Автоматизация и моделирование в проектировании и управлении. 2023. № 3 (21). С. 13-22.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2023. № 3 (21). P. 13-22.

Научная статья
Статья в открытом доступе
УДК 004.056.57
doi: 10.30987/2658-6436-2023-3-13-22

ПРОЕКТИРОВАНИЕ ВСПОМОГАТЕЛЬНОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ НА ОСНОВЕ АНАЛИЗА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наталия Михайловна Кузнецова[1], Татьяна Владимировна Карлова[2], Александр Юрьевич Бекмешов[3]
[1] Московский государственный технологический университет «СТАНКИН», г. Москва, Россия
[2, 3] Институт конструкторско-технологической информатики Российской академии наук, г. Москва, Россия
[1] knm87@mail.ru
[2] karlova-t@yandex.ru
[3] b-a-y-555@yandex.ru

Аннотация. *Целью научной работы является создание методики проектирования вспомогательной автоматизированной системы принятия управленческих решений на основе анализа уровня информационной безопасности интеллектуальных ресурсов крупного промышленного предприятия. Основу методики составляет принцип комплексности обеспечения информационной безопасности. Статья посвящена решению задачи создания удобного вспомогательного инструмента для проведения аудита событий информационной безопасности. Новизной работы является предложенная креативная концепция использования максимального объема данных о событиях информационной безопасности для принятия управленческого решения (в том числе кадрового управленческого решения). Результатом исследования являются рекомендации по созданию вспомогательной автоматизированной системы аудита и анализа уровня информационной безопасности интеллектуальных ресурсов крупного промышленного предприятия.*

Ключевые слова: автоматизация, управленческое решение, защита информации, аудит информационной безопасности, интеллектуальные ресурсы, информационная безопасность

Для цитирования: Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Проектирование вспомогательной автоматизированной системы принятия управленческих решений на основе анализа уровня информационной безопасности // Автоматизация и моделирование в проектировании и управлении. 2023. №3 (21). С. 13-22. doi: 10.30987/2658-6436-2023-3-13-22.

Original article
Open Access Article

DESIGNING AN AUXILIARY AUTOMATED MANAGEMENT DECISION MAKING SYSTEM BASED ON INFORMATION SECURITY LEVEL ANALYSIS

Natalia M. Kuznetsova[1], Tatyana V. Karlova[2], Alexander Yu. Bekmeshov[3]
[1] Moscow State University of Technology «STANKIN», Moscow, Russia
[2, 3] Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia
[1] knm87@mail.ru
[2] karlova-t@yandex.ru
[3] b-a-y-555@yandex.ru

Abstract. *The aim of the scientific work is to create a methodology for designing an auxiliary automated management decision making system based on analysing information security level of intellectual resources of a large industrial enterprise. The methodology is based on the principle of comprehensive information security. The article is devoted to solving the problem of creating a convenient auxiliary tool for auditing information security events. The novelty*

of the work is the proposed creative concept of using the maximum amount of data on information security events to make a management decision (including a personnel management decision). The study results are recommendations for building an auxiliary automated system for auditing and analysing the information security level of intellectual resources of a large industrial enterprise.

Keywords: automation, management decision, information protection, information security audit, intellectual resources, information security

For citation: Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Designing an Auxiliary Automated Management Decision Making System Based on Information Security Level Analysis. Automation and modeling in design and management, 2023, no. 3 (21). pp. 13-22. doi: 10.30987/2658-6436-2023-3-13-22.

Введение

Аудит событий информационной безопасности является важным этапом обеспечения защиты стратегически важных ресурсов промышленного предприятия, в том числе интеллектуальных ресурсов. Для отдела безопасности и руководства предприятия крайне важно своевременное выявление причины понижения уровня защиты ресурсов. Автоматически собранные данные о событиях информационной безопасности позволят своевременно выявить источники инцидентов и угроз, а также принять управленческие решения по их устранению (в том числе кадровые управленческие решения). Проектирование автоматизированной системы аудита и анализа событий информационной безопасности должно осуществляться с учетом требований обеспечения структурированности, актуальности, целостности, доступности и конфиденциальности обрабатываемой в системе информации.

