

РАЗРАБОТКА ФУНКЦИОНАЛЬНОЙ МОДЕЛИ ПРОЦЕССА АУТЕНТИФИКАЦИИ СОТРУДНИКА НА КПП

С.А. Евдокимова, Е.О. Залукаев

ФГБОУ ВО «Воронежский государственный университет инженерных
технологий»

В статье описывается разработанная функциональная модель в нотации IDEF0 процесса аутентификации сотрудника на КПП, на основе анализа которой отмечаются недостатки бумажных пропусков. Для повышения уровня информационной безопасности и пропускной способности предлагается усовершенствованная модель процесса аутентификации сотрудника на основе биометрии лица.

Ключевые слова: методология IDEF0, модель «AS-IS», модель «TO-BE», идентификация, аутентификация, биометрические признаки.

DEVELOPMENT OF A FUNCTIONAL MODEL OF THE EMPLOYEE AUTHENTICATION PROCESS AT THE CHECKPOINT

S.A. Evdokimova, E.O. Zalukaev

Voronezh State University of Engineering Technologies

The article describes the developed functional model in the IDEF0 notation of the employee authentication process at the checkpoint, based on the analysis of which the shortcomings of paper passes are noted. To increase the level of information security and throughput, an improved model of the employee authentication process based on facial biometrics is proposed.

Keywords: IDEF0 methodology, «AS-IS» model, «TO-BE» model, identification, authentication, biometric features.

Процесс аутентификации сотрудника на контрольно-пропускном пункте (КПП) является ключевым элементом системы безопасности предприятия. Для обеспечения эффективной и надежной защиты объектов необходимо четко

проанализировать существующий процесс аутентификации, построив функциональную модель «Как есть» (AS-IS), и предложить оптимальное решение с использованием биометрической аутентификации в модели «Как должно быть» (TO-BE) [1-8].

Рассматриваемая компания занимается разработкой и внедрением инновационных технологических решений автоматизации бизнес-процессов, технической поддержкой интернет-ресурсов, разработкой и сопровождением программного обеспечения для различных организаций.

Проведенный анализ существующего процесса аутентификации сотрудников на КПП описан с помощью функциональных диаграмм в нотации IDEF0 (рисунки 1, 2) [1-8].

На рисунке 1 показана контекстная диаграмма процесса аутентификации сотрудника на КПП, которая представляет собой общую структуру существующего процесса аутентификации по пропуску.

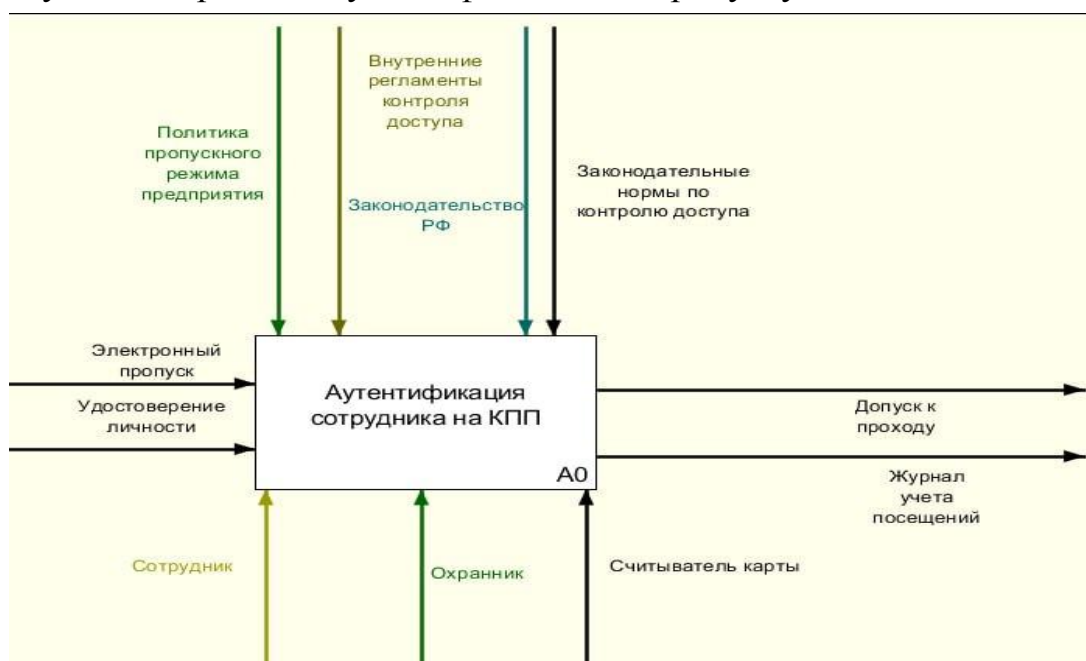


Рисунок 1 – Контекстная диаграмма «AS-IS» Аутентификация сотрудника на КПП

Входными данными контекстной диаграммы являются:

