
И. А. Иванченко
ПРИКЛАДНАЯ ВИДЕОАНАЛИТИКА
практическое пособие

Игорь Анатольевич Иванченко

Прикладная видеоаналитика. Практическое пособие

http://www.litres.ru/pages/biblio_book/?art=69770638
SelfPub; 2023

Аннотация

Представлена методика оптимизации деятельности специалистов в процессе сбора и анализа видеоданных. На основе накопленного практического опыта в сфере обеспечения безопасности объектов торговой недвижимости, производства и транспортной инфраструктуры рассмотрены методы проведения служебных проверок, вопросы интеграции систем видеонаблюдения с другими компонентами интегрированной системы безопасности, требования к подготовке специалистов.Для специалистов служб безопасности, сотрудников частных охранных организаций, сотрудников подразделений транспортной безопасности, занимающихся вопросами анализа видеоданных. Также пособие будет полезно профильным специалистам при подготовке технического задания на проектирование систем видеонаблюдения и интегрированных систем безопасности.

Содержание

Игорь Иванченко
Прикладная видеоаналитика. Практическое пособие

О тайном догадывайся по явному
Солон

ВВЕДЕНИЕ

Последние годы динамика внедрения систем видеонаблюдения в сфере торговой недвижимости, производства и транспортной инфраструктуры остается положительной. Даже после ухода некоторых производителей систем видеонаблюдения с российского рынка, по оценке специалистов компании ivideon[1], в 2022 г. российский парк видеокамер должен был достигнуть порядка 21 млн шт. Вместе с количеством видеокамер меняется и качество получаемых видеоматериалов – как правило, в современных видеосистемах используется разрешение не менее 2 Мп с частотой кадров не менее 24 к./с.

Более того, для ряда объектов законом установлены обязательные технические требования в т. ч. к системам видеонаблюдения. В частности, в требованиях к функциональным свойствам технических средств обеспечения транспортной безопасности, утвержденных Постановлением Правительства РФ от 26.09.2016 г. № 969, в т. ч. указаны требования к минимальному разрешению видеокамер (1,2 Мп) и частоте кадров не менее 16 к./с.

---

[1] Интернет-ресурс RB.RU (ООО «Русбейс»). Быстро меняющийся ландшафт рынка видеонаблюдения: что нужно знать. Автор: Заур Абуталимов.URL: https://rb.ru/opinion/videosurveillance-market-trends/

Для торговых объектов обязательные для собственника требования к системам видеонаблюдения изложены в Постановлении Правительства РФ № 1273[2].

В связи с приведенными примерами можно утверждать, что первоначальное «насыщение» объектов системами видеонаблюдения завершено, соответственно, возникает вопрос – насколько эффективно используются полученные видеоматериалы, какие проблемы возникают при поиске и анализе видеоданных, какая квалификация специалистов, эксплуатирующих эти системы, является оптимальной для реализации полного функционала, заложенного на этапе проектирования.

Особое внимание хотелось бы остановить на вопросах подготовки специалистов. Очевидно, что весь потенциал системы видеонаблюдения (в т. ч. как компонента интегрированной системы безопасности) возможно реализовать только в случае соответствия квалификации персонала уровню сложности системы. Тренды последнего времени – использование интегрированных систем безопасности, создание ситуационных центров с возможностью объединения различных источников данных требуют от специалистов дополнительных компетенций.

Особенно явно это проявляется при анализе видеоданных как одном из этапов при проведении служебных проверок и

[2] Постановление Правительства РФ от 19.10.2017 г. № 1273.URL: https://base.garant.ru/71793560/

расследований, т. к. в ряде случаев специалист не только выполняет линейные операции по поиску и обработке информации, но и формирует экспертную модель, по которой проводится анализ. Второй пример – мероприятия по анализу видеоданных, направленные на поиск аномалий в производственной деятельности. В этом случае необходимо не только знать методологию поиска и анализа видеоинформации, но и разбираться в бизнес-процессах предприятия, уметь формировать выгрузки из базы 1С, формировать SQL-запросы в различные базы данных, в совершенстве знать остальные компоненты интегрированной системы безопасности.

Кроме того, одна из компетенций, которой должен обладать специалист по видеоанализу, – создание алгоритмов детекции событий и настройка уровней реагирования. Как уже отмечалось ранее, практически на всех крупных объектах отдельные компоненты системы безопасности объединены в интегрированные или комплексные системы. Управление этими системами, реагирование на тревожные события и анализ полученной информации осуществляется с использованием систем сбора и обработки информации (далее по тексту СОИ) на основе программно-аппаратных комплексов.

Основной целью внедрения подобных систем является возможность избавить оператора от огромного потока малозначимой информации и сосредоточить его внимание на наиболее важных событиях, которые требуют немедленной реакции. Это достигается проставлением весовых коэффи-

циентов событиям и их последующим ранжированием. Процедуру настройки системы СОИ, как правило, проводит экспертная группа, в нее в обязательном порядке включают специалистов-экспертов, которые будут заниматься последующей эксплуатацией системы.

Кроме оперативного мониторинга, использование систем сбора и обработки информации позволяет значительно увеличить эффективность проводимых аналитических мероприятий при проведении служебных расследований и проверок. Это достигается за счет:

– агрегации разных типов данных в рамках одной информационной модели;

– использования различных физических принципов для индексирования события (оптический, инфракрасный, акустический, вибрационный и другие каналы);

– создания виртуальных извещателей, состоящих из извещателей, работающих на разных физических принципах или использующих в качестве одного из каналов оптические данные (например, видеокамеры с интегрированными «тревожными входами»).

Таким образом, еще раз хотелось обратить внимание на актуальность вопросов, связанных с уровнем подготовки специалистов-экспертов, работающих в сфере обработки видеоинформации как частного случая, так и обработки данных всей системы СОИ предприятия в целом.

Именно с целью повышения квалификации специали-

стов-экспертов в данном руководстве рассмотрены практические примеры успешной реализации методик проведения служебных расследований с использованием видеоданных и данных, полученных с систем СОИ, рассмотрены технические вопросы, связанные с этапами создания и эксплуатации систем видеонаблюдения как составной части интегрированных систем безопасности.

Отдельно рассмотрены вопросы, связанные с определением перечня необходимых компетенций специалиста-эксперта, методов подготовки и разработки экспертных методик выявления аномалий в производственной деятельности предприятий.

Безопасность – это процесс, а не результат.
Великий князь Константин

1. Интегрированные системы безопасности

В данной главе рассмотрены вопросы создания и эксплуатации интегрированных систем безопасности. Основной акцент сделан на практических вопросах, возникающих у специалистов, использующих эти системы в своей профессиональной деятельности.

Определение интегрированной системы безопасности.

Чем интегрированная система безопасности отличается от комплексной.

В каких случаях внедрение интегрированной системы безопасности является обязательным для собственника.

Примеры реализации интегрированных систем безопасности.

Основные компоненты интегрированной системы безопасности.

