый рынок электроэнергии (мощности) // Возобновляемая энергетика XXI век: энергетическая и экономическая эффективность: Международный конгресс, 13–14 октября 2017 г. Москва. Сколково.

АЛГОРИТМИЧЕСКИЕ АСПЕКТЫ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ПЕРЕДАЧИ И ОБРАБОТКИ ВИДЕОИЗОБРАЖЕНИЙ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Черепков С. А.,
канд. тех. наук,
Орешин Н. А.,
канд. тех. наук, профессор,
Шеховский Д. А.,
Викторов М. А.
(Академия ФСО России)

Для решения научной задачи, направленной на повышение эффективности функционирования территориально-распределенной автоматизированной системы контроля и управления доступом (АСКУД) предложена методика формирования потока фотографических кадров, мультимедийного потока, идентификации кадров-вставок в потоке видеоданных и восстановления потока. Данная методика основана на процессах, обеспечивающих минимизацию числа операторов, необходимых для выполнения задач контроля и управления доступом при ограничениях на психофизиологические возможности человека.

Суть методики заключается в последовательном выполнении шагов, представленных алгоритмом, показанном рисунке 1.

Поскольку при мониторинге состояния точки, зоны и пространства доступа оператору субъекта управления необходимо знать дату появления события и идентификационный признак наблюдаемого объекта, поэтому в методике используются три оператора:

$F_1 : \mathrm{K}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t) \to \mathrm{K}^{\ddot{\mathrm{A}}}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t)$ – описывающий механизм включения в поток фотографических кадров $\mathrm{K}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t)$ дату появления события;

$F_2 : \mathrm{K}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t) \to \mathrm{K}^{\ddot{\mathrm{O}}\ddot{\mathrm{I}}}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t)$ – описывающий механизм включения в поток фотографических кадров $\mathrm{K}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t)$ цифровой подписи;

$F_3 : \mathrm{K}^{\ddot{\mathrm{A}}}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t),\ \mathrm{K}^{\ddot{\mathrm{O}}\ddot{\mathrm{I}}}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t) \to \mathrm{K}_{\ddot{\mathrm{I}}\hat{\mathrm{E}}\hat{\mathrm{A}}}(t)$ описывающий механизм формирования потока кадров-вставок $\mathrm{K}_{\ddot{\mathrm{I}}\hat{\mathrm{E}}\hat{\mathrm{A}}}(t)$ из потоков фотографических кадров $\mathrm{K}^{\ddot{\mathrm{A}}}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t)$ и $\mathrm{K}^{\ddot{\mathrm{O}}\ddot{\mathrm{I}}}_{\hat{\mathrm{O}}\ddot{\mathrm{I}}}(t)$.

Заметим, что объем цифровой графической информации кадров-вставок $\kappa_{\hat{\mathrm{E}}\hat{\mathrm{A}}_k} \in \mathrm{K}_{\ddot{\mathrm{I}}\hat{\mathrm{E}}\hat{\mathrm{A}}}(t)$ не велик по сравнению с видеопотоком $\mathrm{K}_{\hat{\mathrm{A}}\ddot{\mathrm{I}}}(t)$. Поэтому требования к числу операторов, к пропускной способности сети передачи данных, а также к быстродействию используемых ЭВМ в субъекте управления не значительны. В зависимости от принятой орга-

низации обслуживания электронный фотоаппарат фиксирует не только ввод идентификационных признаков субъектом доступа, но и проход его через УПУ. Благодаря такому использованию электронного фотоаппарата исключается возможность проникновения в точки, зоны и пространство доступа лиц, использующих чужие идентификационные признаки. Несомненно, это значительно повышает качество доступа в автоматизированных системах без использования операторов.

Кадры-вставки $\kappa_{\hat{E}\hat{A}_k}$ со служебной информацией могут передаваться по сети передачи данных в едином потоке $K_{\ddot{I}\hat{E}\hat{A}}(t)$, либо в мультимедийном потоке $K_{\grave{I}\ddot{I}}(t)$, образованным объединением видеопотока $K_{\hat{A}\ddot{I}}(t)$ и потока кадров-вставок $K_{\ddot{I}\hat{E}\hat{A}}(t)$, то есть $K_{\grave{I}\ddot{I}}(t) = K_{\hat{A}\ddot{I}}(t) \cup K_{\ddot{I}\hat{E}\hat{A}}(t)$.

В связи с этим в мультимедийном потоке будем различать два класса кадров $\Psi_1, \Psi_2 \in \Psi$.

