DOI 10.37882/2223-2966.2024.8.18

АДАПТАЦИЯ ЭКСПЕРТНОЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ НЕФТЕСЕРВИСНЫХ ПРЕДПРИЯТИЙ

ADAPTATION OF AN EXPERT INFORMATION AND ANALYTICAL DECISION SUPPORT SYSTEM IN THE FIELD OF INFORMATION SECURITY FOR OILFIELD SERVICE ENTERPRISES

A. Krasnov
I. Chekanov
K. Lyssev

Summary. For manufacturing enterprises with a high degree of automation, existing in highly competitive conditions, there is an urgent issue of ensuring information security in accordance with the requirements of the legislation of the Russian Federation. In particular, the need to identify priority areas and assets to be protected, cost optimization, accumulation and preservation of information, automation of the work of information security specialists. Expert information and analytical decision support systems are used to automate work with the regulatory framework in the field of information security. The article examines the existing problems of information security at oilfield service enterprises, the features, and ways of adapting the developed system to ensure information protection, management and reduction of risks associated with confidential information.

Keywords: management, automation, expert information and analytical system, information security, oilfield service enterprises.

Краснов Андрей Евгеньевич
доктор физико-математических наук, профессор, Российский Государственный Социальный Университет
krasnovmgutu@yandex.net
Чеканов Иван Романович
Аспирант, Российский Государственный Социальный Университет
cartmen98@yandex.ru
Лысцев Константин Сергеевич
Аспирант, Российский Государственный Социальный Университет
Konstantin.Lystsev@bk.ru

Аннотация. Для производственных предприятий с высокой степенью автоматизации, существующих в условиях высокой конкуренции, стоит актуальный вопрос обеспечения информационной безопасности в соответствии с требованиями законодательства Российской Федерации. В частности, необходимость определения приоритетных направлений и активов, подлежащих защите, оптимизация затрат, накопление и сохранение информации, автоматизация работы специалистов защиты информации. Для автоматизации работы с нормативной базой в области информационной безопасности применяются экспертные информационно-аналитические системы поддержки принятия решений. В статье рассматриваются существующие проблемы информационной безопасности на нефтесервисных предприятиях, особенности и способы адаптации разработанной системы для обеспечения защиты информации, управления и снижения рисков, связанных с конфиденциальной информацией.

Ключевые слова: управление, автоматизация, экспертная информационно-аналитическая система, информационная безопасность, нефтесервисные предприятия.

Введение

В условиях высокой конкуренции промышленных предприятий обеспечение информационной безопасности является актуальной задачей, основанной на соблюдении требований законодательства Российской Федерации. Специалисты по защите информации сталкиваются с широким перечнем задач, определяемых спецификой и направлением деятельности организации.

Значимое место в промышленности страны занимают нефтесервисные предприятия. Они осуществляют добычу, переработку и транспортировку нефти и газа. Организации обладают значительным объемом информации относительно важнейших сырьевых и ресурсных показателей, требующих защиты от утечек, несанкционированного доступа и других угроз.

Работа специалистов отдела информационной безопасности (ИБ) требует особой внимательности, ответственного подхода к комплексу проблем, возникающих ввиду различных особенностей технологических процессов и производств, в том числе на нефтесервисных предприятиях.

Для автоматизации процесса поиска и анализа регламентирующих документов специалистами ИБ и поддержки принятия управленческих решений руководством предприятия применяются различные ин-

струменты. Наиболее перспективным и комплексным направлением, согласно проведенным исследованиям [1], [2], является использование экспертных информационно-аналитических систем (ЭИАС).

В связи с этим, целью данной статьи является анализ проблем информационной безопасности на нефтесервисных предприятиях и предложение подхода к адаптации разработанной ЭИАС для предприятий данного профиля.

Для реализации цели сформулированы следующие задачи:

1. Рассмотреть структуру и архитектуру разработанной интеллектуальной системы.
2. Провести анализ деятельности нефтесервисных предприятий, учитывая основные аспекты и особенности их функционирования в контексте информационной безопасности.
3. Определить приоритетные направления работы специалистов ИБ в сфере нефтесервисных предприятий, учитывая их специфику и требования к обеспечению безопасности информационных ресурсов.
4. Выявить особенности инструментов автоматизации работы специалистов ИБ, применяемых на данных предприятиях, анализируя их эффективность, надежность и соответствие требованиям безопасности.
5. Разработать и предложить подходы к адаптации разработанной интеллектуальной системы к деятельности специалистов ИБ на нефтесервисных предприятиях, учитывая специфику сферы и опираясь на современные требования и стандарты в области информационной безопасности.

В ходе исследования применялись методы анализа научных и практических работ в области информационной безопасности, а также подходы системного анализа.