Исследование возможных причин инцидентов информационной безопасности

Причины инцидентов информационной безопасности (ИИБ) промышленного предприятия можно разделить на группы:

– неисправность программного и аппаратного обеспечения (ПАО) основных автоматизированных систем (АС);

– ошибки проектирования основных АС;

– непреднамеренные ошибки работников предприятия (добросовестное заблуждение, усталость, болезнь и т.д.);

– преднамеренные действия работников предприятия (в данном случае работники являются внутренними нарушителями);

– преднамеренные действия лиц, которые не являются работниками предприятия (являются внешними нарушителями).

В рамках создания методики проектирования вспомогательной автоматизированной системы аудита и анализа инцидентов информационной безопасности (ВАСААИИБ) в качестве возможных причин ИИБ рассматривались: неисправности ПАО; непреднамеренные ошибки работников; преднамеренные действия работников предприятия.

Исследование потребности в автоматизированной системе аудита и анализа инцидентов информационной безопасности

Как аудит, так и анализ ИИБ являются важными функциональными элементами комплексного обеспечения защиты стратегически важных ресурсов промышленного предприятия [1, 2].

В связи с тем, что в рамках анализа ИИБ приходится обрабатывать большие объемы данных, необходимо создание вспомогательного инструмента (ВАСААИИБ), позволяющего обрабатывать данные об ИИБ, предоставлять результаты интеллектуального анализа заинтересованным лицам, а также обеспечивать хранение данных об ИИБ.

Анализом ИИБ занимаются работники отдела информационной безопасности (ОИБ). Однако предоставление данных анализа необходимо также лицам, принимающим управленческие решения – руководству предприятия и руководству структурных

подразделений.

Таким образом, данные анализа ИИБ должны быть предоставлены следующим заинтересованным лицам: работникам ОИБ; руководству структурных подразделений предприятия; руководству предприятия.

Аудит ИИБ позволит решить задачу структурированного хранения данных об ИИБ.

Анализ входных данных автоматизированной системы аудита и анализа инцидентов информационной безопасности

В качестве входных данных ВАСААИИБ необходимо рассматривать:

– данные функционирования локальной вычислительной сети (ЛВС);

– журналы аудита использования ПАО;

– данные о работнике из отдела кадров (ОК):

а) дата зачисления в штат;

б) данные о предыдущих местах работы;

в) образование;

– данные, собранные средствами видеонаблюдения:

а) местонахождение;

б) физиогномика;

в) походка;

г) голос;

– другие динамические биометрические характеристики работников предприятия:

а) клавиатурный почерк;

б) скорость печатания;

в) количество обращений к документам, обновлений версий создаваемого программного обеспечения (ПО);

– данные о телекоммуникации работников (данные, собранные исключительно со служебных аппаратов и на территории предприятия).

Архитектура автоматизированной системы аудита и анализа инцидентов информационной безопасности

При проектировании ВАСААИИБ необходимо учитывать все требования, предъявляемые к обработке и хранению информации:

– для принятия рационального и своевременного управленческого решения информация о ИИБ, предоставляемая ВАСААИИБ, должна быть актуальной;

– для четкого определения локализации и временных характеристик ИИБ предоставляемые ВАСААИИБ данные должны быть структурированы и целостны. Также информация должна быть предъявлена работникам ОИБ и руководству в удобном и понятном виде (посредством интуитивно понятного интерфейса (ИПИ));

– данные о текущих ИИБ, а также о ранее зарегистрированных ИИБ должны быть доступны заинтересованным лицам;

– обеспечение конфиденциальности данных крайне важно как для корректности проведения анализа ИИБ, так и для уменьшения репутационных рисков предприятия.

На рис. 1 представлена архитектура проектируемой ВАСААИИБ.

