ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.5
CC BY 4.0
DOI: 10.21822/2073-6185-2024-51-2-164-174 Оригинальная статья / Original article

Архитектура системы управления инцидентами информационной безопасности на предприятии нефтегазового сектора

О.Л. Цветкова, А.Р. Айдинян
Донской государственный технический университет,
344002, г. Ростов-на-Дону, пл. Гагарина, 1, Россия

Резюме. Цель. В настоящее время на предприятиях широко внедряются системы управления инцидентами информационной безопасности, которые предназначены для решения таких задач как своевременное установление факта возникновения инцидента, проведение анализа и исследования причинно-следственных связей, повлекших увеличение вероятности возникновения нарушений, модификация или создание новых нормативных документов, описывающих организационные мероприятия, внедрение технических и программных средств, обеспечивающих превентивные меры защиты. Предприятие нефтегазового сектора, атакованное злоумышленниками, может столкнуться с различными проблемами, среди которых особенно существенными для производственного процесса являются полная или частичная остановка производства, выход из строя дорогостоящего оборудования. Кроме того, актуальность процессов управления инцидентами информационной безопасности для предприятий нефтегазового сектора обусловлена тем, что реализация угроз может привести не только к финансовым потерям, но и к серьезному вреду экологии. **Метод.** Разработанная архитектура системы управления инцидентами информационной безопасности основана на использовании цикла Шухарта-Деминга. **Результат.** Получена модель архитектуры системы управления инцидентами информационной безопасности, которая может использоваться на предприятиях нефтегазового сектора для эффективного и своевременного отслеживания и анализа возникающих инцидентов, планирования мер по устранению последствий реализации инцидентов, предотвращения их повторного возникновения. **Вывод.** Предлагаемая архитектура системы управления инцидентами информационной безопасности позволяет учесть особенности предприятий нефтегазового сектора, связанные с влиянием информационной безопасности на производственный процесс в связи с высокой автоматизации производственного процесса и высокими техногенными рисками.

Ключевые слова: система управления инцидентами, управление инцидентами, информационная безопасность, архитектура системы управления инцидентами, цикл Шухарта-Деминга

Для цитирования: О.Л. Цветкова, А.Р. Айдинян. Архитектура системы управления инцидентами информационной безопасности на предприятии нефтегазового сектора. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(2):164-174. DOI:10.21822/2073-6185-2024-51-2-164-174

Architecture of the Information Security Incident Management System at Oil and Gas Enterprises

O.L. Tsvetkova, A.R. Aidinyan
Don State Technical University,
1 Gagarina Square, Rostov-on-Don, 344002, Russia

Abstract. Objective. Currently, enterprises are widely implementing information security incident management systems, which are designed to solve such problems as timely identification of the fact of an incident, analysis and research of cause-and-effect relationships

that lead to an increase in the likelihood of violations, modification or creation of new regulatory documents describing organizational activities, implementation of technical and software tools that provide preventive protection measures. An enterprise in the oil and gas sector that has been attacked by attackers may face various problems, among which the complete or partial shutdown of production and the failure of expensive equipment are especially significant for the production process. In addition, the relevance of information security incident management processes for enterprises in the oil and gas sector is due to the fact that the implementation of threats can lead not only to financial losses, but also to serious environmental damage. **Method.** The developed architecture of the information security incident management system is based on the use of the Shewhart-Deming cycle. **Result.** A model of the architecture of an information security incident management system has been obtained, which can be used at enterprises in the oil and gas sector for effective and timely tracking and analysis of emerging incidents, planning measures to eliminate the consequences of incidents, and preventing their reoccurrence. **Conclusion.** The proposed architecture of the information security incident management system allows us to take into account the characteristics of oil and gas sector enterprises associated with the impact of information security on the production process due to the high automation of the production process and high man-made risks.