Экспертная информационно-аналитическая система помощи принятия решений в области информационной безопасности

Система создана с целью автоматизации работы с законодательной и нормативной базой в области ИБ и, благодаря обширному функционалу, позволяет сотрудникам организации вести разноплановую работу с документами данной области. В процессе работы система предоставляет руководителю и сотрудникам удобный и эффективный инструмент для поиска и анализа документов, определяющих требования информационной безопасности для принятия решений в возникающих ситуациях.

Кроме того, система включает базу подготовленных экспертных рекомендаций, инструкций, опорных документов и шаблонов в соответствии с решаемой типовой процедурой на предприятии.

ЭИАС использует различные методы и алгоритмы для анализа документов ИБ, включая распознавание запроса пользователя, анализ ключевых слов и фраз и определение соответствия требованиям нормативных актов [3]. Это позволяет существенно сократить время и усилия, требуемые для поиска и анализа документов в области информационной безопасности.

Разработанную систему можно охарактеризовать, как экспертную информационно-аналитическую систему (ЭИАС), т. к. она не ограничена по информационно-аналитическим технологиям, но имеет ограничения по технологиям экспертных систем:

- Не использует механизм объяснения, при выводе применяются продукционные технологии;
- Не использует логику исчислений и высказываний.
- Использует статические данные, вводимые пользователем.

При этом продукции основаны не на формальной цепочке выводов, а на правилах, определяемых экспертами, т. е. скрытой логики их вывода по знанию ситуаций, что дополнительно классифицирует систему, как статическую, поскольку изменений в процессе решения типовых процедур не предполагается.

Разработанная ЭИАС «Фемида» [4] объединяет несколько инструментов в области информационной безопасности:

1. Справочные системы, такие как «КонсультантПлюс», «Гарант» и другие, являются одним из наиболее широко известных и активно применяемых инструментов данного типа [5]. Они позволяют осуществлять точный поиск необходимой информации на основе актуализируемой базы данных и предоставлять широкий набор документов.

2. Перечни документов, например «Справочник законодательства РФ в области информационной безопасности» [6], предоставляющих практическую полноту и актуальность информации. Они помогают ориентироваться в нормативных актах в формате каталогизатора.

3. Карта законодательства в области ИБ, отражающая иерархию законов и нормативных актов, что помогает легко находить связи между ними [7].

Однако, перечисленные инструменты не лишены недостатков [8], и разработанная ЭИАС позволяет комплексно подходить к поиску и решению ситуаций ИБ на предприятиях за счет базы знаний экспертов.

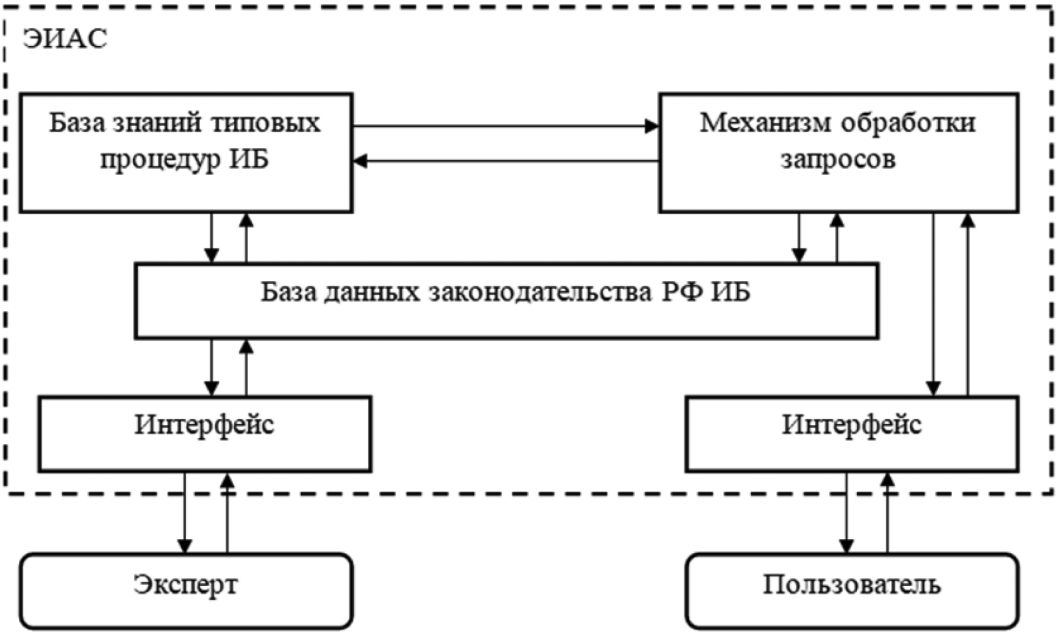

Рис. 1. Схема элементов ЭИАС

Разработанная система имеет ряд структурных компонентов:

1. База данных (БД) (законодательные и нормативные документы РФ);
2. База знаний (экспертные решения);
3. Машина логического вывода [9];
4. Интерфейс системы.