Согласно рис. 1, ВАСААИИБ включает модули: сбора данных об ИИБ; анализа данных для принятия управленческих решений (УР); хранения данных – БД ИИБ; сравнения с историей ИИБ; принятия УР; предоставления вариантов УР.

Данные из модуля сбора передаются в модуль анализа. Модуль анализа данных, в свою очередь, передает обработанную информацию в модуль принятия УР и в БД ИИБ.

Модуль сравнения текущего ИИБ с историей ИИБ определяет степень схожести инцидента с характеристиками происшедших ранее ИИБ.

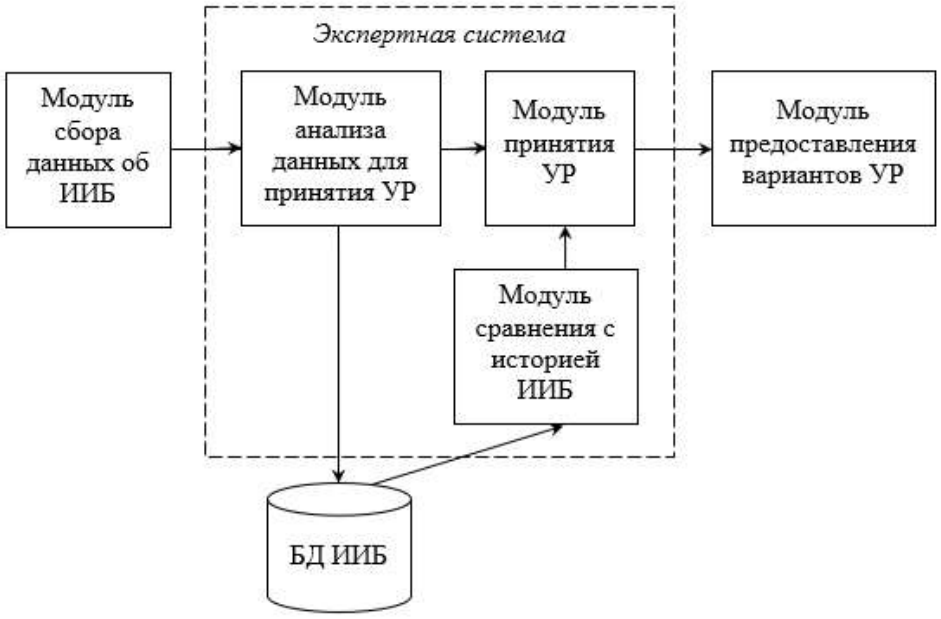

Рис. 1. Архитектура проектируемой ВАСАИИБ

Fig. 1. Topology of synthesized auxiliary automated information security incident audit and analysis systems

Модуль принятия УР на основе данных, поступивших от модуля анализа о текущем ИИБ, и информации от модуля сравнения с историей ИИБ, формирует варианты УР и передает их в модуль предоставления.

Модуль предоставления вариантов УР передает альтернативы УР пользователям ВАСАИИБ (работникам ОИБ и руководству) посредством ИПИ.

Модуль сбора данных об инцидентах информационной безопасности. Модуль сбора данных обеспечивает корректное формирование целостной и иерархической структуры данных об ИИБ, агрегируя информацию, поступившей от: системы видеонаблюдения за работниками предприятия; журнала аудита использования ПАО; ОК (информация о работниках); датчиков контроля состояния ЛВС; использовании служебных телекоммуникационных устройств.

Центральными узлами формируемой иерархической структуры данных об ИИБ являются работники предприятия. На рис. 2 представлен алгоритм формирования структурированных данных об ИИБ.

Согласно рис. 2, в случае если при мониторинге ЛВС обнаруживается сбой или «подозрительное» состояние, производится одновременное обращение к системе видеонаблюдения и системе мониторинга журнала аудита использования ПАО основной АС предприятия.