Keywords: incident management system, incident management, information security, incident management system architecture, Shewhart-Deming cycle

For citation: O.L. Tsvetkova, A.R. Aidinyan. Architecture of the Information Security Incident Management System at Oil and Gas Enterprises. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(2):164-174. DOI:10.21822/2073-6185-2024-51-2-164-174.

Введение. В настоящее время на предприятиях различных отраслей все более важной становится задача создания системы мероприятий для обнаружения и реагирования на инциденты информационной безопасности (ИБ) в приемлемые сроки.

Такая деятельность необходима, поскольку под угрозой находятся не только конфиденциальность, целостность и доступность информации, но и репутация, финансовые ресурсы и эффективность работы предприятия. Инциденты ИБ могут серьезно повлиять на производственные процессы, привести к финансовым и репутационным потерям.

Постановка задачи. Важность этого исследования заключается в том, что управление инцидентами ИБ является ключевым элементом системы защиты информации.

Полученные данные на этапе управления инцидентами ИБ необходимы для рискового анализа ИБ, оценки эффективности принимаемых мер по обеспечению ИБ и других аспектов.

Управление инцидентами ИБ включает деятельность руководителей предприятий, сотрудников службы защиты информации, которая направлена на выполнение анализа инцидентов и принятие соответствующих мер, направленных на реализацию оперативного реагирования на угрозы ИБ.

Согласно [1], событие ИБ - идентифицированное проявление определенного состояния системы, сервиса или сети, которое указывает на возможное нарушение политики ИБ или отказ в работе защитных мер, либо возникновение ранее неизвестной ситуации, связанной с безопасностью; инцидент ИБ - это единичное или серия нежелательных неожиданных событий ИБ, которые имеют значимую вероятность нарушения бизнес-процессов и угрожают ИБ. В [2] указаны основные этапы работы с инцидентами ИБ: оперативно выявить и отреагировать на появление инцидента, устранить последствия, обозначить и реализовать меры по предотвращению повторного возникновения подобных инцидентов.

Для реализации этих этапов создается группа реагирования на инциденты ИБ, состоящая из обученных и надежных сотрудников предприятия [2]. При этом рекомендуется включение представителей различных подразделений, включая службу ИБ,

информационные технологии, персонал и юридическую службу, в состав группы.

Задачи группы реагирования на инциденты ИБ:

- гарантирование наличия высококвалифицированных специалистов на предприятии, которые занимаются анализом инцидентов и формированием алгоритмов реагирования на инциденты;
- разработка отчетов о возникновении и анализе инцидентов для руководства;
- максимальное сокращение материальных и репутационных убытков, возникающих как последствия инцидентов для предприятия.

Методы исследования. Для эффективного реагирования на инциденты ИБ рекомендуется создать группу из представителей различных подразделений компании, включая службу ИБ, службу информационных технологий, службу персонала и юридическую службу. Кроме того, в группу могут быть привлечены бизнес-менеджеры профильных подразделений и внешние эксперты для получения дополнительных знаний и опыта.

В настоящее время имеется множество рекомендательных и законодательных документов, которые содержат информацию по реализации управления инцидентами ИБ, и формируют основные направления деятельности [3, 4]:

- разработка моделей угроз и потенциальных нарушителей ИБ;
- оценка рисков, связанных с нарушениями политики безопасности;
- внедрение и изменение мер по защите информации;
- создание и организация процессов функционирования службы ИБ на предприятии;
- управление возникающими инцидентами ИБ;
- обеспечение требуемого уровня защищенности персональных данных сотрудников и клиентов организаций.

Работа с инцидентами ИБ, как правило, преследует достижение следующих целей:

- минимизировать возможный ущерб от инцидентов и предотвратить их появление в будущем;
- собирать статистику для корректной оценки рисков, связанных с ИБ;
- осуществлять постоянный мониторинг событий для выявления взаимосвязей между различными событиями и инцидентами.