- электронный пропуск – предоставляет информацию о праве доступа сотрудника;
- удостоверение личности - используется для подтверждения личности сотрудника, если отсутствует пропуск.

К механизмам процесса относятся:

- сотрудник – физическое присутствие человека, требующего доступа;
- охранник – человек, осуществляющий охрану объекта, проверку документов и принятие решения о допуске;
- считыватель карты – выполняет чтение данных с электронного пропуска.

Выходными данными являются:

- допуск к проходу – разрешение на вход/выход сотрудника на территорию предприятия;
- журнал учета посещений – запись информации о времени и событии прохождения сотрудниками и посетителями КПП.

К стрелкам управления относятся:

- законодательство РФ;
- политика пропускного режима предприятия;
- законодательные нормы по контролю доступа;
- внутренние регламенты контроля доступа.

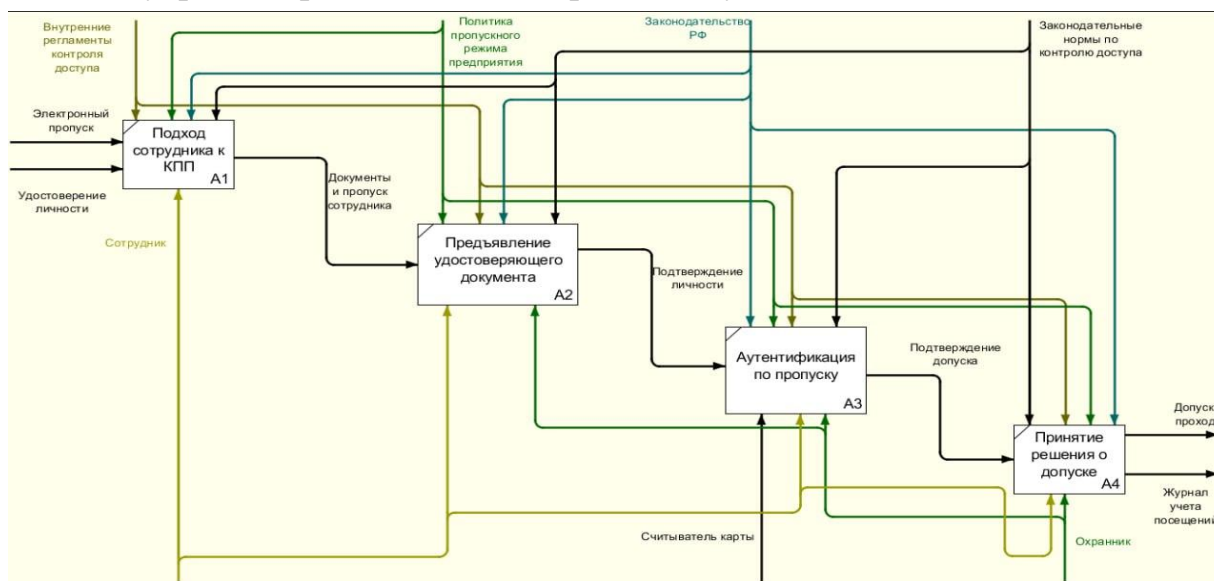


Рисунок 2 – Диаграмма декомпозиции процесса «AS-IS» Аутентификация сотрудника на КПП

На диаграмме декомпозиции (рисунок 2) выделены следующие подпроцессы:

- A1 Подход сотрудника к КПП – сотрудник подошел к контрольному пункту;
- A2 Предъявление удостоверяющего документа – сотрудник предоставил электронный пропуск или удостоверение личности;

- А3 Аутентификация по пропуску – охранник сверяет предоставленные документы с внутренними регламентами и политикой пропускного режима;

- А4 Принятие решения о допуске – на основе результатов проверки охранник принимает решение о разрешении или отказе в доступе.