При обработке видео-контента особое внимание уделяется физическим объектам (помещениям), где находится «подозрительный» участок ЛВС. Основной задачей сбора информации от системы видеонаблюдения на данном этапе является идентификация работников, находящихся в данных помещениях во время и до ИИБ.

Аналогично обрабатывается информация мониторинга журнала аудита использования ПАО – тщательно анализируется использование ПАО, которое может быть задействовано во время ИИБ.

Важно отметить, что первоисточником тревоги может являться не только срабатывание системы мониторинга ЛВС (см. рис. 2), но и система видеонаблюдения, а также система мониторинга журнала аудита. При этом аналогично запускается «цепная реакция» срабатывания оставшихся систем.

Например, система видеонаблюдения обнаружила подозрительную активность работника (попытку входа на несоответствующую допуску территорию предприятия, продолжительное нахождение не на своем рабочем месте и т.д.). Автоматически срабатывают проверки системы мониторинга ЛВС и журнала аудита использования ПАО работниками на данном участке.

Рис. 2. Алгоритм формирования структурированных данных об ИИБ
Fig. 2. Algorithm for generating structured data on information security incidents

Согласно рис. 3, взаимодействие системы мониторинга ЛВС, системы мониторинга журнала аудита использования ПАО основной АС предприятия и системы наблюдения на этапе предварительного сбора данных об ИИБ является равноправным.

Далее производится формирование списка работников, причастных к ИИБ. На основании данного списка одновременно: формируется запрос данных о работниках в ОК; производится сбор данных о физиогномике и динамических биометрических характеристиках работников до и во время ИИБ; производится сбор данных о производимой телекоммуникации работников.

Данные о физиогномике и динамических биометрических характеристиках работников поступают от системы видеонаблюдения. Таким образом, ресурсы системы видеонаблюдения используются на двух этапах алгоритма работы модуля сбора данных об ИИБ (см. рис. 2).

В качестве данных физиогномики рассматриваются динамические характеристики лица работника (мимика), отражающие его психоэмоциональное состояние [3].

Важно отметить, что сбор динамических биометрических характеристик может быть осуществлен не только системой видеонаблюдения, но и системой биометрической аутентификации. Важно, чтобы данные системы не вступали в конкурентное противоречие.

Рис. 3. Взаимодействие системы мониторинга ЛВС, системы мониторинга журнала аудита использования ПАО основной АС предприятия и системы наблюдения на этапе предварительного сбора данных об ИИБ

Fig. 3. Interaction of local area network monitoring system, audit log monitoring system using the software and hardware of the enterprise's main automated system and surveillance system during the preliminary collection of information security incident data

Контроль телекоммуникации осуществляется для определения фактов нарушений (доказательства противоправных действий) работников: организации утечки данных, сговора работников и т.д.

На этапе формирования данных об ИИБ создается иерархическая информационная структура, корневыми узлами которой являются работники предприятия, причастные к ИИБ.

Иерархическая структура может быть представлена в виде графа: дерева (в случае одного работника, причастного к ИИБ); леса – совокупности деревьев (в случае нескольких работников, причастных к ИИБ).

Пример иерархической структуры данных об ИИБ в виде дерева представлен на рис. 4.