Взаимодействие элементов представлено на схеме (см. рис. 1).

Эксперт и пользователь системы взаимодействуют с элементами системы с помощью интерфейса. Эксперт участвует в подготовке, структуризации и систематизации базы данных и базы знаний ЭИАС.

Структура системы:

Основой структуры экспертной информационно-аналитической системы являются нормативные акты Российской Федерации, которые регулируют информационную безопасность в различных сферах.

1. «Информация»:
1.1. Информация ограниченного доступа;
1.2. Общедоступная информация;
1.3. Информация, доступ к которой не может быть ограничен;
2. «Защита информации»:
2.1. Физическая защита;
2.2. Аппаратная защита;
2.3. Программная защита;
2.4. Организационная защита;
2.5. Психологическая защита;
2.6. Правовая защита;
3. «Аудит»:
3.1. Аттестация аппаратно-программных комплексов;
3.2. Внутренний аудит;
3.3. Внешний аудит;
4. «Контроль»:
4.1. Контроль доступа;
4.2. Контроль сети;
4.3. Контроль политик и процедур;
4.4. Контроль событий;
4.5. Контроль защиты информации;
5. «Управление»:
5.1. Управление рисками;
5.2. Управление программами безопасности;
5.3. Управление ресурсами;
5.4. Управление персоналом;
5.5. Управление инцидентами;
6. «Угрозы»:
6.1. Модель угроз;
6.2. Модель нарушителя;
6.3. Вредоносное программное обеспечение;
6.4. Сетевые атаки.

Структурирование и представление групп позволяет пользователям ориентироваться на обобщенные понятия в области информационной безопасности и находить требуемые документы РФ.

Связь групп и подгрупп реализованной базы данных ЭИАС обусловлена выявленными семантическими отношениями ее документов и представлена следующим образом (см. рис. 2).

1. Группа «Информация» связана с:
- «Защита информации»;