Текущий процесс аутентификации на КПП основан на ручной проверке документов сотрудниками охраны. Этот подход имеет высокую зависимость от человеческого фактора, что может привести к ошибкам и несанкционированному доступу. Низкая скорость обработки запросов, особенно при высокой интенсивности потока сотрудников, также является недостатком существующего процесса.

Программно-аппаратные средства контроля доступа, основанные на распознавании лиц, все больше внедряются на предприятиях и становятся ключевым элементом современной инфраструктуры безопасности. Биометрические решения опираются на уникальные черты внешности, и такой подход практически исключает возможность передачи доступа посторонним лицам. Камеры, интегрированные в турникеты или входные группы, позволяют мгновенно распознавать сотрудников, не требуя от них дополнительных действий.

Поэтому для устранения выявленных недостатков действующего процесса разработана функциональная модель «ТО-ВЕ» процесса аутентификации на основе технологии распознавания лиц (рисунки 3 и 4).

Теперь входными данными модели «ТО-ВЕ» является биометрический параметр Лицо – изображение лица сотрудника, захваченное камерой видеонаблюдения.

К механизмам процесса добавились:

- комплекс автоматической аутентификации – программно-аппаратный комплекс, выполняющий распознавание лиц и сравнение с базой данных;

- хранилище биометрических данных – база данных, содержащая зарегистрированные шаблоны лиц сотрудников;

- считыватель биометрических данных – эта камера, выполняющая захват лиц.

На диаграмме декомпозиции модели «ТО-ВЕ» (рисунок 4) определены следующие подпроцессы:

- А1 Подход сотрудника к КПП – сотрудник приближается к контрольному пункту;

– А2 Считывание биометрического параметра: Лица – комплекс автоматической аутентификации захватывает изображение лица сотрудника и передает его на обработку;

– А3 Принятие решения о допуске: – система сравнивает полученные биометрические данные с хранилищем и выдает решение о разрешении или отказе в доступе.



Рисунок 3 – Контекстная диаграмма «ТО-ВЕ» Аутентификация сотрудника на КПП с использованием биометрии

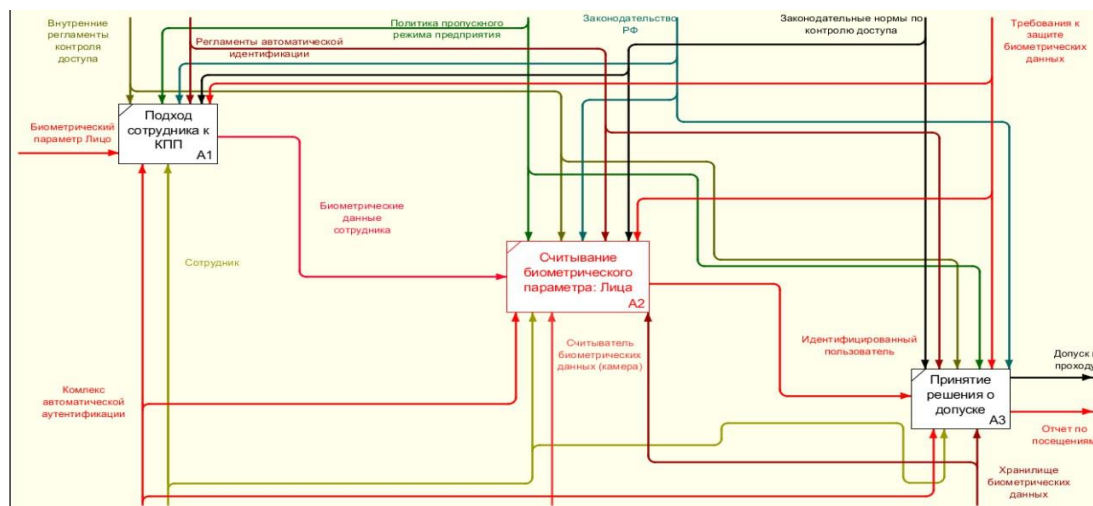


Рисунок 4 – Диаграмма декомпозиции «ТО-ВЕ»

Новый процесс аутентификации на КПП использует современную технологию распознавания лиц, которая значительно повышает безопасность и эффективность контроля доступа. Для реализации модернизированного

процесса идентификации и аутентификации сотрудников база данных контрольно-пропускной системы должна быть заполнена биометрическими данными сотрудников, имеющих право доступа к объекту. Архитектура программного продукта должна быть спроектирована с учетом требований ФЗ-152 «О персональных данных» и других законодательных актов РФ, а также к масштабируемости, отказоустойчивости, безопасности и удобству эксплуатации системы.