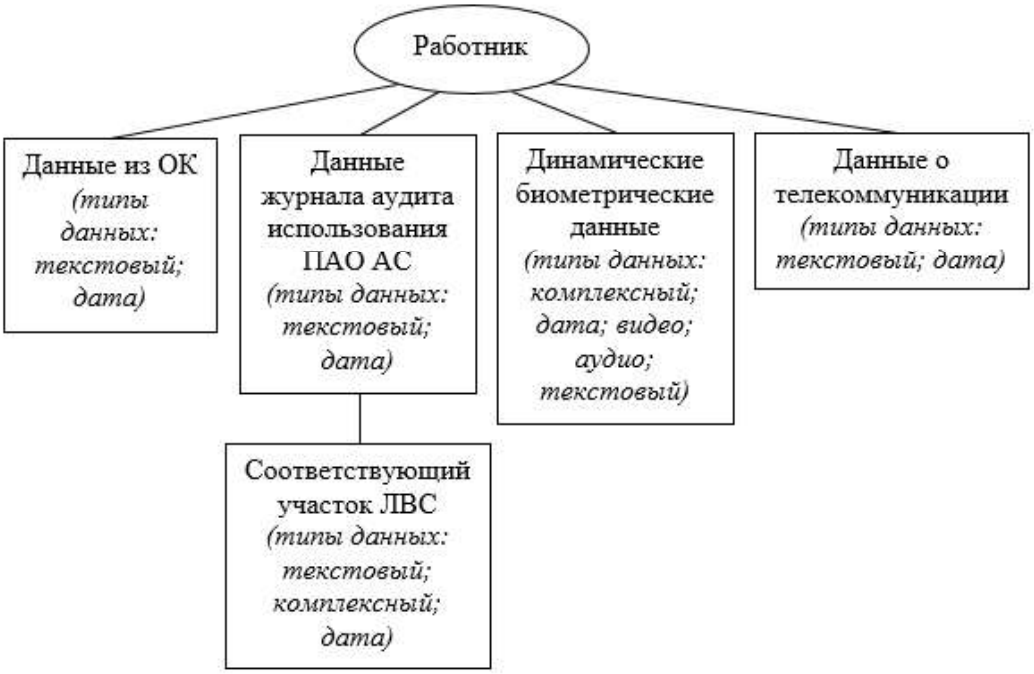

Рис. 4. Пример иерархической структуры данных об ИИБ

Fig. 4. Example of hierarchical structure of information security incident data

Модуль анализа данных для принятия управленческих решений. Для принятия рационального оптимального УР (в том числе кадрового) в вопросах обеспечения информационной

безопасности стратегически важных ресурсов предприятия необходимо точное определение уровня опасности. Для его определения необходимо введение понятия приоритета сохранения ресурсов.

Наивысшим приоритетом, безусловно, является жизнь и здоровье работников предприятия.

Далее необходимо оценить приоритет сохранения параметров информационной безопасности для каждого вида ресурса предприятия (инфраструктурных, интеллектуальных, информационных ресурсов и т.д.).

При этом интеллектуальные ресурсы обладают большим приоритетом и уровнем стратегической важности по сравнению с информационными, программно-аппаратными ресурсами.

Для формирования УР также важна оценка рисков понижения уровня информационной безопасности. Общий риск может быть рассчитан по формуле (1), исходя из коэффициентов уязвимости ресурсов и вероятности реализации угрозы.

$$R = \sum_{i=1}^{N} V_i \cdot Pt_i, \quad (1)$$

где V_i – коэффициент уязвимости ресурса i; Pt_i – вероятность реализации угрозы для ресурса i.

Именно вероятности реализации Pt_i угрозы могут быть оценены с помощью графа данных об ИИБ.

Для точного подсчета вероятности реализации угрозы необходимо введение характеристик данных об ИИБ – вес.

Вес данных об ИИБ (вероятность реализации угрозы) рассчитывается как:

$$W_i = Ps_i \cdot Pt_i, \quad (2)$$

где Ps_i – приоритет сохранения ресурса i; Pt_i – вероятность реализации угрозы для ресурса i.

Структура данных об ИИБ позволяет оценить общую вероятность реализации угрозы, а также вероятности реализации угроз для каждого из задействованных в ИИБ ресурсов.

Таким образом, для принятия рационального оптимального УР, необходимо учитывать: приоритет сохранения ресурсов; коэффициент уязвимости ресурсов; вероятность понижения уровня информационной безопасности (вероятность реализации угрозы).

Корневыми узлами структуры данных об ИИБ являются работники предприятия, в связи с чем важно также учитывать, чтобы предоставляемая модулем информация была доступна и понятна привлеченным экспертам – психиатрам.