Важно обращать внимание на повторяющиеся инциденты одного типа, а также на отсутствие информации о каких-либо инцидентах, поскольку это может указывать на проблемы в системе ИБ, такие как неправильная настройка средств защиты, ошибки в классификации инцидентов или отсутствие осведомленности персонала.

Как правило, процесс управления инцидентами ИБ автоматизируется, используются специализированные программно-аппаратные продукты.

Управление инцидентами ИБ является неотъемлемой частью работы службы безопасности практически любого предприятия, которое имеет информационные системы и оперирует цифровыми данными [5]. К ним относятся:

1. Крупные и средние коммерческие предприятия в различных секторах, таких как финансы, производство, телекоммуникации, здравоохранение и другие, должны обладать процессом управления инцидентами ИБ. Они обычно имеют специализированные службы безопасности, которые занимаются обнаружением, анализом и реагированием на инциденты;

2. Государственные учреждения, такие как министерства, агентства, правительственные службы и военные структуры, имеют высокую потребность в управлении инцидентами ИБ, так как они оперируют с большим количеством конфиденциальной информации и критической инфраструктурой;

3. Университеты, школы, колледжи и другие образовательные учреждения также нуждаются в управлении инцидентами ИБ. Они хранят персональные данные студентов и сотрудников, а также проводят исследования, которые требуют защиты от утечек

и несанкционированного доступа;

4. Медицинские учреждения, включая больницы, клиники и страховые компании, имеют огромное количество конфиденциальных медицинских данных, которые требуют высокого уровня защиты и управления рисками;

5. Банки, страховые компании, инвестиционные фонды и другие финансовые организации обрабатывают большие объемы финансовых данных и личной информации клиентов. Они должны иметь мощные механизмы управления инцидентами ИБ для защиты от финансовых мошенничеств и нарушений данных;

6. Технологические компании, разрабатывающие программное обеспечение, интернет-провайдеры, хостинг-провайдеры сталкиваются с высоким уровнем угроз в области ИБ.

Проведение анализа инцидентов оказывает значительное влияние на процесс обеспечения требуемого уровня защищенности информации предприятий, поскольку позволяет:

- понимать угрозы и уязвимости, с которыми сталкиваются предприятия, что помогает оценить риски и разработать соответствующие меры безопасности для предотвращения будущих инцидентов;
- выявить слабые места в информационных системах и процессах безопасности, а тем самым внести улучшения, включая внесение изменений в архитектуру системы, обновление политик безопасности, обучение персонала и дополнительные меры защиты;
- определить идентичности атакующих лиц, методов их действий и используемых уязвимостей, что позволит выполнить предъявление обвинений и судебного преследования;
- выявить причины инцидентов и разработать меры предосторожности для предотвращения повторения подобных инцидентов.

Для предприятий нефтегазового сектора анализ инцидентов ИБ имеет особую важность по нескольким причинам:

- критическая инфраструктура: Предприятия нефтегазового сектора управляют критической инфраструктурой, включая нефтепромысловые объекты, газопроводы, нефтеперерабатывающие заводы и т.д. Инциденты ИБ могут иметь прямое влияние на безопасность и непрерывность работы этих объектов, что может привести к серьезным последствиям в виде прекращения производства, утечки опасных веществ или экологических проблем;
- конкурентные преимущества: в нефтегазовой отрасли конкуренция высока, и компании вкладывают значительные средства в исследования и разработки. Анализ инцидентов ИБ помогает предотвратить утечку конфиденциальной информации, такой как результаты исследований, новые технологии, стратегии развития, что может подорвать конкурентные преимущества и репутацию компании;
- защита персональных данных: предприятия нефтегазового сектора обрабатывают большое количество персональных данных, включая данные о сотрудниках, клиентах, контрагентах и партнерах. Утечка таких данных может привести к серьезным правовым и репутационным последствиям, а также нарушению соответствия законодательству о защите персональных данных;
- сети связи и телекоммуникации: предприятия нефтегазового сектора имеют обширные сети связи и телекоммуникаций, которые играют важную роль в обеспечении операций и связи между различными объектами и подразделениями. Анализ инцидентов ИБ позволяет выявить уязвимости в сетях и телекоммуникациях, а также предпринять соответствующие меры для защиты от несанкционированного доступа и нарушений безопасности;
- кибератаки и шпионаж: нефтегазовый сектор является привлекательной целью для