Цели интеграции.

Система видеонаблюдения как компонент интегрированной системы безопасности, отличие от остальных компонентов системы.

Физические ограничения, которые необходимо учитывать при проектировании системы видеонаблюдения как источ-

ника анализируемых данных.

Информационная модель системы СОИ.

Практика эксплуатации интегрированных систем безопасности.

1.1. Система видеонаблюдения как компонент интегрированной системы безопасности

Интегрированная система безопасности – система безопасности объекта, объединяющая в себе целевые функциональные системы, предназначенные для защиты от угроз различной природы возникновения и характера проявления [3]. В состав интегрированной системы безопасности, как правило, входят следующие функциональные системы:

– система видеонаблюдения,

– система охранной и тревожной сигнализации,

– система контроля и управления доступом,

– технические средства досмотра (обязательны для обеспечения транспортной безопасности),

– системы связи и передачи информации,

– системы СОИ,

– системы противопожарной защиты (пожарная сигнализация, автоматическая система пожаротушения).

Именно интеграция всех систем на программном и (или) аппаратном уровне в рамках единого информационного про-

[3] ГОСТ Р 57674–2017.UPL: https://docs.cntd.ru/document/1200147050

странства позволяет получить максимальный эффект в части поиска и анализа информации и обеспечить максимально быстрое реагирование на тревожные события. Этим объясняется различие между интегрированными системами безопасности и комплексными, которые функционируют как отдельные системы.

Как уже было отмечено, система видеонаблюдения играет особую роль в системе СОИ, поскольку она единственный компонент системы, который является не только источником информации, но и средством для верификации тревожных сообщений от остальных компонентов. Пример – сработка периметрального извещателя, которая может быть вызвана как проникновением нарушителя на охраняемую территорию, так и ложной сработкой из-за ветра. При наличии системы видеонаблюдения оператору оперативно выводится изображение «тревожного» сектора, и в зависимости от полученной видеоинформации принимается решение либо о вызове группы задержания, либо о перепостановке на охрану сработавшего извещателя.

Следует отметить, что для обеспечения транспортной безопасности собственник объекта обязан использовать интегрированные системы безопасности (системы СОИ), имеющие соответствующий сертификат.

Почему мы постоянно акцентируем внимание на использовании системы видеонаблюдения в составе интегрированной системы безопасности, а далее и в составе информаци-

онной системы предприятия в целом? Прежде всего потому, что эти системы,сами являются поставщиками информации для индексации видеоархива и формирования базы данных для последующего анализа. Автономная система видеонаблюдения, даже наделенная интеллектуальными функциями, в основном работает в режиме «черного ящика», к которому обращаются в случае выявления какого-либо инцидента и ценность которого ограничена глубиной архива.

1.2. Проектирование системы видеонаблюдения с точки зрения специалиста-эксперта

Как отмечалось выше, одной из тенденций развития рынка интегрированных систем безопасности является построение систем, которые могут на начальном этапе обнаружить тревожное событие, индексировать его, присвоить весовой коэффициент, разослать полученную информацию по заданному сценарию пользователям системы для верификации события и принятия решения. В свою очередь, индексация событий создает базу для проведения анализа как повторяющихся бизнес-процессов, так и для поиска аномалий, в т. ч. аномалий, связанных с мошенническими действиями.

В связи с этим обратим внимание на некоторые технические характеристики систем видеонаблюдения, которые непосредственно влияют на возможность проведения дальнейшего анализа событий и не всегда учитываются на этапах подготовки технического задания и разработки проекта.

Прежде всего рассмотрим рекомендуемые технические характеристики видеокамер:

– разрешение не менее 2 Мп,

– динамический диапазон от 120 дБ,

– размер матрицы не менее 1/2,8”,

– термокожух (обязателен для внешней установки),

– наличие «тревожных» входов / выходов (обязательно при необходимости интеграции с другими системами на аппаратном уровне),

– требования к подсветке выбираются в зависимости от объекта,

– при использовании объектива с трансфокатором обязателен механический привод.

Этот набор параметров сформирован на основании опыта эксплуатации систем видеонаблюдения значительного количества объектов разного класса функциональности и массива в нескольких тысяч видеокамер. Комментируя вышесказанное, отметим: видеокамера – это первое звено в цепочке передачи информации. От качества полученных видеоданных будет зависеть возможность или ее отсутствие для проведения качественного анализа. Более сложная ситуация для «внешних» видеокамер, снег, дождь, изменение освещенности днем и ночью, засветка при восходе-закате солнца мало того, что значительно усложняют саму возможность получения качественных видеоданных, они осложняют процесс настройки видеокамеры для целей видеоанализа (использование разных режимов в течение суток, сезонная адаптация параметров).

В ряде случаев при проектировании системы видеонаблюдения приходится в т. ч. создавать дополнительную ин-

фраструктуру для гарантированного получения качественных видеоданных (навесы и индукционные петли на въездных группах, отдельная система охранного освещения, подбор специальных прожекторов для системы распознавания номерных знаков и т. д.).

Еще одно условие получения качественных видеоданных, о котором иногда забывают на этапе проектирования, – чистый объектив видеокамеры, на любом промышленном предприятии или объекте транспортной инфраструктуры достаточно сложная ситуация с наличием пыли и другой субстанции, которая оседает на объективах. Учитывая, что место расположения видеокамеры может быть на высоте от 6 до 12 метров, механическая очистка объективов требует времени, соблюдения ограничений, связанных с нормами проведения работ на высоте, поэтому в ряде случаев рационально использовать кожухи с интегрированными стеклоочистителями.

1.3. Разработка сценариев реагирования на события. Информационная модель системы СОИ

На первый взгляд вопрос разработки сценариев на событие в рамках информационной модели системы СОИ выходит за рамки вопросов, связанных с видеоанализом. При более глубоком изучении этого вопроса становится очевидным тот факт, что в сферу компетенций специалиста-эксперта в т. ч. входит задача поддержания информационной модели системы СОИ в актуальном состоянии. Для этого необходимо в совершенстве знать алгоритм настройки всех компонентов системы:

– настройка извещателей, интегрированных в систему видеонаблюдения (чувствительность, диапазон измерений, юстировка в пространстве);

– настройка детекторов видеокамеры (детектор движения, детектор пересечения линии, уровень реагирования на звук, вход в выделенную область, подсчет объектов, распознавание номеров машин и т. д.);

– настройка детекторов видеосервера (межкамерный тре-

кинг, сопровождение объекта, детектор машин, детектор людей, подсчет людей, тепловая карта, наличие аномалий – закрытие объектива, изменение юстировки, пропадание сигнала, детектор очереди и т. д.);

– настройка связи между элементами систем (видеокамера – извещатель, видеокамера – событие, видеокамера – отсутствие события), настройка составных и виртуальных извещателей;

– сопряжение потоков данных, проставление весовых коэффициентов, настройка маршрутов передачи информации.