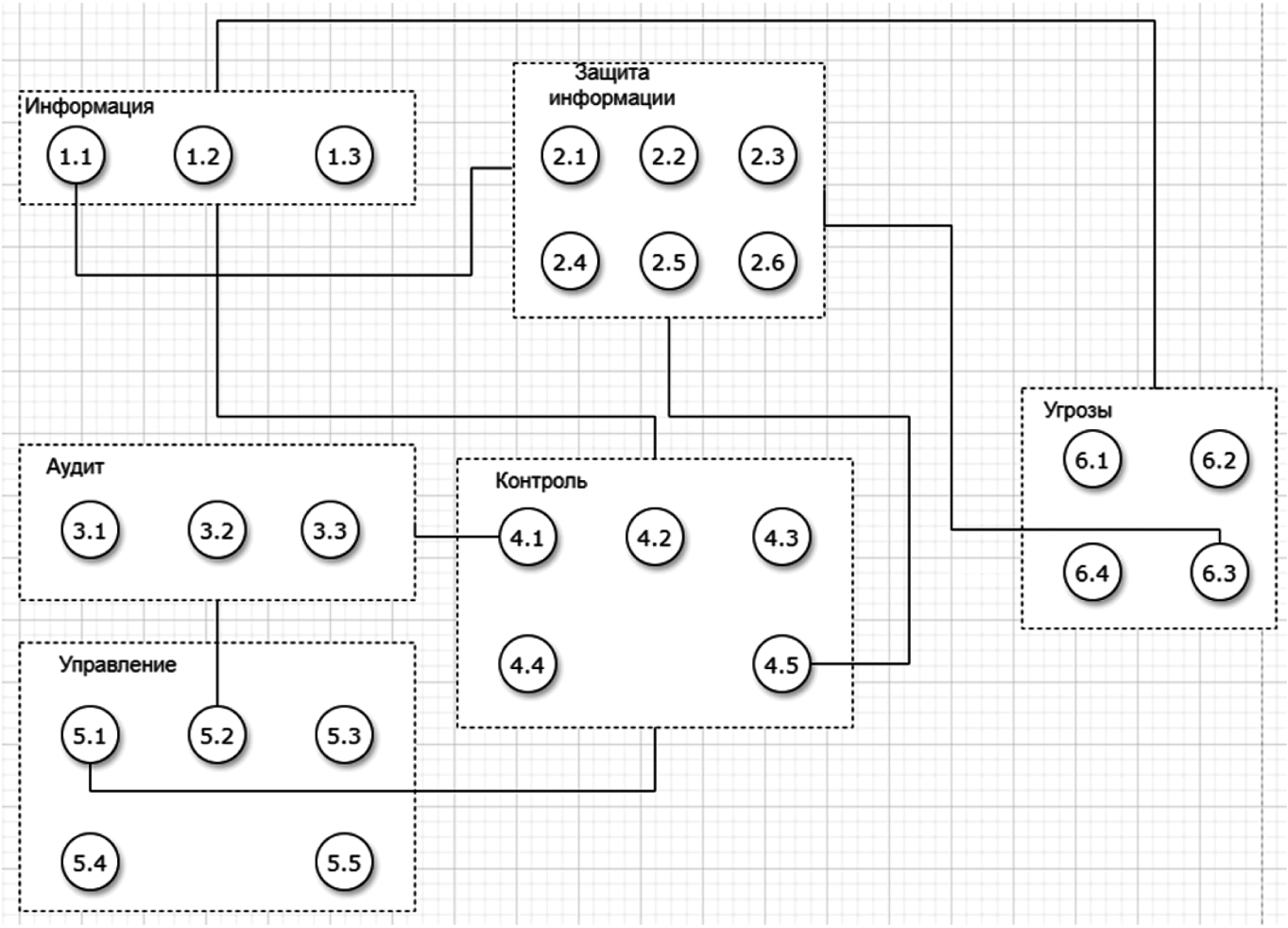

Рис. 2. Структура БД

- «Контроль»;
- «Угрозы».

2. Группа «Защита информации» связана с:
- «Информация» (подблок «Информация ограниченного доступа»);
- «Контроль» (подблок «Контроль защиты информации»);
- «Угрозы» (подблок «Вредоносное программное обеспечение»).

3. Группа «Аудит» связана с:
- «Контроль» (подблок «Контроль доступа»);
- «Управление» (подблок «Управление программами безопасности»).

4. Группа «Контроль» связана с:
- «Защита информации» (подблок «Контроль защиты информации»);
- «Управление» (подблок «Управление рисками»).

5. Группа «Управление» связана с:
- «Контроль» (подблок «Управление рисками»).

6. Группа «Угрозы» связана с:
- «Защита информации» (подблок «Вредоносное программное обеспечение»).

Представленная структура позволяет отразить целостную картину взаимосвязей групп и подгрупп выявленных направлений в области ИБ.

Архитектура ЭИАС

Архитектура экспертной информационно-аналитической системы, основанной на базе данных, представляет собой совокупность реляционных таблиц, взаимосвязанных между собой ключами (см. рис. 3).

В состав схемы входят таблица «Keywords» — с ключевыми словами (семантическими составляющими), «Document_type» — тип нормативно-правового акта. Таблицы «Blocks», «Subblock», «documents_subblocks» описывают представленные структурой БД выделенные группы и подгруппы документов.

Структура ЭИАС может быть изменена и дополнена, в то время как архитектура остается неизменной. Данная особенность позволяет характеризовать ЭИАС инвариантной и применимой в различных областях [10].