Таким образом, внедрение биометрической аутентификации сотрудников на КПП даст следующие преимущества:

- безопасность – защиту от подделки документов и спуффинга;
- повышение производительности – автоматизация процесса снижает время обработки до нескольких секунд;
- масштабируемость – возможность обслуживания большого количества сотрудников без увеличения числа операторов;
- контроль – полный аудит всех событий через журналы и отчеты.

Список литературы

1. Новикова, Т.П. Разработка алгоритма и модели функционирования информационной системы для платного отделения стоматологической поликлиники / Т.П. Новикова, А.А. Бодин, С.А. Евдокимова // Моделирование систем и процессов. – 2021. – Т. 14, № 1. – С. 51-58.

2. Выбор критерия оптимальности при принятии управленческих решений в сложных технических системах / А.В. Скрыпников [и др.] // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 120-128.

3. Новикова, Т.П. Математическая модель интермодальных грузовых перевозок / Т.П. Новикова, С.А. Евдокимова, А.И. Новиков // Моделирование систем и процессов. – 2024. – Т. 17, № 2. – С. 62-70.

4. Высоцкая, И.А. Обоснование информационно-интеллектуальной поддержки принципов действия технических систем / И.А. Высоцкая // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 19-26.

5. Developing a risk management process for infrastructure projects using IDEF0 / H.-P. Tserng, I.-C. Cho C.-H. Chen, Y.-F. Liu // Sustainability (Switzerland). – 2021. – Vol. 13(12). – С. 6958.

6. Новикова, Т.П. Разработка алгоритма и модели функционирования информационной системы для обучения и тестирования операторов СІР-мойки

/ Т.П. Новикова, А.В. Данилов, А.И. Новиков // Моделирование систем и процессов. – 2019. – Т. 12, № 2. – С. 72-78.

7. Сравнение нотаций DFD, IDEF0, IDEF3, EPC и BPMN с нотацией УФО-анализа / О.А. Зимовец, Е.В. Малкуш, С.И. Маторин, Н.И. Корсунов // Экономика. Информатика. – 2024. – Т. 51, № 4. – С. 936-945.

8. Функциональное моделирование формализации тактик реализации вредоносного программного обеспечения / И.И. Корчагин [и др.] / Безопасность информационных технологий. – 2024. – Т. 31, № 4. – С. 87-98.

References

1. Novikova, T.P. Development of an algorithm and a model for the functioning of an information system for a paid department of a dental clinic / T.P. Novikova, A.A. Bodin, S.A. Evdokimova // Modeling of systems and processes. – 2021. – Vol. 14, No. 1. – Pp. 51-58.

2. Selection of the optimality criterion in making managerial decisions in complex technical systems / A.V. Skrypnikov [et al.] // Modeling of systems and processes. – 2024. – Vol. 17, No. 1. – Pp. 120-128.

3. Novikova, T.P. Mathematical model of intermodal freight transportation / T.P. Novikova, S.A. Evdokimova, A.I. Novikov // Modeling of systems and processes. – 2024. – Vol. 17, No. 2. – Pp. 62-70.

4. Vysotskaya, I.A. Substantiation of information and intellectual support for the principles of operation of technical systems / I.A. Vysotskaya // Modeling of systems and processes. – 2024. – Vol. 17, No. 1. – Pp. 19-26.

5. Developing a risk management process for infrastructure projects using IDEF0 / H.-P. Tserng, I.-C. Cho C.-H. Chen, Y.-F. Liu // Sustainability (Switzerland). – 2021. – Vol. 13(12). – C. 6958.

6. Novikova, T.P. Development of an algorithm and a model for the functioning of an information system for training and testing CIP-washing operators / T.P. Novikova, A.V. Danilov, A.I. Novikov // Modeling of systems and processes. – 2019. – Vol. 12, No. 2. – Pp. 72-78.

7. Comparison of notations DFD, IDEF0, IDEF3, EPC and BPMN with UFO analysis notation / O.A. Zimovets, E.V. Malkush, S.I. Matorin, N.I. Korsunov // Economy. Computer science. – 2024. – Vol. 51, No. 4. – Pp. 936-945.

8. Functional modeling of the formalization of tactics for the implementation of time-bearing software / I.I. Korchagin [et al.] / Information technology security. – 2024. – Vol. 31. No. 4. – Pp. 87-98.