Условно говоря, нужны две компетенции – техническая (внесение изменений в систему на уровне администратора) и аналитическая (изменение информационной модели в зависимости от изменения внешних факторов, целей обработки информации, выявления новых угроз).

Именно поэтому мы рассматриваем «техническую» компетенцию как обязательную в основной деятельности специалиста-эксперта.

Кратко о «аналитической» компетенции – как правило, информационную модель системы СОИ можно разделить по уровню сложности на две составляющие, это набор «стандартных» алгоритмов и «уникальные», которые разрабатываются под требования конкретного объекта и производственных процессов.

В свою очередь, «стандартные» алгоритмы можно разделить на:

– обязательные (выполнение которых обусловлено наличием соответствующего нормативного акта),

– технологические,

– обеспечения безопасности,

– контрольные.

К обязательным алгоритмам в качестве примера мы можем отнести запрет на проход на территорию людей без масок или средств индивидуальной защиты (далее по тексту СИЗ). Соответственно, сценарий будет создан из следующих шагов:

– идентификация лица без маски (СИЗ);

– блокировка карты доступа или запрет доступа на территорию объекта, если идентификация осуществляется по другому критерию (лицо, рисунок вен ладони и т. д.);

– индексация видеоряда зоны доступа с присвоением ID события, точки прохода, идентификатора нарушителя;

– присвоение коэффициента значимости события и передача информации по заданным адресам (подразделение охраны, отдел кадров и т. д.);

– запись события и логов действий операторов системы в архив.

К «технологическим» алгоритмам можно отнести весь набор алгоритмов, предназначенных для контроля ради нормального функционирования всей интегрированной системы безопасности и в ряде случаев смежных систем, например, это климатические установки.

Примерный перечень событий для активации «технологических» сценариев:

– закрытие объектива видеокамеры,

– пропадание сигнала с видеокамеры,

– невозможность постановки извещателя на «охрану»,

– превышение температуры / влажности в выделенном помещении,

– сработка извещателя затопления.

Очевидно, что «технологические» события имеют минимальный весовой коэффициент, основные пользователи информации этого рода – технические службы, осуществляющие эксплуатационное обслуживание систем. Оперативный персонал получает эту информацию в качестве уведомления для принятия решения не в режиме «тревоги», а в режиме «уведомления о неисправности системы» для изменения режима реагирования (например, при получении информации о неисправности раздела охранной сигнализации дается команда изменить маршрут патрулирования объекта).

Алгоритмы обеспечения безопасности включают в себя сценарии при реагировании на проникновение на объект или в выделенное помещение, пожар, активацию «тревожной кнопки» и т. д.

Контрольные алгоритмы предназначены в первую очередь для фиксации действий персонала (логирование реакции на тревожные события, идентификация при смене дежурства и т. д.)

Отличительной особенностью «стандартных» алгоритмов является то, что они достаточно хорошо прописаны практически в любой системе СОИ либо просты в реализации в связи с относительной простотой и интуитивно понятны в процессе формализации.

Более сложными являются «уникальные» алгоритмы, которые создаются для контроля производственных процессов конкретного предприятия. В ряде случаев для формирования технического задания создается экспертная группа, включающая в себя специалистов разных подразделений. В любом случае специалист-эксперт занимает особое место в этой группе, т. к. обладает знаниями о возможности системы в целом и отдельных компонентов в частности.

В завершение этой части необходимо отметить, что максимального эффектп для проведения эффективных аналитических мероприятий в рамках создания информационной модели системы СОИ удается достичь при организации обмена данными между учетной системой предприятия (например 1С) и системой СОИ. При реализации такого обмена термин «обогащение данных» приобретает явный практический смысл, т. к. возможности для формирования поисковых запросов становятся практически неограниченными.

1.4. Практика эксплуатации интегрированных систем безопасности

Прежде чем перейти к определению проблемы, кратко остановимся на этапах создания интегрированной системы безопасности:

– разработка технического задания,
– проектирование,
– монтаж и пусконаладка,
– испытания и ввод в эксплуатацию.

Все без исключения вышеперечисленные этапы достаточно хорошо формализованы, организации, осуществляющие проектные и монтажные работы, обладают огромным опытом деятельности, квалифицированным персоналом, компетенции подтверждены лицензиями, членством в СРО и другими документами. Поэтому с «технической» стороны по сути проблем нет, кроме проблемы выбора производителя оборудования и подрядной организации.

Проблемы начинаются на этапе начала эксплуатации. Название проблемы – кто должен обучать персонал, который будет эксплуатировать систему? В лучшем случае в пунктах договора на пусконаладочные работы будут разделы, обя-

зывающие исполнителя провести обучение. Как показывает практика, обучение проводят те же специалисты, которые проводят пусконаладку. Они очень хорошо знают предметную область в «технической» части, но плохо представляют специфику оперативного мониторинга объекта или работы ситуационного центра и тем более не обладают опытом проведения аналитических мероприятий. Второй подход – обучение проводят специалисты организаций, с которыми заключен договор на техническое обслуживание системы, полагаем, понятно, что и в этом случае ситуация не меняется в лучшую сторону.

Второй аспект – образовательный и профессиональный ценз обучаемого персонала. Не секрет, что должности оператора ПЦН (пульта централизованного наблюдения), диспетчера, сотрудника подразделений транспортной безопасности седьмой категории (работники, управляющие техническими средствами обеспечения транспортной безопасности) не являются конкурентными по уровню заработной платы, соответственно, образовательный ценз и мотивация такого персонала в ряде случаев не позволяют реализовать весь потенциал системы, заложенный на этапе проектирования.

Поэтому в ряде случаев и возникает явный разрыв между потенциальными возможностями интегрированных систем безопасности и реальным функционалом, реализованным на практике.

Без данных вы просто еще один человек с собственным мнением.

Уильям Эдвардс Деминг

2. Методология поиска и анализа информации

В данной главе рассмотрена практика поиска и анализа информации в интегрированных системах безопасности и информационных системах предприятия.

Поиск события в видеоархиве.

Поиск информации в целях проведения служебного расследования.

Анализ информации, выявление аномалий.

Алгоритмы поиска и анализа информации.

2.1. Черный ящик. Видеоархива всегда не хватает

Как показывает практика, большинство систем видеонаблюдения используются в режиме «черного ящика», т. е. при возникновении какого-либо инцидента оператор ищет информацию по времени (если оно известно), если нет, пытается найти искомый видеофрагмент по описанию. Основные трудности, с которыми сталкиваются операторы при таком режиме функционирования системы:

– глубина архива недостаточна, видеозапись отсутствует;

– событие произошло, например, неделю назад, точная дата неизвестна, соответственно, оператору необходимо просмотреть огромный массив видеоданных;

– оператор не нашел нужное событие.

На глубину архива оператор повлиять не может, этот параметр заложен на стадии проектирования, но у персонала, который настраивает систему видеонаблюдения, есть достаточно большой спектр возможностей по оптимизации, даже при фиксированной емкости накопителей. Тут мы опять возвращаемся к вопросу компетенций персонала.