кибератак и шпионажа. Компании в этой отрасли могут сталкиваться с угрозами со стороны злоумышленников, конкурентов, желающих получить доступ к конфиденциальной информации или нанести ущерб. Анализ инцидентов ИБ позволяет обнаруживать и реагировать на такие угрозы, а также предпринимать меры для их предотвращения.

Обсуждение результатов. Процесс управления инцидентами ИБ включает несколько основных задач. На начальном этапе выполняется обнаружение потенциальных инцидентов с помощью систем мониторинга, инструментов анализа журналов и других технологий.

Следующем этапом явления классификация и оценивание приоритетности инцидентов. Как правило, приоритетность определяется на основе выявленного типа инцидента, уровня его влияния на функционирование и целостность предприятия, возможности реализации актуальных угроз или возникновения новых источников угроз.

После этого происходит реагирование на инциденты, включающее немедленные меры по остановке инцидента и минимизации ущерба.

Далее проводится детальный анализ инцидента для определения его источника, использованных уязвимостей и методов атаки. Все инциденты регистрируются и документируются для последующего использования и улучшения процесса безопасности.

После реагирования и анализа инцидента необходимо восстановить информационные системы и данные, а также провести улучшения процесса реагирования на основе полученного опыта [6].

В научной статье авторы провели сравнительный анализ подходов защиты стран-партнеров в вопросе критической информационной инфраструктуры [7]. В качестве результаты авторы сформировали предложения по совершенствованию российского законодательства в сфере управления ИБ на объектах критической информационной инфраструктуры.

В другой работе авторы поставили своей целью исследования сбор общедоступной информации для определения основных проблем, препятствующих эффективному управлению рисками ИБ в сфере бизнеса [8].

Были выявлены основные проблемы управления рисками ИБ, характерные для отдельных этапов целостного процесса, а материалы, представленные в работе, могут послужить базисом для дальнейших исследований по теме, а также для формирования рекомендаций по разрешению выявленных проблем.

Конкретные шаги и детали реагирования на инциденты могут различаться в зависимости от предприятия и его потребностей в области безопасности.

Эффективность и скорость управления инцидентами ИБ зависят от следующих факторов:

- координации и согласованности действий всех участников процесса, чтобы быстро и эффективно реагировать на инциденты;
- доступности и анализа информации, связанной с инцидентом для принятия правильных решений;
- оперативности и корректности полученных результатов, чтобы принять эффективные меры по устранению инцидента.

Для описания процесса управления инцидентами ИБ используется классическая модель PDCA (Планирование (Plan) — Выполнение (Do) — Проверка (Check) — Действие (Act)), которая представляет собой модель непрерывного улучшения процессов [9]. В [1] модель PDCA представляется как основа функционирования процессов системы управления ИБ. Согласно модели PDCA жизненный цикл процесса управления инцидентами ИБ представляется в виде, показанном на рис. 1.

Применительно к процессу управления инцидентами ИБ, этот цикл может быть использован для обеспечения эффективности и постоянного совершенствования процесса.

Процесс управления инцидентами ИБ состоит из четырех основных этапов:

Этап 1 — Plan (Планирование). На этом этапе разрабатываются стратегии для реагирования на происшествия и утверждаются документы, определяющие организационные процессы. Также выделяются необходимые ресурсы, проводится обучение сотрудников, а также проверяется эффективность разработанной схемы реагирования на происшествия.