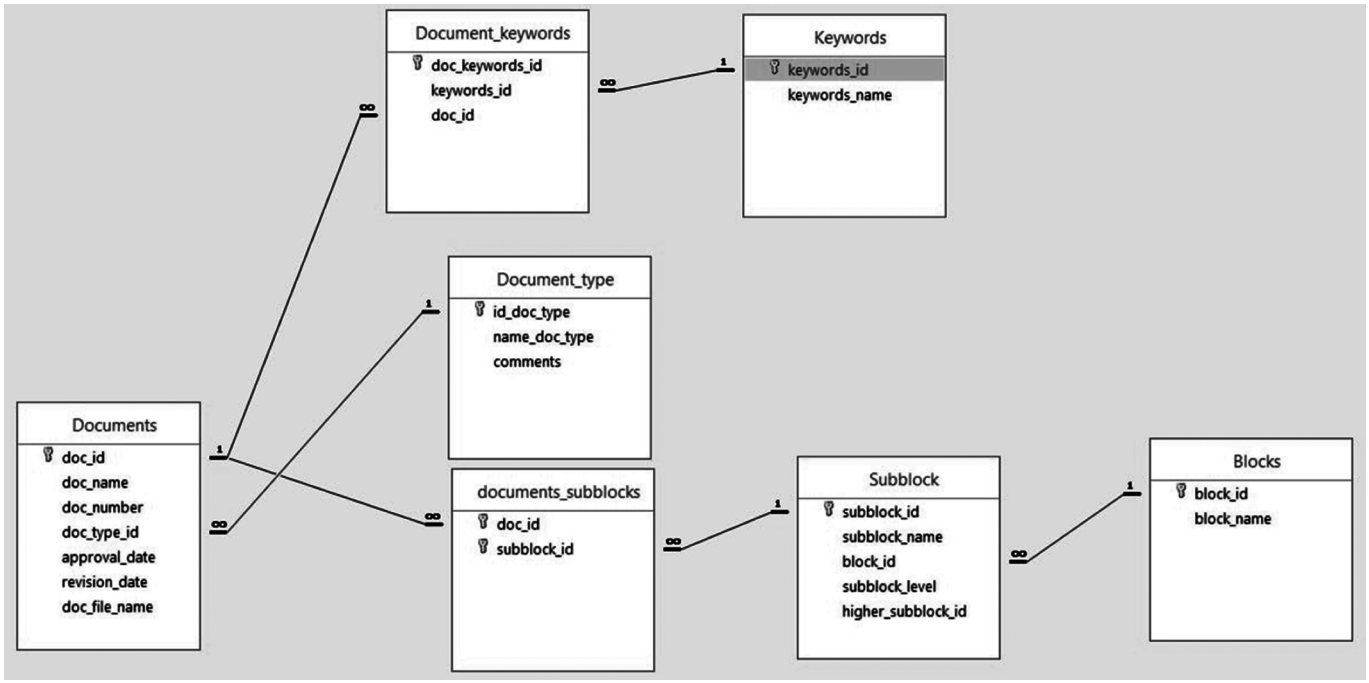

Рис. 3. Архитектура БД ЭИАС

Особенности работы нефтесервисных предприятий

Нефтесервисное предприятие — это компания, которая предоставляет различные услуги и оборудование для добычи, производства и транспортировки нефти и газа. К ним могут относиться бурение и ремонт скважин, строительство и обслуживание нефтяных и газовых месторождений, проведение геофизических исследований, снабжение оборудованием и материалами, техническую поддержку и другие связанные услуги [11]. Нефтесервисные предприятия являются важной составляющей в нефтяной и газовой промышленности, обеспечивая необходимыми ресурсами и экспертизами для эффективной работы данной отрасли.

Нефтегазовый сервис — это средство обеспечения энергетической и экологической безопасности страны. Например, в США и Китае к этому виду работ допущены, в основном, национальные компании. Это обусловлено стратегической значимостью для безопасности страны информации, получаемой с его помощью, о состоянии и перспективах минерально-сырьевых ресурсов государства (результаты геологоразведочных работ, сейсморазведки, бурения, геофизических исследований скважин на суше и море). Сервис обеспечивает необходимый уровень добычи и транспорта нефти и газа (проектирование разработки и обустройство месторождений, ремонт скважин, автоматизация промыслов, повышение нефтеотдачи, трубопроводы, строительство морских платформ и др.), является информационной основой экологической безопасности на суше, море и в недрах при добыче нефти и газа [12].

Финансовая емкость нефтесервисного рынка России значительна, и имеет тенденцию к ежегодному росту. Так, если в 2018 г. рынок нефтесервиса составлял 1,2 триллиона рублей, то в 2023 г. составил уже 1,48 триллиона.

Этому способствует медленное, но стабильное увеличение инвестиций в разведку и добычу, которые в 2022 г. составили 1,8 триллиона рублей [13].

Основными направлениями нефтяного сервиса являются бурение, гидроразрыв пласта, текущий и капитальный ремонт скважин, геологоразведка.

Приведенные данные говорят о том, что нефтесервис является самостоятельным сегментом нефтяной промышленности, критически важным, обеспечивающим нужный уровень добычи нефти и газа. Кроме того, нефтесервис, в силу своей технологичности, высокой степени механизации и автоматизации, является критической информационной инфраструктурой. Учитывая изложенное, изучение специфики обеспечения информационной безопасности нефтесервисных предприятий имеет значительный научный и практический потенциал.

Особенностями условий труда на нефтесервисных предприятиях являются: непрерывный характер, высокая степень механизации, автоматизация. Местом проведения работ является обособленно обустроенная местность — месторождения, расположенные, как правило, в большом отдалении от населённых пунктов.

Перечисленные факторы приводят к тому, что предприятия применяют вахтовый метод работы, содержат большой штат персонала.

Вертикально интегрированными нефтяными компаниями на нефтяных месторождениях организован серьёзный пропускной режим, в связи с чем между ними и нефтесервисными предприятиями организован постоянный документооборот по оформлению пропусков. Кроме того, помимо собственных сотрудников на нефтесервисные предприятия возложена обязанность по подготовке документов на получение пропусков и для субподрядных организаций.

Внутренние локальные документы нефтяных компаний, требования федерального законодательства устанавливают высокие требования к обучению персонала, состоянию здоровья, периодичности медицинских обследований.

Перечисленные факторы демонстрируют особую важность для нефтесервисных предприятий в защите персональных данных.

Приведенная статистика отражает, что нефтесервисный рынок является высококонкурентным, в связи с чем, в сегменте информационной безопасности возникают два важных направления.

Первое — защита коммерческой информации. Конкурирующие компании по-разному подходят к организации производства, использованию финансовых инструментов, оптимизации затрат. Данная информация является критической для компании и подлежит защите.

Второе — обеспечение бесперебойного функционирования каналов связи, программного обеспечения. Нефтесервисным компаниям присуща высокая мобильность, регулярные переезды на новые проекты и локации, которые требуют организации удаленных офисов, проектов. Кроме того, нефтесервис отличается высокой технологичностью, развитым уровнем автоматизации и широким применением различного программного обеспечения.