Модуль хранения данных об инцидентах информационной безопасности. При хранении структурированных данных об ИИБ важно обеспечение основных параметров безопасности:

– конфиденциальности – доступ к структурированным данным об ИИБ должен предоставляться исключительно работникам ОИБ и руководству;

– целостности – сформированная в модуле анализа структура данных об ИИБ должна быть сохранена;

– доступность – работникам ОИБ и руководству должен быть предоставлен доступ к любой записи об ИИБ за запрашиваемый период.

Кроме того, необходимо обеспечение высокой скорости предоставления запрашиваемой информации об ИИБ.

В связи с данными требованиями необходимо, чтобы БД ИИБ была организована таким образом, чтобы:

– данные об ИИБ хранились распределенно (в том числе на нескольких физических серверах);

– данные были зашифрованы;

– скорость сбора данных о запрашиваемых ИИБ была минимальна.

На рис. 5 представлена структура БД ИИБ.

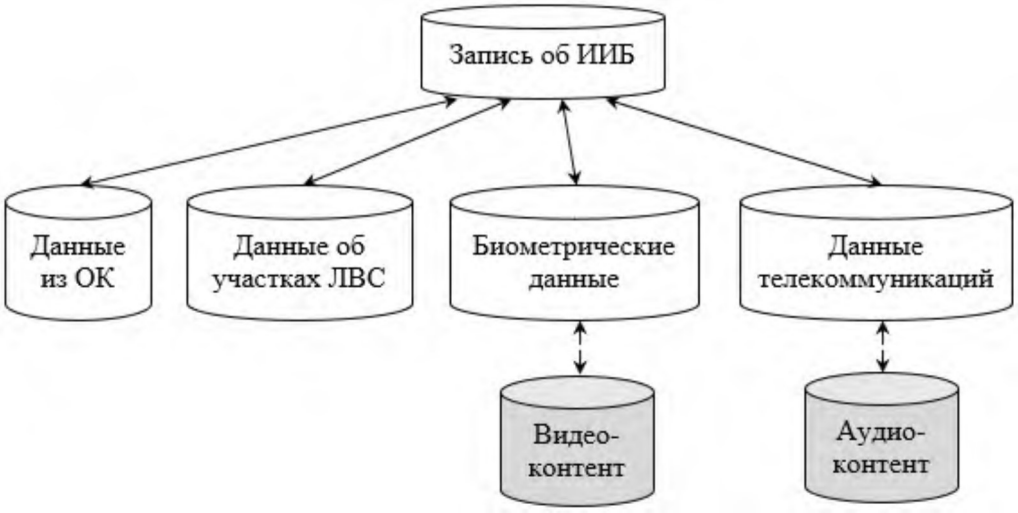

Рис. 5. Структура БД ИИБ
Fig. 5. Structure of information security incident database

Данные из ОК являются текстовыми, об участках ЛВС – комплексными, метаданные об динамических биометрических характеристиках и телекоммуникациях – текстовыми, в связи с чем они не являются «тяжеловесными» (в отличие от видео и аудио-контента). Таким образом, скорость сборки будет минимальна.

Важно отметить, что видео и аудио-контент также хранится в записи об ИИБ, но предоставляется по дополнительному запросу. Для первоначального запроса истории ИИБ достаточно метаданных о видео и аудио-контенте, но не сам контент.

Модуль сравнения инцидента информационной безопасности с историей инцидентов. Данный модуль может работать в двух режимах: вызов функций модуля работником ОИБ или руководителем для сравнения текущего ИИБ с предыдущими; фоновый режим работы сравнений и анализа свершившихся ИИБ (из БД ИИБ).

Главными функциями модуля являются: нахождение сходств ИИБ; выявление стратегии злоумышленника; поиск (вычисление) злоумышленника. Перечисленные функции выполняются последовательно.

Однако помимо выполнения главных функций модуль сравнения ИИБ может выявлять атаки «нулевого дня» – новые виды атак, с которыми еще не сталкивалась система защиты.