Прежде всего остановимся на вопросе – какая глубина архива является оптимальной? Тезис «чем больше, тем луч-

ше» не проходит, т. к. стоимость накопителей с каждым годом растет, а высокое качество видеоматериалов находится в обратной пропорции к емкости накопителей.

Опытным путем и требованиями ряда нормативных актов[4] минимально достаточной определена глубина архива в 30 суток. Однако любой специалист-практик вспомнит массу случаев, когда очень важная информация, которая могла быть ключевой для раскрытия хищения или мошенничества, не была получена, потому что информация о факте стала известна, например, через два месяца. Иногда собственники объектов идут на траты и выделяют средства на увеличение емкости архива до трех и более месяцев, но практика показывает, что в ряде случаев видеозаписи нужны были и за больший период времени. Особенно часто такая информация нужна аудиторам, которые могут проявить интерес к событиям, которые произошли более года назад.

Методы решения этой проблемы способами, не связанными с увеличением емкости накопителей, мы рассмотрим позже.

Как мы уже отмечали, поиск информации при известной или приблизительно известной дате и времени не представ-

---

[4] В частности, по требованиям п. 30 Постановления Правительства РФ от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищенности мест массового, пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии РФ и форм паспортов безопасности таких мест и объектов (территорий)» глубина видеоархива должна быть не менее 30 дней.

ляет труда, все без исключения интерфейсы современных видеорегистраторов и программных продуктов ПАК позволяют ввести необходимые параметры и перейти непосредственно к нужному фрагменту. Иногда у операторов возникают проблемы с копированием найденного фрагмента на внешний носитель и «вырезкой» искомого фрагмента из общего видеоряда.

Намного более сложная задача – поиск фрагмента события, временные параметры которого определены диапазоном дат, например – вывоз похищенного материала был осуществлен в течение недели, въездная группа неизвестна, номерной знак и модель транспортного средства также неизвестны. Самый примитивный сценарий – когда оператор вынужден часами сидеть и просматривать видеоматериалы в поисках искомого события, и то если присутствуют возможность визуальной идентификации указанных признаков (вывоз в открытой бортовой машине). Этот пример еще раз подтверждает тезис о том, что ценность видеоматериалов не столько в их наличии, сколько в возможности найти нужное событие в огромном информационном массиве.

В практике проверочных мероприятий в отношении действий операторов относительно часто приходится сталкиваться с «пропуском» оператором нужного фрагмента при поиске видеоданных. Чаще всего это происходит с неопытными операторами, которые при просмотре видеоархива используют повышенную скорость воспроизведения более чем

в 4 раза) и просто не замечают нужное событие. Как уже отмечали, это прежде всего вопрос компетенций.

Между тем при анализе таких ошибок было выявлено, что у многих операторов была возможность значительно повысить эффективность поиска с помощью встроенных инструментов, даже без предварительной индексации видеофайлов. Речь идет прежде всего об опции с обобщенным названием Smart Search (у некоторых производителей она может называться по-другому). В отличие от аппаратных детекторов видеокамер и программных детекторов видеорегистраторов и видеосерверов, которые нужно заранее настраивать, задавая фиксированные зоны детекции, эта опция работает с архивом. При просмотре видеофрагмента вы выделяете нужную область, например, зону кадра, где должно проехать транспортное средство, после чего самим видеорегистратором осуществляется поиск фрагментов только с движением в этой области, таким образом вы получаете фиксированный набор видеофрагментов с проезжающим транспортом, при правильно настроенном фильтре остальной массив видеоданных можно не просматривать.

2.2. Служебная проверка или расследование

Организация поисковых и аналитических мероприятий при проведении служебной проверки или расследования предполагает наличие всего спектра инструментов, о которых упоминалось ранее. Прежде всего это наличие интегрированной системы безопасности, доступ к информационной системе предприятия для формирования запросов и получения отчетов, развитая система индексирования различных типов данных. В автоматическом режиме должны генерироваться следующие потоки данных:

– распознавание номеров автотранспорта на всех входных группах (в идеале зонирование предприятия и получение возможности идентификации транспортного средства по зонам),

– данные со средств весового контроля (если таковые имеются),

– данные СКУД,

– индексация видеоряда и снимков.

На последнем пункте остановимся более подробно. Мы обещали вернуться к теме увеличения архива без увеличения емкости накопителей. Естественно, в первую оче-

редь необходимо использовать возможности, предоставляемые производителями оборудования:

– использование современных кодеков в т. ч. H.265+;

– использование записи только по детектору движения (подходит для ограниченного количества контролируемых зон, используется только в случае крайней необходимости, когда глубина архива важнее потенциальной возможности «пропустить» нужную сцену);

– возможность снижать качество видеозаписи по истечении основного срока хранения или изменять частоту кадров архива.

Более интересен подход, связанный с фиксацией события в виде индексированного снимка (фрагмента видеозаписи), который может храниться практически неограниченное количество времени. Как мы уже отмечали – система видеонаблюдения является в т. ч. средством верификации, причем как оперативной, так и для подтверждения ранее произошедших событий. Дополнение «основного» видеоархива с ограниченной глубиной архивом снимков и коротких видеофрагментов с глубиной в несколько лет как раз и является эффективным средством для расширения функционала интегрированной системы безопасности. Примерами могут являться снимки всех въезжающих транспортных средств, причем одновременно можно делать снимок фронтальный с возможностью идентификации номерного знака и обзорный с верхнего сектора. Второй пример – снимок с видеокамеры,

логически связанной с системой охранной сигнализации при срабатывании периметрового извещателя.

Таким образом, используя вышеуказанную модель организации хранения данных, мы можем анализировать данные за достаточно большой период времени.

Ключевой особенностью сбора и анализа информации, осуществляемых специалистом-экспертом в рамках служебного расследования, является отсутствие конкретной информации о дате и месте наступления событий, которые могут явиться основой для верификации нарушения и формирования доказательной базы.

Некоторые авторы работ по теории корпоративного мошенничества используют термин «матрица расследования»[5].

Действительно, только при анализе значительного количества на первый взгляд разрозненной информации, полученной из различных источников, возможно как установить сам факт совершения противоправных действий, так и сформировать доказательную базу.

В отношении важности компонента системы видеонаблюдения как источника информации для формирования доказательств было отмечено: «Аудио- и видеозаписи представляют собой особый источник сведений, требующий дополнительного теоретического осмысления. При этом совер-

[5] Лактионова М. О. Методика проведения расследования корпоративного мошенничества в хозяйствующем субъекте / М. О. Лактионова, С. Н. Кашурников // Вестник евразийской науки. – 2022. – Т. 14. – № 6.URL: https://esj.today/PDF/57ECVN622.pdf

шенно очевидно, что технические возможности, существующие в настоящее время в распоряжении не только государства, но и частных лиц, выводят этот источник сведений на беспрецедентный по информативности и потенциалу познания уровень»[6].

