

УДК 004.624

Разработка программного модуля поиска нарушений для интегрированной системы безопасности

В. И. Ронзин, Е. Ю. Никитина

Пермский государственный национальный исследовательский университет

Россия, 614990, г. Пермь, ул. Букирева, 15

ronzin9696@gmail.com; +79323327301

Рассмотрен способ обнаружения нарушений требований трудового распорядка работниками организации с помощью реализации внешнего программного модуля, который интегрирует данные из системы контроля и управления доступом и системы управления видеонаблюдением внутри интегрированной системы безопасности и позволяет выявлять два вида нарушений. В рамках производственной практики от Пермского университета данный программный модуль частично реализован и внедрен в одном из крупных учреждений Пермского края.

Ключевые слова: программные системы; контроль доступа; интегрированные системы безопасности; обработка данных.

DOI: 10.17072/1993-0550-2020-1-69-73

Введение

В настоящее время в крупных организациях внедряются интегрированные системы безопасности (ИСБ), которые обеспечивают контроль доступа на территорию учреждения, управляют пожарной и охранной сигнализацией, вентиляцией, электропитанием и организуют систему управления эвакуацией в случае чрезвычайной ситуации на объекте.

Данные системы автоматизируют процессы, связанные с обеспечением безопасности работников и клиентов на территории учреждения. Их применение в значительной мере ускоряет работу контрольно-пропускного пункта в крупном учреждении, позволяет быстро выявлять неисправности в системах энергоснабжения, вентиляции и пожарной сигнализации. Также современные ИСБ реализуют встроенные программные системы управления IP-видеокамерами (ПСУВ), которые позволяют обрабатывать видеопотоки с большого числа ви-

деокамер, находящихся на территории учреждения, и по ним создавать видеоархив.

ПСУВ позволяют создавать историю событий, происходивших на территории организации, к которой можно обратиться в случае возникновения нестандартных ситуаций для анализа происшедшего и вынесения взвешенного управленческого решения.

На практике с точки зрения безопасности большой интерес представляет анализ и сопоставления данных из ПСУВ с данными из системы контроля и управления доступом (СКУД) интегрированной системы безопасности, а именно сопоставление идентификатора сотрудника из СКУД и кадров из видеопотока входа на контролируемую зону для выявления разного рода нарушений, начиная от передачи электронно-пропускной карты третьим лицам и заканчивая нарушениями работниками требований трудового распорядка.

1. Описание решения по выявлению нарушений в ИСБ

Для разработки решения были рассмотрены две интегрированные системы безопасности, одна из которых была ранее внедрена на рассматриваемом предприятии по решению руководства этого предприятия. К разработке решения было предъявлено требование универсальности с тем, чтобы при возможной смене интегрированной системы безопасности результат разработки оказался переносимым для применения совместно с другой ИСБ.

Были рассмотрены системы "Орион Про" и "Индибирка".

При рассмотрении функциональных возможностей обеих систем было выявлено, что каждая из них обладает программными модулями, которые позволяют:

- 1) создавать в системе пользователей и привязывать к их электронным профилям персональные электронно-пропускные карты;
- 2) СКУД позволяет фиксировать в базе данных события о прохождении работника организации через терминал входа в здание;
- 3) ПСУВ позволяет формировать видеоархив, реагируя на события СКУД;
- 4) программный модуль генерации отчетов позволяет извлекать данные о событиях СКУД из базы данных.

Рассмотренные интегрированные системы безопасности позволяют реализовывать внешний программный модуль, который будет анализировать выходные данные СКУД и ПСУВ и выявлять акты несанкционированного доступа на территорию организации, связанные с использованием индивидуальной электронно-пропускной карты третьим лицом, а также обнаруживать нарушения требований трудового распорядка работниками учреждения.

Выходные данные СКУД внешний программный модуль будет получать в отчетах, формируемых системой генерации отчетов, а выходные данные ПСУВ будет получать из архива, сформированного на основе видеопотоков камер, подключенных к системе.

Модули СКУД и ПСУВ внутри различных ИСБ достаточно гибко настраиваются. Это позволяет при одинаковой настройке вы-

ходных параметров данных модулей дать возможность обработки генерируемых ими данных разрабатываемому нами решению.

Общая схема взаимодействия внешнего программного модуля и ИСБ с целью поиска нарушений требований трудового распорядка представлена на рис. 1.