Кроме того, данный модуль позволяет оценивать динамику изменений (в том числе долгосрочную) психоэмоционального состояния работников. Психоэмоциональное состояние работников можно отнести к понятию человеческого фактора.

Согласно исследованиям, показатель значимости человеческого фактора при авариях составляет: военная авиация – 0,85; промышленное строительство – 0,70; ядерная энергетика – 0,55; технологическое оборудование – 0,40 [4, 5].

В работах [5 – 9] в качестве основных причин техногенных аварий приведены: сонливость – 10 %; стресс – 20 %; усталость – 20 %; алкогольное опьянение – 40 %.

Таким образом, вовремя обнаруженное изменение в психоэмоциональном состоянии работника позволит снизить риск возникновения техногенных аварий, а также предупредить их.

Модуль принятия управленческого решения. Входными данными для модуля являются:

– структурированная информация о текущем ИИБ (от модуля анализа данных об ИИБ);

– данные сравнения текущего ИИБ с предыдущими (от модуля сравнения ИИБ);

– данные анализа свершившихся ИИБ (от модуля сравнения ИИБ).

Выходными данными модуля являются несколько ветвей УР. При этом в каждую ветвь входит:

– информация о границах ответственности за ИИБ – определение лиц, причастных к ИИБ и мер их ответственности;

– список принимаемых мер (последовательности действий) по предотвращению ИИБ

(локализации, блокировки дальнейшего распространения и т.д.);

– список принимаемых мер (последовательности действий) по устранению последствий ИИБ;

– общая стоимость реализации рекомендуемых принимаемых решений по устранению ИИБ;

– определение репутационных рисков предприятия.

Для определения перечисленных параметров в модуле может быть использован механизм искусственного интеллекта (применены нейронные сети).

Модуль визуализации. К основным задачам модуля визуализации относятся:

– предоставление удобного интуитивно-понятного человеко-машинного интерфейса;

– предоставление возможности масштабирования пространства ИИБ от составных частей основных АС предприятия до отдельного ПАО АС.

Проектируемая система является вспомогательной для принятия УР. Ответственность за принятие УР возлагается на человека (работника ОИБ, руководителя).

Заключение

В связи с многообразием и объемом информации, необходимой для принятия управленческих решений при защите ресурсов промышленного предприятия, необходимо создание вспомогательных автоматизированных систем. Кроме того, при анализе инцидентов информационной безопасности большое влияние может оказать «человеческий фактор»: от невнимательности, ведущей к упущению важных деталей, до умышленного укрывания виновников.

В статье представлена методика создания вспомогательной автоматизированной системы анализа инцидентов информационной безопасности, представлены модульная архитектура, алгоритм обработки и способ хранения данных об инцидентах информационной безопасности.

Применение представленной вспомогательной системы принятия решения позволит рационализировать работу отдела информационной безопасности и руководства предприятия, а также позволит снизить риск возникновения антропогенных аварийных ситуаций.

Список источников:

1. Кузнецова Н.М., Карлова Т.В. Основные принципы защиты автоматизированных систем крупных промышленных предприятий от комплексных кибер-атак Научно-технический журнал «Вестник Брянского государственного технического университета». 2017. №4 (57). с. 84-89.
2. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Построение модульной структуры автоматизированной системы комплексного обеспечения защиты стратегически важных ресурсов предприятия транспорта Вестник Брянского государственного технического университета. 2021. № 9 (106). С. 36–42.
3. Экман П. Психология эмоций. 2-е изд. / Пер. с англ. – СПб.: Питер. 2010. 334 с.
4. Lez'er V., Muratov I., Korpusova N., Issues of transport security and human factors. E3S Web Conf., 2019. Vol. 91. P. 08062.
5. Жумажанова С.С., Сулавко А.Е., Лукин Д.В. Анализ термограмм лица и шеи для распознавания состояния сонливости пользователей на основе классификатора Байеса / Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас». №2 (129). 2020. 76 с.