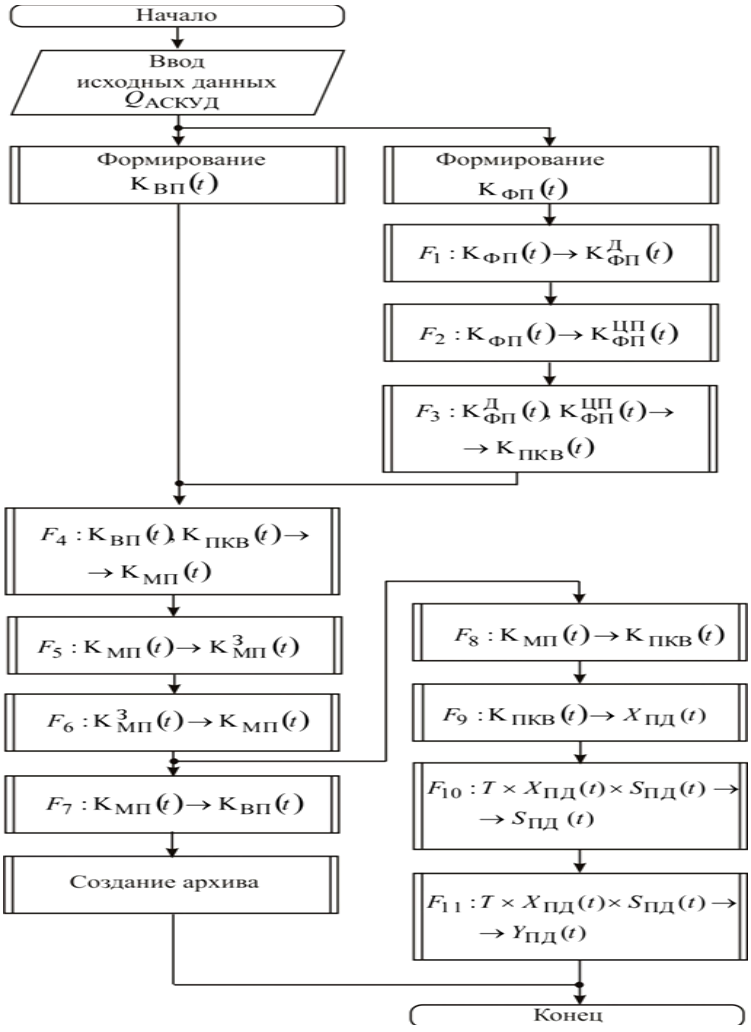

Рисунок 1. Алгоритм формирования потока фотографических кадров, мультимедийного потока, идентификации кадров-вставок в потоке видеоданных и восстановления потока в АСКУД.

Класс Ψ_1 объединяет видеокадры (кадры видеосюжета) $\kappa_{âèä_k} \in K_{ÂÏ}(t)$, которые несут сведения о наблюдаемом объекте в период его обычного функционирования (когда вопрос о допуске персонала к объекту не рассматривается). Класс Ψ_2 объединяет кадры-вставки $\kappa_{ÊÂ_k} \in K_{ÏÊÂ}(t)$, которые несут сведения о наблюдаемом объекте в период его активного функционирования (когда решается вопрос о допуске персонала к наблюдаемому объекту).

Алгоритм формирования мультимедийного потока представлен в виде отображения $F_4 : K_{ÂÏ}(t), K_{ÏÊÂ}(t) \to K_{ÏÏ}(t)$.

Защита информации при передаче мультимедийного потока $K_{ÏÏ}(t)$ по каналам сети передачи обеспечивается применением двух операторов:

$F_5 : K_{ÏÏ}(t) \to K_{ÏÏ}^{C}(t)$ − описывающий механизм формирования защищенного мультимедийного потока $K_{ÏÏ}^{C}(t)$;

$F_6 : K_{ÏÏ}^{C}(t) \to K_{ÏÏ}(t)$ − описывающий механизм восстановления на приеме мультимедийного потока $K_{ÏÏ}(t)$.

Алгоритм выделения из мультимедийного потока $K_{ÏÏ}(t)$ и восстановления видеопотока $K_{ÂÏ}(t)$ в методике отражен оператором $F_7 : K_{ÏÏ}(t) \to K_{ÂÏ}(t)$. Для возможного дальнейшего использования (например, при проведении расследования) восстановленный видеопоток архивируется в субъекте доступа.

Алгоритм, отражающий механизм выделения потока кадров-вставок $K_{ÏÊÂ}(t)$ из мультимедийного потока $K_{ÏÏ}(t)$ в методике представлен оператором $F_8 : K_{ÏÏ}(t) \to K_{ÏÊÂ}(t)$.

Идентификация кадров-вставок мультимедийного потока $K_{ÏÏ}(t)$ осуществляется при предположении, что изображения видеокадров $\kappa_{âèä_k} \in K_{ÂÏ}(t)$ и кадров-вставок $\kappa_{ÊÂ_k} \in K_{ÏÊÂ}(t)$ являются растровыми, то есть представляющими собой сетку пикселей − цветных точек на носителе цифрового изображения [0].