Нефтесервисные предприятия относятся к перечню предприятий, определяемых Федеральным законом от 26 июля 2017 г. №187 «О критической информационной инфраструктуре» [14], [15]. В связи с этим, определяются дополнительные требования в области информационной безопасности. Обеспечение требований федерального законодательства подразумевает постоянную работу по сбору информации о вовлечении в производство новых основных средств, регулярное категорирование объектов, оценку угроз, их моделирование и планирование средств и методов их нейтрализации. Кроме того, данное направление требует постоянного взаимодействия с органами государственной власти, такими как ФСТЭК, НЦКИ.

Перечисленные направления обеспечения информационной безопасности основные, но не являются исчерпывающими. Все они требуют административного регулирования и регламентирования, накопления и обработки большого массива информации.

Таким образом, нефтесервисные предприятия требовательны к следующему перечню информационных блоков:

1. Нормативная база федерального законодательства. На сегодняшний день в Российской Федерации принято и действует множество законов и подзаконных актов, так или иначе регулирующих вопросы информационной безопасности. В этот же блок возможно включить и отраслевое законодательство для конкретного предприятия, имеющее в своей структуре вопросы информационной безопасности. Важными нормативными актами являются, например, Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Локальные нормативные акты предприятия, регламентирующие вопросы информационной безопасности: политики, регламенты, инструкции, приказы. В этот же блок могут быть добавлены локальные нормативные документы по информационной безопасности вертикально интегрированных нефтяных компаний, которые, как правило, являются приложениями к договорам на оказание услуг.
3. Критическая информационная инфраструктура. Как указано выше, нефтесервисные предприятия по-своему ОКВЭД относятся к критической информационной инфраструктуре, что в соответствии с Федеральным законом от 26 июля 2017 г. №187 «О критической информационной инфраструктуре» подразумевает ряд мероприятий. Создание и функционирование постоянных комиссий по категорированию, категорирование и основных средств, переписка и взаимодействие с уполномоченными органами государственной власти (Министерство энергетики РФ, ФСБ РФ, ФСТЭК), оценка угроз, подготовка модели и т.д.
4. Защита персональных данных. Вопросы защиты персональных данных регулируются Федеральным законом от 27 июля 2006 г. №152 «О персональных данных».
5. Защита коммерческой информации. Обеспечивается, согласно Федеральному закону от 29 июля 2004 г. №98 «О коммерческой тайне».
6. Защита ИТ инфраструктуры, включая постоянную оценку защищенности, антивирусную политику, реализацию рекомендаций НЦКИ, наличие обнов-

лений и т. д. Здесь важным является соответствие рекомендациям Федерального стандарта ГОСТ Р ИСО/МЭК 27001–2021 «Информационные технологии. Методы и средства обеспечения информационной безопасности. Системы менеджмента информационной безопасности. Требования».

По причине того, что многие документы в области информационной безопасности должны быть разработаны и утверждены в соответствии с требованиями федеральных законов и стандартов, актуальным вопросом остается автоматизация работы специалистов по разработке документов.

В таких условиях возникает практический вопрос, как осуществлять хранение информации, ее обмен, накопление статистики, обработку и обеспечение доступности для сотрудников нефтесервисных предприятий в перечисленных информационных блоках. Какие технологии и инструменты необходимо применять, чтобы обеспечить надежную сохранность информации, ее систематизацию и передачу, и развитие в условиях текучести персонала.

Адаптации разработанной интеллектуальной системы к деятельности специалистов ИБ на нефтесервисных предприятиях

Проведенный анализ потребностей нефтесервисных предприятий отразил важные аспекты в работе специалистов с нормативными документами в области информационной безопасности. Подготовленная база данных разработанной ЭИАС включает указанные нормативные акты и позволяет осуществлять навигационные и аналитические работы в рассматриваемой области, однако, согласно поставленным задачам, отсутствует решение вопроса автоматизации подготовки документов.

Для этого требуется включить в структуру разработанной ЭИАС дополнительный модуль автоматизированного составления документов. С его помощью эксперты смогут формировать шаблонные формы в соответствии с законодательством РФ для последующей автоматизированной обработки и сохранения полученных документов пользователями ЭИАС.

Алгоритм работы модуля автоматизированного составления документов представляется следующим образом:

1. Пользователь заполняет анкету с данными организации;
2. Введенные данные подставляются на соответствующие места в документе путем алгоритма простой замены;
3. Пользователь получает возможность сохранить комплект подготовленных документов в соответствии с введенными данными, при условии полного заполнения необходимых полей.

Особенностью реализации является то, что экспертам необходимо заранее подготовить формы шаблонов расширения .doc и обозначить места размещения вводимых пользователем данных.