Возвращаясь к термину «матрица расследования» следует пояснить, что источником информации при проведении служебной проверки являются не только технические средства, входящие в состав интегрированной системы безопасности, но и информация, полученная в ходе опроса должностных лиц, материалы, полученные в ходе ревизий, инвентаризаций, выгрузки из учетных систем предприятия и т. д.

Иногда именно изучение первичных документов (материалов конкурсных отборов, проведенных тендеров, полученных коммерческих предложений) является первым этапом для получения информации о возможных нарушениях, связанных с корпоративным мошенничеством.

В сложных случаях для проведения служебного расследования целесообразно формировать экспертную группу или комиссию, в которую, кроме сотрудников подразделения безопасности, входят профильные специалисты по аудиту, технические специалисты и юристы.

В этом случае основными задачами специалиста-эксперта

[6] Обидин К. В. О соотношении основания для возбуждения уголовного дела и оснований для предъявления обвинения в условиях цифровизации уголовного судопроизводства // Актуальные проблемы российского права. 2019. – № 6. – С. 147–155.URL: https://doi.org/10.17803/1994-1471.2019.103.6.147-155

будут:

– верификация информации в рамках «матрицы расследования»;

– формирование доказательной базы в соответствии с критериями относимости, допустимости и достоверности;

– выявление потребности в получении дополнительных сведений, формирование запросов в информационные базы предприятия и (или) запросов должностным лицам предприятия;

– передача информации руководителю экспертной группы (комиссии) информации для формирования заключения оп результатам служебной проверки.

2.3. Анализ информации. Поиск аномалий

Кардинально отличается методология действий специалиста-эксперта при анализе информации в рамках проведения мероприятий по поиску аномалий. Главное – он проводит работу не от выявленного факта совершения противоправных действий (или выявленных случаев недостачи материальных ценностей), а самостоятельно проверяет гипотезу о наличии причин и условий, которые не были идентифицированы на этапе оценки рисков при описании основных бизнес-процессов и создании системы контроля.

Естественно, квалификация специалиста-эксперта для проведения подобных мероприятий должна включать в себя глубокие знания бизнес-процессов предприятия.

В ряде случаев «заказчиком» таких мероприятий выступает подразделение, отвечающее за внедрение системы менеджмента качества (СМК) в рамках проводимого аудита или актуализации документации, регламентирующих выполнение требований СМК. При этом максимальный эффект достигается за счет того, что, имея «инструментальные» источники информации, специалист-эксперт выявляет реальные угрозы для предприятия, которые могут быть подтвер-

ждены документально.

На этом этапе снова хотелось бы вернуться к выражению «матрица расследования», т. к. оно наиболее емко характеризует суть работы специалиста-эксперта по анализу многомерных данных и сопоставления информации, которая на первый взгляд не является значимой.

В качестве примера можно привести следующую схему анализа – от обобщенной к целевой, которая на ряде предприятий была успешно реализована и способствовала предотвращению реального ущерба в цепочке поставок материалов:

– из всего массива данных о заезжающем на предприятие транспорте (дата, время, государственной номер) выявляются аномальные (в данном случае были выявлены транспортные средства, которые заезжали на предприятие только в выходные и праздничные дни), естественно, речь идет о предприятии, которое работает в круглосуточном режиме;

– после фильтрации данных и анализа времени заезда получаем еще один демаскирующий признак – эти транспортные средства иногда заезжали и в будние дни, но только в ночное время;

– далее проводится анализ режима работы основных подразделений предприятия, связанных с осуществлением деятельности в области логистики и контроля, которое иногда называют «день / ночь 48», и сравниваем со списком ранее выявленных транспортных средств, после чего получаем ин-

формацию о том, что контролируемые транспортные средства заезжали только в период работы одной и той же смены;

– следующий этап – верификация и выявление с использованием системы видеонаблюдения аномалий на этапах весового контроля, контроля качества поставляемых материалов, разгрузки в местах хранения материалов, для выявления нарушений в части осуществления функции контроля над качеством поставляемых материалов;

– формирование доказательной базы, инициализация служебной проверки по выявленным фактам, привлечение виновных лиц к ответственности.

Из приведенного примера понятно, что речь шла о нарушениях со стороны персонала предприятия, связанного с приемом материалов ненадлежащего качества в сговоре с поставщиками.

Этот пример выбран в связи с тем, что первый, самый важный этап по выявлению аномалий был приведен обезличенно, или, используя терминологию специалистов-профайлеров, без учета «криминального знания», т. к. сам факт заезда на территорию предприятия в определенные дни не может быть идентифицирован как угроза или риск. Еще раз акцентируем внимание на этом моменте с точки зрения психологии мошенника – он тоже просчитывает риски быть разоблаченным, поэтому заведомо старается исключить все демаскирующие признаки, и в первую очередь связанные с оформлением документов.

О психологии мошенничества будет более подробно рассказано в следующих разделах, пока отметим только тот факт, что, как правило, мошеннические действия планируют квалифицированные специалисты, работающие на предприятии не один год, хорошо знающие специфику работы предприятия, осуществляемые контрольные и режимные мероприятия, места установки технических средств охраны. Именно поэтому возможность анализа данных, на которые потенциальный мошенник не обращает внимания или которые не может контролировать, не только важна, но в ряде случаев является единственно возможной для выявления аномалий.

2.4. Методики анализа видеоинформации

Ранее уже отмечалось, что индексация видеоданных является эффективным способом повышения скорости поиска видеоинформации и одним из инструментов верификации данных в процессе анализа. В свою очередь, широкое внедрение технологий машинного зрения и технологий распознавания позволяет использовать обработанные видеоданные как источник информации для учетных систем предприятия и использовать не только в целях обеспечения безопасности, но и для управления логистикой, построения отчетов для различных подразделений организации, может являться источником данных для систем поддержки принятия решений (СППР).

Если обратиться к истории вопроса, длительное время система безопасности предприятия была автономной, аналоговые методы накопления и обработки видеоданных исключали возможность их использования, кроме как в целях визуального мониторинга территории или просмотра видеозаписей. Широкий спектр возможностей для интеграции этого источника информации как в систему СОИ, так и в информационную систему предприятия в целом и СППР в частно-

сти, возник после перехода на цифровые способы формирования, передачи и хранения видеоинформации. Естественно, степень интеграции системы безопасности предприятия с иными информационными системами зависит от категории объекта и ограничений по информационной безопасности.

Соответственно, аналитические мероприятия, проводимые специалистом-экспертом, рсуществляются по схожим методикам, которые используются в СППР. Возможно, единственное отличие – это целевая группа получателей информации (как правило, аналитические отчеты в СППР предназначены для топ-менеджеров и затрагивают вопросы бизнес-аналитики и стратегического развития предприятия, отчеты для целей безопасности имеют более прикладной характер и предназначены для лиц, определяющих политику в области оценки рисков, поиска уязвимостей и оперативного управления безопасностью).