References:

1. Kuznetsova N.M., Karlova T.V. Basic Principles for Large Enterprise Automated System Protection Against Cyber Attacks. Bulletin of Bryansk State Technical University. 2017;4(57):84-89.
2. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Construction of a Modular Structure of an Automated System for Integrating Support for the Protection of Strategically Important Resources of a Transport Enterprise. Bulletin of Bryansk State Technical University. 2021;9(106):36-42.
3. Ekman P. Emotions Revealed. 2nd ed. Saint Petersburg: Peter; 2010.
4. Lez'er V, Muratov I, Korpusova N. Issues of Transport Security and Human Factors. In: Proceedings of E3S Web Conference; 2019;91. p. 08062.
5. Zhumazhanova S.S., Sulavko A.E., Lukin D.V. Analysis of Face and Neck Thermograms for Users' Drowsiness Recognition Based on the Bayesian Classifier. Information Security Questions. 2020;2(129):76.

6. Prevalence of Drowsy Driving Crashes Estimates from a Large-Scale Naturalistic Driving Study // AAA Foundation. 2018 [Электронный ресурс]. URL: https://aafoundation.org/prevalence-drowsy-driving-crashes-estimates-large-scale-naturalistic-driving-study (дата обращения: 07.09.2022).

7. The Effects of a Heavy Workload on Employees [Электронный ресурс]. URL: https://bizfluent.com/indo-8178431-effects-heavy-workload-employees.html (дата обращения: 07.09.2022).

8. Drive fatigue and road accidents – RoSPA [Электронный ресурс]. URL: https://www.rospa.com/road-safety/advice/drivers/fatigue/road-accidents (дата обращения: 07.09.2022).

9. Driving Drunk of High Puts Everione in Danger [Электронный ресурс]. URL: https://www.nhtsa.gov/drunk-driving/drive-sober-or-get-pulled-over (дата обращения: 07.09.2022).

6. Prevalence of Drowsy Driving Crashes Estimates from a Large-Scale Naturalistic Driving Study. AAA Foundation [Internet]. 2018 [cited 2022 Sep 07]. Available from: https://aafoundation.org/prevalence-drowsy-driving-crashes-estimates-large-scale-naturalistic-driving-study.

7. The Effects of a Heavy Workload on Employees [Internet] [cited 2022 Sep 07]. Available from: https://bizfluent.com/indo-8178431-effects-heavy-workload-employees.html.

8. Drive Fatigue and Road Accidents – RoSPA [Internet] [cited 2022 Sep 07]. Available from: https://www.rospa.com/road-safety/advice/drivers/fatigue/road-accidents.

9. Driving Drunk of High Puts Everyone in Danger [Internet] [cited 2022 Sep 07]. Available from: https://www.nhtsa.gov/drunk-driving/drive-sober-or-get-pulled-over.

Информация об авторах:

Кузнецова Наталия Михайловна
кандидат технических наук, доцент Московского государственного технологического университета «СТАНКИН»

Карлова Татьяна Владимировна
доктор социологических наук, кандидат технических наук, профессор Института конструкторско-технологической информатики Российской академии наук

Бекмешов Александр Юрьевич
кандидат технических наук, доцент Института конструкторско-технологической информатики Российской академии наук

Information about the authors:

Kuznetsova Natalia Mikhailovna
Candidate of Technical Sciences, Associate Professor of Moscow State University of Technology «STANKIN»

Karlova Tatyana Vladimirovna
Doctor of Sociology, Candidate of Technical Sciences, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Bekmeshov Alexander Yurievich
Candidate of Technical Sciences, Associate Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 05.05.2023; одобрена после рецензирования 07.06.2023; принята к публикации 14.06.2023.

The article was submitted 05.05.2023; approved after reviewing 07.06.2023; accepted for publication 14.06.2023.

Рецензент – Пугачев А.А., доктор технических наук, доцент, Брянский государственный технический университет.

Reviewer – Pugachev A.A., Doctor of Technical Sciences, Associate Professor, Bryansk State Technical University.