Данные могут быть статическими, например: название организации, ФИО руководителя и т. д. и динамическими, например временными, указание даты подготовки документа. Кроме того, данные могут быть простыми и комплексными, когда имеется возможность указания нескольких значений, генерирующих таблицы в получаемом документе.

Новая общая структура ЭИАС выглядит следующим образом (см. рис. 4).

Таким образом, важным дополнительным компонентом ЭИАС для адаптации к применению на нефтесервисных предприятиях является модуль автоматизированного составления документов. Новая функциональная возможность позволяет автоматизировано формировать необходимые документы и управлять процессами информационной безопасности на предприятии.

Заключение

В данном исследовании были рассмотрены проблемы обеспечения информационной безопасности на нефтесервисных предприятиях и предложен подход к адаптации разработанной экспертной информационно-аналитической системы для предприятий данного направления.

Проведенный анализ существующих инструментов для работы специалистов по информационной безопасности выявил необходимость использования комплексного подхода, реализованного в разработанной ЭИАС.

Анализ деятельности нефтесервисных предприятий отразил высокий объем конфиденциальной информации и комплекса задач, определяемых спецификой технологических процессов и производств и регламентируемых законодательством Российской Федерации.

Кроме того, в работе определены приоритетные направления деятельности специалистов по информационной безопасности на нефтесервисных предприятиях, такие как обеспечение соответствия требованиям законодательства РФ, защита конфиденциальных данных, разработка локальных нормативных документов и др.

Для адаптации ЭИАС к деятельности нефтесервисных предприятий предложено дополнить ее модулем авто-

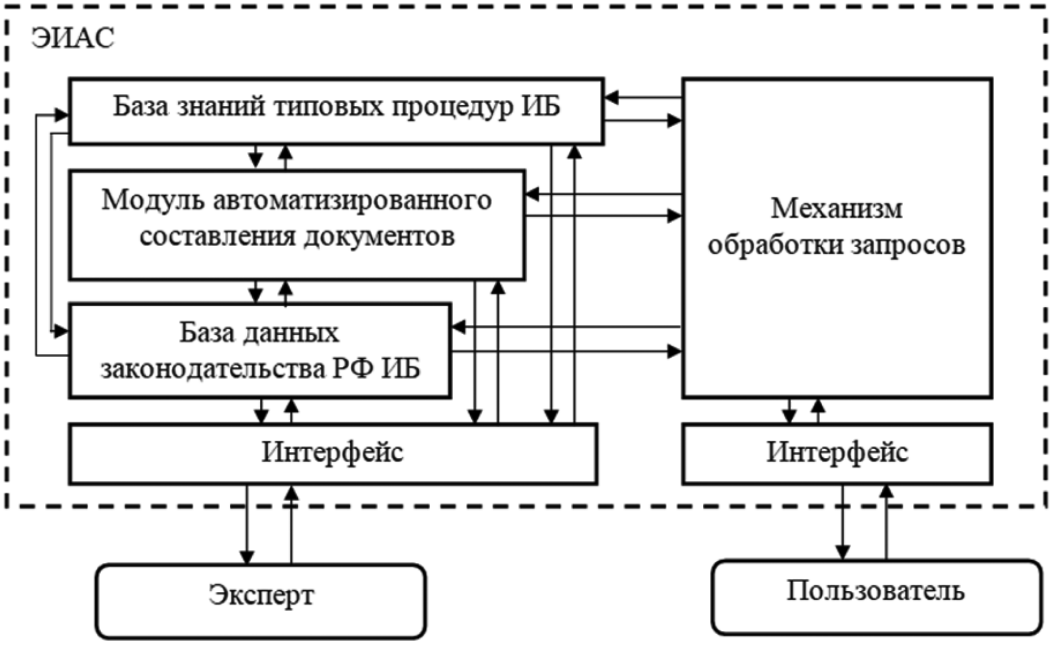

Рис. 4. Измененная структура ЭИАС

матизированного составления документов в соответствии с требованиями законодательства РФ и отраслевой спецификой. Это позволит повысить эффективность работы специалистов по защите информации, минимизировать человеческий фактор в подготовке документов, обеспечить соблюдение нормативных требований.

Таким образом, результаты проведенного исследования демонстрируют актуальность и практическую значимость применения разработанной ЭИАС для нефтесервисных предприятий с целью повышения уровня информационной безопасности и определяют направления разработки аналогичных систем для предприятий любого профиля.