Следует отметить, что форма реализации общей информационной модели предприятия не зависит от вида реализации конкретной системы. Типовой набор модулей и иерархия системы будет одинаковой. Пример реализации СППР[7] приведен ниже:

---

[7] Прокопенко Н. Ю. Системы поддержки принятий решений [Электронный ресурс]: учеб. пособие / Н. Ю. Прокопенко: Нижегор. гос. архитект.-строит. ун-т. – Н. Новгород: ННГАСУ, 2017. – 188 с.

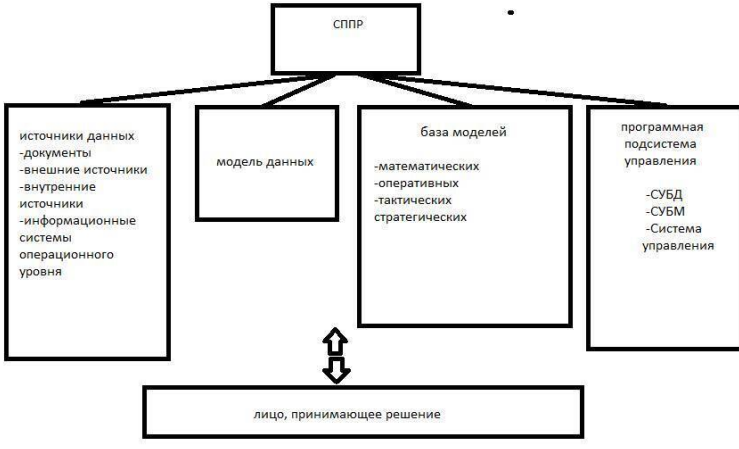

Рис. 1. Структура СППР

Основной функциональный набор методик СППР позволяет реализовать:

– формирование консолидированной отчетности,

– многомерный анализ данных (OLAP),

– выявление скрытых закономерностей (Data Mining),

– статистический анализ и прогнозирование временных рядов,

– формирование преднастроенных запросов,

– интеллектуальный поиск (по неполным данным и неформальным запросам).

Точное определение функционалу OLAP дано автором сетевого ресурса «Введение в многомерный анализ»[8]: «Следует отметить, что OLAP-функциональность может быть реализована различными способами, начиная с простейших средств анализа данных в офисных приложениях и заканчивая распределенными аналитическими системами, основанными на серверных продуктах. Т. е. OLAP – это не технология, а идеология».

Это определение еще раз подтверждает ранее выдвинутый тезис о возможности использования методов анализа информации для выявления аномалий, которые ранее не рассматривались в контексте прикладных задач обеспечения безопасности.

Кроме того, автором монографии[9] рассматривается возможность оперативной обработки информации, полученной от извещателей (датчиков в терминологии автора) с использованием методов многомерного анализа.

Как уже отмечалось, методики СППР прежде всего предназначены для решения бизнес-задач. Для использования в прикладных целях обеспечения безопасности, естественно, используется относительно небольшой набор следующих ал-

---

[8] Введение в многомерный анализ [Раздел сайта] –URL: https://habr.com/ru/articles/126810/ (дата обращения 19.09.2023 г.)

[9] Аббасова Т. С. Повышение эффективности систем поддержки принятий решений на основе многомерных хранилищ данных: монография / Т. С. Аббасова, В. М. Артюшенко, Э. Э. Акимкина; под науч. ред. д-ра техн. наук, проф. В. М. Артюшенко. – Москва; Берлин: Директ-Медиа, 2021. – 128 с.

горитмов[10]:

– авторегрессионный – модель временного ряда, в которой его текущее значение линейно зависит от предыдущих. Основное назначение – прогнозирование, выявление тенденций и других особенностей;

– алгоритм последовательного покрытия – генерирующий набор классифицирующих правил, которые последовательно разделяют обучающее множество на подмножества до тех пор, пока в каждом из них не останутся только объекты одного класса;

– бинарная классификация – классификация с бинарной выходной переменной, которая может принимать только два значения. Относит объект к одному из двух классов;

– дискриминационный порог – в статистике и машинном обучении значение дискриминирующей функции в задачах бинарной классификации, которое позволяет разделять классы;

– задача классификации – задача разделения множества наблюдений на группы, называемые классами;

– квантование – процесс обработки данных, который преобразует непрерывные данные в дискретные путем замены значений диапазонами;

– класс – группа объектов или явлений, обладающими общими свойствами. Выявление классифицирующих правил

[10] Вики [Раздел сайта] –URL: https://wiki.loginom.ru/algorithms.html (дата обращения 20.09.2023 г.)

называется задачей классификации, а процесс распределения объектов по классам – классификацией;

– корреляция – статистическая взаимосвязь двух или нескольких случайных величин;

– нормализация данных – метод предобработки числовых признаков в обучающих наборах данных с целью приведения их к некоторой общей шкале измерений без потери информации о различии диапазонов;

– регрессионный анализ – набор статистических процедур для изучения зависимостей между случайными переменными;

– скоринговая карта – набор характеристик с присвоенными весовыми коэффициентами;

– сэмплинг – процесс отбора из исходного набора данных выборки наблюдений, представляющих интерес для анализа;

– теорема Байеса – определяет вероятность события с привлечением связанным с ним знаний и условий. Например, если вероятность возникновения пожара связана с проведением огневых работ, то учет проведения огневых работ позволяет более точно оценить вероятность пожара в контролируемый период времени;

– факторный анализ – направление математической статистики, помогающее обнаружить наиболее важные факторы, которые влияют на исследуемые процессы или объекты.

В заключение этого раздела особо выделим методику разведочного анализа, которая в целом объединяет все алгорит-

мы, необходимые для достижения целей обработки данных в контексте предметной области, рассматриваемой в данном пособии.

Понятие «разведочный анализ данных» введено математиком Джоном Тьюки, который сформулировал цели такого анализа:

– максимальное «проникновение» в данные,
– выбор основных структур,
– выбор наиболее важных переменных,
– обнаружение отклонений и аномалий,
– проверка основных гипотез,
– разработка начальных моделей.

Возможность украсть создает вора.
Ф. Бэкон

3. Психология мошенничества

Как уже было отмечено ранее, данное пособие прежде всего адресовано специалистам, связанным с обеспечением безопасности. Поэтому обойти область знаний, связанную с психологией мошенничества и практикой противодействия, в связи с ее относительной «отвлеченностью» от названия пособия и «технической» направленности в целом все-таки было бы неверно.

Тем более в процессе изложения материала мы опять вернемся к теме подготовки данных для анализа и особое внимание обратим на возможные искажения данных как результат направленных действий заинтересованных лиц.

3.1. Модель нарушителя

В процессе проектирования систем безопасности на этапе создания модели угроз и проведения оценки уязвимости объекта[11], как правило, рассматривается модель нарушителя.