Выбор растрового изображения обосновывается следующими важными характеристиками [1]:

− ограниченное количество пикселей, которое может указываться отдельно как по ширине и высоте (например, 1024×768, 640×480), так и в целом на изображение;

− достаточное для практики количество используемых цветов, то есть глубина цвета;

− возможность использования различных цветовых моделей (цветовых пространств), в частности *RGB*.

К основным преимуществам растрового изображения по отношению к векторному изображению можно отнести:

− растровую графику редактируют с помощью эффективных растровых графических редакторов;

− растровая графика создается видеокамерами, регистраторами, фотоаппаратами, сканерами непосредственно в растровом редакторе, также путем экспорта из векторного редактора или в виде снимков экрана;

− растровая графика позволяет создать практически любой рисунок, и передать эффект перехода от одного цвета к другому без потерь в размере файла;

− распространённость – растровая графика используется сейчас практически везде: от маленьких значков до плакатов;

− высокая скорость обработки сложных изображений, если не нужно масштабирование;

− растровое представление изображения естественно для большинства устройств ввода-вывода графической информации, таких как мониторы (за исключением векторных устройств вывода), матричные и струйные принтеры, цифровые фотоаппараты, сканеры, а также сотовые телефоны.

При растровом изображении каждый *k*-ый кадр $\kappa_k \in \mathrm{K}_{\text{ÏÏ}}\ (t)$ представляется в виде множества пикселей $\pi_{i,j}^k$ на прямоугольном носителе, которое математически будем описывать двумерной матрицей $\kappa_k = \left\| \pi_{i,j}^k \right\|, i = \overline{1,I},\ j = \overline{1,J}$, где k – номер наблюдаемого кадра (видео $\kappa_{\text{âèä}\ k} \in \mathrm{K}_{\text{ÂÏ}}\ (t)$ или кадра-вставки $\kappa_{\text{ÊÂ}_k} \in \mathrm{K}_{\text{ÏÊÂ}}\ (t)$), i и j – соответственно номера столбца и строки матрицы, на пересечениях которых расположен пиксель.

Поскольку пиксель $\pi_{i,j}^k$ характеризуется определённым цветом $c_{i,j}^k$, то растровым изображением кадра I_k является множество цветных точек на носителе видеоинформации: $\mathrm{I}_k = \left\| c_{i,j}^k \right\|, i = \overline{1,I},\ j = \overline{1,J}$.

При описании цвета пикселя в методик ее использована аддитивная цветовая модель *RGB*, предложенная Максвеллом Д. К. (аббревиатура английских слов *Red*, *Green*, *Blue* – красный, зелёный, синий). Данная модель основана на декартовой системе координат с осями величин r, g и b, значения которых определяют интенсивности соответственно красного, зеленого и синего цветов [0].

Учитывая, что в данной модели цвет $c_{i,j}^{k}$ пикселя *k*-го кадра характеризуется интенсивностями трех цветовых составляющих r_{ij}^{k}, g_{ij}^{k}, b_{ij}^{k}, то величину c_{ij}^{k} в дальнейшем математически будем описывать упорядоченным множеством $c_{ij}^{k} = \left(r_{ij}^{k} \ , g_{ij}^{k}, b_{ij}^{k} \right)$.

Таким образом, в модели *RGB* цветовое пространство $Q_{\text{ÖÏÏ}} = \left(c_{ij} \,/ i = \overline{1, I}; y = \overline{1, Y} \right)$ пикселя (цветовая палитра пикселя) можно представить в виде куба, показанного на рисунке 2.

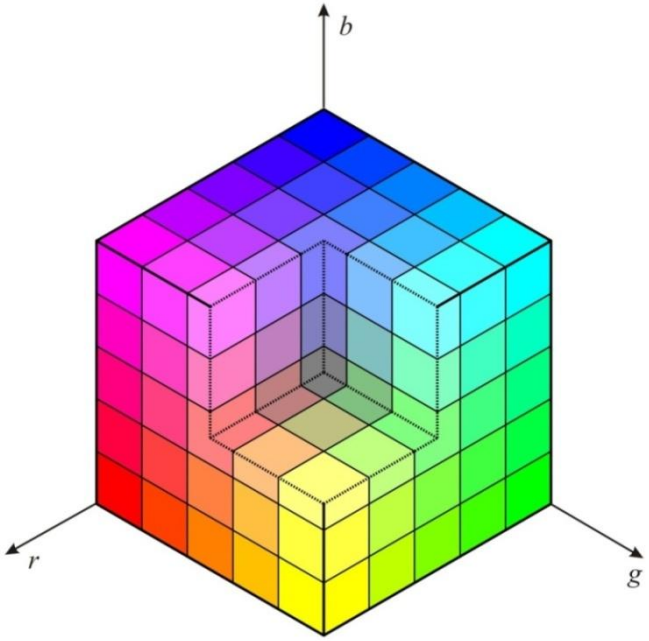

Рисунок 2. Аддитивная *RGB* модель
цветового пространства пикселя.