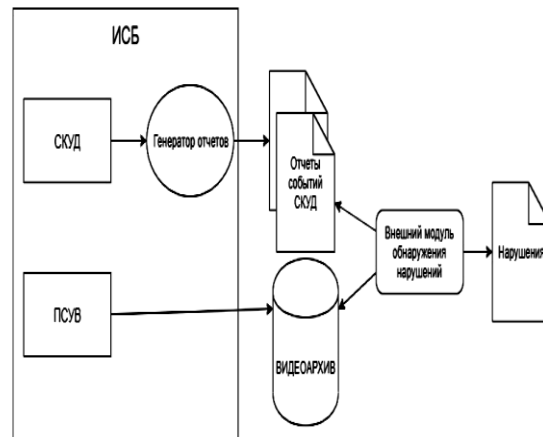


Рис. 1. Схема интеграции и обработки данных СКУД и ПСУВ через внешний программный модуль

2. Описание конфигурации модулей интегрированной системы безопасности

В базе данных ИСБ в организации хранится следующая информация о пользователях системы:

- 1) идентификатор персональной электронно-пропускной карты;
- 2) полное имя;
- 3) персональная фотография;
- 4) номер компании;
- 5) название отдела;
- 6) должность;
- 7) пол.

СКУД сконфигурирована таким образом, что автоматически сохраняет в базе данных информацию о проходе работником через терминал входа в здание, реагируя на прикладывание электронно-пропускной карты.

ПСУВ сконфигурирована таким образом, чтобы автоматически производилась обработка событий от ИСБ. В момент возникновения события камеры, установленные непосредственно у терминала входа в здание, записывают 20 сек. видеопотока в архив – 10 сек. до возникновения события и 10 сек. после его возникновения.

Таким образом, формируется видеоархив событий СКУД о проходе работниками терминалов входа в здание.

Перед началом разработки внешнего программного модуля была произведена настройка системы генерации отчетов для последующего извлечения данных о событиях СКУД из ИСБ. В системе генерации отчетов было создано задание на формирование один раз в месяц отчета "Первый вход и последний выход" работников за прошедший месяц и сохранения его в CSV формате.

Данный отчет включает в себя полную информацию о сотруднике, хранящуюся в базе данных ИСБ, а также информацию за каждый день из СКУД о времени его первого входа на территорию организации и времени последнего выхода. Объем информации в отчете составляет за месяц порядка 20000 записей.

Видеоархив, необходимый для анализа на возможные нарушения в ИСБ, представляет собой определенную структуру папок, разделенных по дате записи видеофайлов.

3. Описание нарушений

Первая задача, которую было необходимо реализовать в рамках внешнего программного модуля – задача нахождения нарушителей, которые приходят на работу вовремя, производя отметку на терминале входа в здание, но уходят с работы раньше положенного времени.

Для решения поставленной задачи было рассмотрено два рода нарушителей:

1) нарушители, которые уходят раньше времени через "черный вход", минуя терминал входа в здание;

2) нарушители, которые уходят раньше времени, оставляя пропускные карты одному человеку, который в конце смены всех отмечает, как вышедших вовремя.

Совместно с руководством организации были определены критерии каждого из вышеуказанных видов нарушений.

Критерий, определяющий наличие нарушения первого вида состоит в том, что программа анализирует временные интервалы работы сотрудников организации, а именно – в какое время они присутствовали на работе. Считается нарушением, если найдена отметка о входе сотрудника в учреждение, но не найдена отметка о выходе из учреждения в

этот же день, при условии, что на следующий день человек вновь пришел на работу.

Дополнение к формулировке критерия было сделано для того, чтобы не считать нарушением тот случай, когда сотрудник остался на ночное дежурство – в таком случае у него будет отметка входа, но отметки выхода не будет, а на следующий день не будет отметки входа, но будет отметка выхода.

Критерий, определяющий наличие нарушения второго вида состоит в том, что нарушением считается ситуация, если группа сотрудников из трех и более человек покинула территорию учреждения, произведя отметку выхода, из одного терминала в течение 7 секунд подряд. Данное нарушение является поводом к просмотру видеозаписи с этого терминала для уточнения обстоятельств события.

4. Реализация программного модуля поиска нарушений

Для реализации внешнего программного модуля был выбран язык программирования C# 7.0 на платформе .NET Framework 4.7.2 в среде разработки Visual Studio 2019 Community. Разработанный модуль является WPF-приложением с использованием библиотек Catel, для реализации паттерна проектирования MVVM. Технологический стек реализации был выбран из-за широкого набора открытых библиотек для платформы .NET и языка C#. Также технология WPF в связке с паттерном MVVM позволяет за короткий срок разработать приложение, обладающее удобным графическим интерфейсом и являющееся легко расширяемым для добавления новой функциональности по мере необходимости.

Приложение состоит из трех сборок:

1) сборка Core – реализовывает загрузку и парсинг получаемого из ИСБ отчета в объекты сборки Domain;

2) сборка Domain – содержит основную логику программы по анализу данных и поиску нарушений сотрудниками режима "вход-выход";

3) сборка BolidGui – графический интерфейс приложения.