Следуя этой методике, рассмотрим модель нарушителя в контексте анализа угроз экономической безопасности и попытаемся выделить основные отличительные характеристики. Поскольку речь идет о внутреннем нарушителе, эти характеристики следующие:

– осведомленность о структуре предприятия, основных бизнес- и технологических процессах;

– осведомленность о внедренных на предприятии мерах контроля и режима, осведомленность о местах установки видеокамер и технических систем охраны;

– в зависимости от занимаемой должности возможность влиять на достоверность информации, отражающей количественный учет движения товарно-материальных ценностей, или информации о количестве и качестве производимых работ (услуг) подрядными организациями.

---

[11] Каликина Т. Н. Транспортная и технологическая безопасность: учебное пособие / Т. Н. Каликина, Н. А. Кузьмина, А. И. Ташлыкова. – Хабаровск: Изд-во ДВГУПС, 2019. – 106 с.

Третий пункт особенно важен в контексте обещания вернуться к теме подготовки данных для анализа, т. к. на основе созданной модели нарушителя мы можем допустить, что в ряде случаев данные, используемые в информационной системе предприятия, изначально недостоверны, соответственно, выходной результат тоже будет искажен.

Мы акцентируем внимание на этой проблеме потому, что очень часто при анализе данных особое внимание обращают на математические модели исследования, параметры информационных систем. Однако забывают, что данные, полученные с технических систем, и данные, которые поступают из документов (товарно-транспортных накладных, актов приемки работ, материалов по проведенным тендерам и т. д.), обладают кардинальным отличием: в первом случае корреляция между источником данных и результатом обработки этих данных отсутствует, во втором всегда есть риск искажения данных как по причине мошенничества, так и по причине халатности.

Соответственно, возможность проверять данные, полученные из различных источников, кардинально меняет уровень защищенности предприятия, в т. ч. от угроз совершения мошеннических действий персонала.

В части психологических характеристик нарушителя особо хотелось бы выделить следующие особенности:

– как показывает практика, чаще нарушитель действует в составе группы с разной степенью осведомленности о харак-

тере нарушений (иногда роль участника группы сводится к фактическому бездействию в части выполнения своих должностных обязанностей). Это обусловлено тем, что любая развитая система контроля на предприятии исключает возможность неконтролируемых действий отдельного сотрудника при перемещении товарно-материальных ценностей или денежных средств;

– отсутствие личной ответственности, оправдание корыстной заинтересованности низким уровнем оплаты труда или иными «внешними» факторами;

– зависимость от чужого мнения, принятие ложных ценностей «здесь всегда так было».

3.2. Методы выявления признаков мошенничества

В предыдущей части мы рассматривали разные источники информации с точки зрения рисков получения недостоверных данных. При оценке достоверности данных целесообразно использовать следующие методы:

– анализ достоверности информации на основании методов математической статистики (особое внимание следует уделять данным, не соответствующим принципам случайного распределения);

– сравнение данных с «эталонным» банком данных (например, тайминг на выполнение конкретной типовой операции);

– выборочная целевая проверка документальных источников информации на предмет выявления признаков фальсификации (создание базы скан-копий для возможности последующего анализа);

– наличие округленных сумм, совпадение сумм до знаков после запятой в коммерческих предложениях разных поставщиков и т. д.;

– информация в документах противоречит техническим параметрам (например, вес ввозимого материала не соответ-

ствует грузоподъемности машины);

– экспертный анализ оригиналов коммерческих предложений, полученных в ходе проведения конкурсного отбора или проведения тендера (признаки подделки, изготовление коммерческих предложений от разных поставщиков одним исполнителем, анализ метаданных цифровых версий документов);

Автор публикации[12], описывая методы противодействия мошенническим действиям, использует термин «диагностика слабых сигналов», ниже приведены выборочные строки из перечня вышеуказанной публикации:

– договоры, не содержащие конкретных условий сделки;

– различные формы стимулирования решения под предлогом срочности, уникальности или отсутствия альтернатив;

– чрезвычайно лояльные контрагенты, выполняющие работы длительное время «без денег»;

– регулярные неурочные работы;

– регулярные поломки контрольно-измерительного оборудования (от нас добавим – поломки технических средств обеспечения безопасности);

– приглашения сотрудников на конференции за счет фирмы потенциального поставщика.

---

[12] Елисеев С. Мошенничество персонала: основные схемы и методы борьбы.URL: http://svel.su/wp- content/uploads/2012/04/moshennichestvo_personala_economicheskie_prestuplenia.pdf

3.3. Корпоративная система противодействия мошенничеству

Корпоративное мошенничество как одна из угроз экономической безопасности предприятия не является уникальной угрозой, присущей только хозяйствующим субъектам нашей страны. В этом отношении интересен опыт зарубежных специалистов по идентификации данного вида угроз.

В отчете, опубликованном ассоциацией сертифицированных экспертов по борьбе с мошенничеством (ACFE) за период 2020–2022 гг., рассмотрены 2110 кейсов в 133 странах.

Ниже приведены выдержки из указанного отчета:

– топ индустрий по коррупции: энергетика (64 %), производство (59 %), транспортировка и складирование (59 %), информационная сфера (58 %), строительство (56 %);

– компании теряют ежегодно около 5 % выручки (показатель не изменился с 2020 г.);

– наиболее распространенным видом корпоративного мошенничества остается незаконное присвоение активов (89 %);

– наименее распространено мошенничество с финансовой отчетностью (9 %).

В целом представленные данные (с учетом региональной

специфики) можно использовать для оценки рисков в т. ч. внутри предприятия, заменяя понятие «индустрия» на «подразделение» или «департамент».

Соответственно, для анализа рисков по рассматриваемой теме в первую очередь нужно обратить внимание на функциональные подразделения в сфере:

– закупочной деятельности,
– строительства,
– реализации товаров / услуг,
– обслуживания и ремонта,
– логистики,
– информационных технологий.

В завершение этой части хотим отметить, что, естественно, при оценке угроз корпоративного мошенничества учитывается образовательный и профессиональный уровень потенциального нарушителя. Потому в этом контексте мы также должны оценивать квалификацию специалистов, которая позволяла бы адекватно противодействовать угрозам.

По мнению автора[13], среди основных проблем противодействия корпоративному мошенничеству остается недостаточная квалификация специалистов (как общая, так и специальная).

---

[13] И. А. Лебедев. Финансовый университет при правительстве РФ. Актуальные вопросы организации защиты компании в современных условиях. Противодействие мошенничеству, правила проведения внутреннего корпоративного расследования. [Раздел сайта].URL: http://www.fa.ru/org/dep/arieb/Documents/Forms/AllItems.aspx (Дата обращения 25.09.2023 г.)

Опыт – это то, что получаешь, не получив того, что хотел.

Карлос Кастанеда

4. Профессиональная подготовка специалистов-экспертов

Актуальность темы профессиональной подготовки специалистов-экспертов хотелось бы подтвердить прежде всего практическими примерами «запросов» со стороны работодателей. Также в этом разделе будет проведен анализ требований к квалификации специалистов, осуществляющих трудовые функции, связанные с обеспечением безопасности и, как частный случай, функции поиска и анализа цифровой информации, которые отражены в профессиональных стандартах, утвержденных в период 2018–23 гг.