Точки, соответствующие красному, зеленому и синему цветам расположены в трех вершинах куба, лежащих на координатных осях r, g, b. Голубой (зеленый плюс синий), пурпурный (красный плюс синий) и желтые (красный плюс зеленый) цвета расположены в трех других вершинах этого куба. Черный цвет находится в начале координат, а белый – в наиболее удаленной от начала координат вершине. Оттенки серого цвета (точки с равными значениями величин r, g, b) лежат на диагонали, соединяющей черную и белую вершины [2]. Различные цвета в этой модели представляют собой точки на поверхности или внутри куба и определяются вектором, проведенным в данную точку из начала

координат, или упорядоченным множеством (кортежем) $c_{i,j}^{k} = \left(r_{i,j}^{k}, g_{i,j}^{k}, b_{i,j}^{k} \right)$.

С учетом введенных обозначений цвета пикселя $c_{i,j}^{k}$ и определения кадра изображение I_k k-го кадра представим в форме матрицы размером $I \times J$, где I и J – соответственно число столбцов и строк матрицы:

$$\mathrm{I}_k = \begin{bmatrix} c_{0,0}^{k} & c_{0,1}^{k} & \cdots & c_{0,J-1}^{k} \\ c_{1,0}^{k} & c_{1,1}^{k} & \cdots & c_{1,J-1}^{k} \\ \vdots & \vdots & \vdots & \vdots \\ c_{I-1,0}^{k} & c_{I-1,1}^{k} & \cdots & c_{I-1,J-1}^{k} \end{bmatrix}. \quad (1)$$

Операторы F_9, F_{10} и F_{11}, используемые в методике, описывают следующие механизмы:

$F_9 : \mathrm{K}_{\text{ïêâ}}(t) \to X_{\text{ïä}}(t)$ – оператор, описывающий механизм формирования входных воздействий $x(t) \in X(t)$ на точки и зону доступа;

$F_{10} : T \times X_{\text{ïä}}(t) \times S_{\text{ïä}}(t) \to S_{\text{ïä}}(t)$ – оператор, описывающий механизм изменения состояния пространства доступа $S_{\text{ïä}}(t)$ в момент времени $t \in T$ при поступлении входного воздействия $x(t) \in X(t)$;

$F_{11} : T \times X_{\text{ïä}}(t) \times S_{\text{ïä}}(t) \to Y_{\text{ïä}}(t)$ – оператор, описывающий механизм реакции пространства доступа $Y_{\text{ïä}}(t)$ в момент времени $t \in T$ при поступлении входного воздействия $x(t) \in X(t)$.

На основании вышеизложенного можно сделать следующий вывод.

Поскольку объем передаваемой видеоинформации, необходимой для видеонаблюдения в режиме реального времени, весьма велик и по известным причинам постоянно возрастает, то сегодня возникает проблема повышения эффективности функционирования СКУД при минимизации числа операторов с учетом потенциальных психофизиологических их особенностей.

В работе предложена методика формирования потока фотографических кадров, мультимедийного потока, идентификации кадров-вставок в потоке видеоданных и восстановления потока, которая обеспечивает при минимальном числе операторов и при ограничениях на психофизиологические возможности человека качественное выполнение задач контроля и управления доступом.

1. Орешин Н. А., Смирных В. А., Орешин А. Н., Демин А. Ю. Модель автоматизированной системы контроля технического состояния объектов доступа, как системы массового обслуживания доступом // Информационные системы и технологии. 2017. № 6. С. 103–112.
2. Орешин Н. А., Смирных В. А., Орешин А. Н., Лазарев С. Н. Автоматизация процесса организации контроля технического состояния объектов системы контроля и управления доступом на основе технологии виртуальных приборов [Электронный ресурс] // Научно-технический сборник АО «Концерн "Системпром"» / Под ред. канд. техн. наук А. П. Мурзина. М.: Издательство АО «Концерн "Системпром"», 2017. № 1. Инв. № Д-2030. С. 361–367.

Сборник научных статей

Под редакцией
Л. Д. Матросовой [и др.]

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ: ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ И ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ

Свидетельство о государственной аккредитации
Рег. № 2660 от 02.08.2017 г.
Подписано в печать 13.11.2018 г. Формат 60x90 1/16.
Усл. печ. л. – 4,31. Тираж 24 экз. Заказ № 122.

Орловский юридический институт МВД России имени В. В. Лукьянова.
302027, г. Орел, ул. Игнатова, 2.