Реализация программы была выполнена в несколько этапов:

1. Написание программного модуля для загрузки и парсинга CSV-отчетов. В этом модуле программа загружает отчет и создает из

него множество объектов сборки домена – сущностей сотрудников и других сущностей, пригодных для анализа.

2. Написание программного модуля домена, в которой реализованы основные сущности и логика по нахождению нарушений режима прохода.

3. При взаимодействии с руководством организации разработка и написание графического интерфейса пользователя для визуализации данных, полученных при анализе CSV-отчета.

5. Тестирование программного модуля на реальных данных

Тестирование разработанного программного модуля поиска нарушений проводилось на трех видах отчетов ИСБ:

1. "Небольшой" отчет (порядка 2000 записей), сформированный на данных за прошедшие два дня работы организации.

2. "Стандартный" отчет (порядка 20000 записей), включающий данные за месяц.

3. "Большой" отчет (порядка 40000 записей), содержащий данные за два месяца работы организации.

В отчете за два дня работы организации обнаружено 12 нарушителей, у каждого из которых по одному нарушению. Общее количество сотрудников, прошедших терминалы на вход за два дня – 546.

В месячном отчете зафиксировано 211 нарушителей. 204 нарушителя 1-го рода и 9 нарушителей 2-го рода, двое из них являются нарушителями 1-го и 2-го рода одновременно. Максимальное количество нарушений – 11.

Для проверки нарушений 2-го рода были просмотрены видеозаписи с терминалов в эти временные интервалы – обнаружено, что нарушения 2-го рода были ложными тревогами, поскольку люди выходили цепочкой. Общее количество сотрудников, прошедших терминалы на вход за месяц, – 758.

В отчете за два месяца было зафиксировано 417 нарушителей. 405 нарушителя 1-го рода и 15 нарушителей 2-го рода, трое из них являются нарушителями 1-го и 2-го рода одновременно. Максимальное количество нарушений – 46. Видеозаписи с терминалов во временных интервалах нарушений 2-го рода, также были проверены – обнаружено, что нарушения второго рода были ложными.

Общее количество сотрудников, прошедших терминалы на вход за месяц – 880.

Выводы

В настоящее время предложено и реализовано решение по интеграции и последующей обработке данных из СКУД и ПСУВ интегрированной системы безопасности с целью поиска нарушений требований трудового распорядка работниками. Решение позволяет находить нарушителей с помощью внедрения внешнего программного модуля, который анализирует данные из отчетов о событиях СКУД, классифицируя события на несанкционированные и штатные.

В дальнейшем внешний программный модуль будет доработан для поиска ситуаций несанкционированного доступа с использованием электронно-пропускных карт третьими лицами.

Внешний программный модуль будет обращаться к видеоархиву ПСУВ для извлечения нескольких кадров в момент прохода сотрудника через терминал входа в здание. Приложение будет предоставлять возможность сопоставлять данные события СКУД прохода работника через терминал (включая фотографию сотрудника из профиля, привязанного к электронно-пропускной карте), с реальным изображением того, кто через этот терминал проходил.

Данная функциональность позволит выявлять несанкционированное использование и передачу электронно-пропускных карт третьим лицам.

Список литературы

1. *Интегрированные системы безопасности: современные решения и тенденции.* URL: http://www.sigma-is.ru/articles/ISB_resheniya_i_tendencii.html (дата обращения: 08.11.2019).
2. *Руководство по эксплуатации АРМ "Орион Про".* URL: https://bolid.ru/files/373/566/re_arm_orion_pro_1.20.1.pdf (дата обращения: 08.11.2019).
3. *Руководство системного программиста СПО "Индирикка".* URL: <http://www.sigma-is.ru/products/software/id-spo/pm5.html> (дата обращения: 08.11.2019).

4. *Руководство* программиста СПО "Инди-гир-ка". URL: <http://www.sigma-is.ru/products/software/id-spo/pm5.html> (дата обращения: 08.11.2019).

5. *Руководство* оператора СПО "Инди-гир-ка". URL: <http://www.sigma-is.ru/products/software/id-spo/pm5.html> (дата обращения: 08.11.2019).

Development of the violation detection software module for the integrated security system

V. I. Ronzin, E. Yu. Nikitina

Perm State University; 15, Bukireva st., Perm, 614990, Russia
ronzin9696@gmail.com; +79323327301

The way of detection of infringements of requirements of a labor schedule by workers of the organization by means of realization of the external program module which integrates the data from system of the control and management of access and system of management of video cameras in the integrated system of safety is considered and allows to reveal two kinds of infringements. Within the framework of industrial practice from the Perm University this software module is partially implemented and implemented in one of the major institutions of the Perm.

Keywords: *software systems; access control; integrated safety systems; data processing.*