ЛИТЕРАТУРА

1. Guo H. Correction to: An Ostensive Information Architecture to Enhance Semantic Interoperability for Healthcare Information Systems / H. Guo, M. Scriney, K. Liu // Information Systems Frontiers. — 2023. — DOI 10.1007/s10796-023-10387-5. — EDN KVNJFF.
2. The Future of Enterprise Information Systems / A. Sunyaev, T. Dehling, S. Strahringer [et al.] // Business & Information Systems Engineering. — 2023. — Vol. 65, No. 6. — P. 731–751. — DOI 10.1007/s12599-023-00839-2. — EDN PWXSGR.
3. Чеканов И.Р. Анализ семантических элементов базы данных экспертной системы для работы с законодательными и нормативными документами в области информационной безопасности / И.Р. Чеканов, А.Е. Краснов // Проблемы управления безопасностью сложных систем : Материалы XXX международной конференции, Москва, 14 декабря 2022 года / Под общей редакцией А.О. Калашникова, В.В. Кульбы. — Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2022. — С. 221–225. — DOI 10.25728/iccss.2022.68.92.031. — EDN CQWTRY.
4. Свидетельство о государственной регистрации программы для ЭВМ № 2023667310 Российская Федерация. Фемида: № 2023665111: заявл. 19.07.2023: опубл. 14.08.2023 / И.Р. Чеканов. — EDN THQUVI.
5. Современные тенденции в развитии коммерческих компьютерных справочно-правовых систем / В.В. Филатов, Е.И. Минайченкова, И.В. Положенцева, Н.Ю. Логунова // Журнал прикладных исследований. — 2022. — Т. 9, № 6. — С. 831–838. — DOI 10.47576/2712–7516_2022_6_9_831. — EDN BZYIRF.
6. Справочник законодательства РФ в области информационной безопасности (версия 04.04.2024) [Электронный ресурс]// Хабр — 2024. — URL: https://habr.com/ru/post/432466/ (Дата обращения: 15.04.2024).
7. [В закладки] Базовая карта законодательства РФ по защите информации и как ей пользоваться [Электронный ресурс]// Хабр — 2024. — URL: https://habr.com/ru/companies/bastion/articles/595215/ (Дата обращения: 15.04.2024).
8. Чеканов И.Р. Автоматизация обеспечения анализа и использования законодательных и нормативных документов в области информационной безопасности / И.Р. Чеканов, А.Е. Краснов // Современные проблемы автоматизации технологических процессов и производств : сборник научных докладов научно-практической конференции с международным участием, посвященной 100-летию со дня рождения Игоря Константиновича Петрова, Москва, 11 октября 2023 года. — Курск: ЗАО «Университетская книга», 2023. — С. 314–320. — EDN FAXADI.
9. Ушков М.Е. Структура информационной системы поддержки принятия решений оператором АЭС / М.Е. Ушков, В.Л. Бурковский // Вестник Воронежского государственного технического университета. — 2021. — Т. 17, № 6. — С. 8–12. — DOI 10.36622/VSTU.2021.17.6.001. — EDN TCDGOO.
10. Смирнов А.В., Левашова Т.В., Пономарев А.В. Поддержка принятия решений на основе человеко-машинного коллективного интеллекта: современное состояние и концептуальная модель. Информационно-управляющие системы. 2020. № 2, с. 60–70. doi:10.31799/1684–8853-2020-2-60-70

11. Сайгаткина С. Вход в Зазеркалье через потолок / С. Сайгаткина // Энергетическая политика. — 2022. — № 11(177). — С. 16–29. — DOI 10.46920/2409–5516_2022_11177_16. — EDN AIZMKK.
12. Давиденко Л.М. Интеллектуальные технологии в практике нефтегазового сектора / Л.М. Давиденко // E-Management. — 2020. — Т. 3, № 4. — С. 4–12. — DOI 10.26425/2658–3445-2020-3-4-4–12. — EDN GTJMHC.
13. Нефтесервисные услуги: структура отрасли / [Электронный ресурс] // Атлас инвестиций российско-китайского энергетического сотрудничества 2021: [сайт]. — URL: https://rcebf.com/atlas/ru/oil-gas-industry-russia/oilfield-services.html (дата обращения: 14.05.2024).
14. Шемякин С.Н. Критическая информационная инфраструктура / С.Н. Шемякин, А.М. Гельфанд, Г.А. Орлов // Наука и инновации — современные концепции : Сборник научных статей по итогам работы Международного научного форума, Москва, 17 января 2020 года / Отв. ред. Хисматуллин.Д.Р. Том 1. — Москва: Инфинити, 2020. — С. 114–118. — EDN IRYHVD.
15. Пестракова К.А. объекты критической информационной инфраструктуры / К.А. Пестракова, И.А. Бельченко // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы XII Межрегиональной научно-практической конференции, Брянск, 30 апреля 2020 года / Под редакцией О.М. Голембиовской, М.Ю. Рытова. — Брянск: Брянский государственный технический университет, 2020. — С. 120–124. — EDN RLDBCV.

© Краснов Андрей Евгеньевич (krasnovmgutu@yandex.net); Чеканов Иван Романович (cartmen98@yandex.ru);
Лысцев Константин Сергеевич (Konstantin.Lystsev@bk.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»