Как было отмечено в начале данного пособия, относительно часто потенциальные возможности современных систем обеспечения безопасности не могут быть реализованы из-за недостаточной квалификации специалистов, непосредственно эксплуатирующих эти системы. Полагаем, что по мере усложнения указанных систем, общей тенденции «цифровизации» всех процессов управления предприятием этот тренд сохранится.

Соответственно, используя обобщенное наименование «специалист-эксперт», мы подразумеваем наличие у такого сотрудника компетенций в различных областях знаний,

он либо самостоятельно, либо в составе группы профильных специалистов принимает участие не только в части оперативного управления системами безопасности, но и в части модернизации и поддержки в актуальном состоянии всех компонентов системы.

Анализируя состояние рынка труда по рассматриваемой тематике и сравнивая «запросы» работодателей к квалификации сотрудников (по открытым материалам сайтов по трудоустройству и профильных интернет-ресурсов), можно определить увеличение частоты запросов к наличию следующих компетенций (стиль запросов сохранен):

– аналитика систем видеонаблюдения и контроля доступа;

– предоставление отчетов и предложений по улучшению безопасности;

– опыт в обработке данных, собранных системой видеонаблюдения, и проведении мероприятий по видеоаналитике;

– знание и понимание бизнес-процессов в складской, кассовой дисциплине, умение контролировать учет товара в системе, анализировать товародвижение, работать с системой видеонаблюдения;

– принимать участие в проведении служебных расследований, работать с видеоархивом;

– управление электронными системами безопасности (СКУД, СВН и др.), взаимодействие с финансовыми и бизнес-подразделениями в процессе Due Diligence.

Еще лет пять назад набор требуемых компетенций в ос-

новном сводился к возможности специалиста осуществлять оперативный мониторинг и работать с видеоархивом системы видеонаблюдения. Необходимо также отметить еще одну тенденцию – в ряде случаев работодатели набор компетенций, связанных с обработкой цифровых видеоданных, требуют от специалистов, выполняющих контрольные функции (аудиторов, сотрудников ревизионных подразделений и т. д.).

В целом это общий тренд современного состояния рынка труда и запросов «реального» сектора экономики». Все больше новых специальностей появляются на стыке исторически сложившихся профессиональных специализаций, а вопросы обеспечения безопасности коммерческого предприятия в первую очередь рассматриваются как бизнес-процессы – регламентированные, открытые, с набором метрик KPI.

Кроме требований работодателей, интересно провести анализ требований к уровню компетенций, определяемых профессиональными стандартами, утвержденными соответствующими приказами Минтруда РФ.

Предлагаем рассмотреть профессиональный стандарт специалиста по моделированию, сбору и анализу данных цифрового следа[14]

[14] Минтруд России. ВНИИ ТРУДА Минтруда России. Профессиональные стандарты [Раздел сайта]URL:https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=86707 (Дата обращения

В разделе «Общие сведения» указан вид профессиональной деятельности – проведение комплексного анализа цифрового следа человека (группы людей) и информационно-коммуникационных систем (далее ИКС).

Трудовые действия:

– разработка метрик оценки качества цифрового следа;

– очистка данных цифрового следа (поиск аномалий, корректировка, подсказка, автоматизация / уменьшение объема ручной работы, поиск дубликатов);

– автоматизация выявления закономерностей в массивах данных;

– анализ потребностей и целей пользователей (людей, групп людей и ИКС);

– экспорт результатов анализа в разных форматах;

– выдача комплексных заключений по результатам обработки данных;

– согласование и утверждение требований к результатам аналитических исследований.

Необходимые знания:

– алгоритмы очистки данных цифрового следа (поиск аномалий, корректировка, подсказка, автоматизация / уменьшение объема ручной работы, поиск дубликатов);

– специализированное программное обеспечение для анализа данных;

– способы визуализации данных;

25.09.2023 г.)

– программное обеспечение для визуализации данных;

– языки программирования;

– математическая статистика;

– систематические классификаторы и рубрикаторы (таксономий и онтологий);

– методы проверки целостности данных;

– требования законодательства Российской Федерации о защите персональных данных и т. д.

В целом трудовые действия и необходимые знания, определяемые в данном профессиональном стандарте, во многом соответствуют набору профессиональных компетенций, ранее рассмотренных в пособии. Основное отличие – в типе ИКС, в стандарте прежде всего идет речь о глобальной ИКС «Internet», в рамках прикладных задач пособия в первую очередь рассматривалась локальные ИКС предприятия. Тем не менее общий понятийный аппарат и схожие цели обработки данных позволяют рассмотреть этот пример как подтверждение наличия запроса на специалистов, способных собирать, анализировать и представлять заказчику обработанные цифровые данные в разных сегментах производственной деятельности.

Вопросы профессиональной подготовки специалистов не могут быть рассмотрены вне анализа программ учебных заведений, осуществляющих подготовку кадров.

Учитывая стремительное развитие новых технологий обработки информации, в ряде случаев целесообразно об-

ратиться еще к одному способу получения знаний – обучению по программам предприятий – изготовителей как программно-аппаратных комплексов, так и производителей программных продуктов для обработки и визуализаций данных и платформ Low-code и No-code.

Преимущество такого подхода обусловлено в т. ч. тем, что очень часто обучение ведут специалисты, которые внедрили тот или иной продукт на реальных предприятиях и способны акцентировать внимание обучающегося на наиболее важных практических аспектах.

В заключение хотелось бы отметить, что ценность специалиста и его востребованность на рынке труда в целом можно описать по следующей схеме: профильное базовое профессиональное образование – практический опыт – повышение квалификации в течение всего периода профессиональной деятельности. Компетенции в части сбора, анализа и представления цифровой информации в целом и видеоданных в частности будут полезны как сотрудникам подразделений безопасности, так и другим сотрудникам, чья деятельность связана с прикладным анализом данных.

Пусть не корят меня за то, что я не сказал ничего нового: ново уже само расположение материала.

Блез Паскаль

Заключение

Ранее мы обозначили круг специалистов, которым может быть интересно данное пособие. Кроме того, мы пытались на только обозначить конкретные методики, но и в целом выявить тенденции на рынке труда, которые помогут специалистам определить вектор своего профессионального развития. Во многом сложившаяся ситуация связана с тем, что исторически «цифровизация» сферы безопасности наступила позже, чем в других бизнес-процессах. Отчасти это произошло из-за того, что многие собственники рассматривали «безопасность» не как основной бизнес-процесс, а как функцию обеспечения деятельности, отчасти это было следствием «закрытости» самих специалистов в данной предметной области. С другой стороны, обозначенный временной лаг как раз позволяет предположить огромный потенциал «цифровизации» этого направления, особенно в контексте обработки видеоданных цифровых систем видеонаблюдения, которые традиционно входят в арсенал технических средств обеспечения безопасности.