Рис. 1. Жизненный цикл процесса управления инцидентами ИБ

Fig. 1. Life cycle of the information security incident management process

Организационно-регламентные документы должны охватывать следующие моменты:

- концептуализация инцидента ИБ и перечисление событий, которые следует считать инцидентами внутри компании;
- описание процедуры уведомления ответственного об инциденте, включающее формат отчета и контактные данные лиц для уведомления;
- указание алгоритма для устранения причин и последствий инцидента;
- предписание алгоритма для расследования инцидента, включающего определение причин и ответственных лиц, а также сбор и сохранение доказательств;
- предложение дисциплинарных мер;
- введение корректирующих и предупреждающих мер для предотвращения возможных инцидентов в будущем.

Важным этапом является выполнение классификации инцидентов ИБ по следующим основным признакам:

- по нарушенным свойствам ИБ, таким как конфиденциальность, целостность и доступность;
- по видам источников угроз, которые вызывают такие инциденты;
- по типу, включая свершившиеся инциденты, попытки осуществления инцидентов и подозрения на инциденты;
- по последствиям для деятельности предприятия, оцененной в денежном выражении или с использованием балльной шкалы;
- по преднамеренности их возникновения (умышленные, вызванные халатностью, случайные);
- по результатам идентификации объектов информационной инфраструктуры, которые пострадали в результате реализации инцидента ИБ;
- по оценке области распространения и воздействия инцидента ИБ, включая ограничения только на одну информационную систему, отдельное структурное подразделение предприятия, все предприятие в целом или выход за пределы предприятия.

Популярным практическим методом классификации инцидентов ИБ является экспертная оценка, реализуемая с помощью привлечения сторонних специалистов. Математическое описание процесса принятия экспертного решения выполняется посредством использования нечеткой логики. Экспертный опыт используется для создания

модели классификации информационно-безопасностных инцидентов, которая состоит из набора лингвистических переменных, связанных с помощью эвристических правил. Примеры эвристических правил, используемых в такой модели, могут включать следующее:

«Если ситуация 1, то выполнять действие 1».

«Если ситуация 2, то выполнять действие 2».

…

«Если ситуация N, то выполнять действие N».

Этап 2 — Do (Выполнение). На этом этапе выполняется обнаружение и идентификация инцидента, предварительный анализ инцидента, реагирование на инцидент.

Команда по управлению инцидентами ИБ принимает активное участие в процессе обнаружения, оценки и ликвидации инцидентов с использованием определенных методов и инструментов.

Этап 3 — Check (Проверка). На этом этапе производится проверка эффективности и соответствия процесса управления инцидентами ИБ заданным целям и метрикам успеха. Это включает анализ данных, сбор статистики и оценку производительности процесса управления инцидентами. Проверка также включает анализ причин инцидентов, обнаружение трендов и выявление слабых мест в процессе управления инцидентами.

Этап 4 — Act (Действие). На этом этапе происходит принятие мер по улучшению процесса управления инцидентами ИБ на основе результатов проверки. Если выявлены недостатки или слабые места, внедряются корректирующие и предупреждающие меры для повышения эффективности процесса. Может потребоваться обновление политик, процедур и инструкций по управлению инцидентами, а также обучение персонала и внесение изменений в технологическую инфраструктуру. После завершения этапа «Act», цикл PDCA повторяется, что создает непрерывный цикл улучшения процесса управления инцидентами ИБ, обеспечивается постоянное совершенствование процесса, адаптация к изменяющимся условиям и эффективное управление инцидентами ИБ на предприятии.

Система управления инцидентами информационной безопасности в нефтегазовом секторе должна быть адаптирована к специфике отрасли, учитывая особенности угроз и требования к безопасности. При этом на предприятиях нефтегазового сектора системы управления инцидентами информационной безопасности необходимы для решения нескольких центральных задач.

Во-первых, принципиально важно регулярно проводить мониторинг и организовать условия для оперативного реагирования на аварии. Система может автоматически обнаруживать аварийные ситуации на объектах нефтегазового сектора, отправлять уведомления операторам и инициировать процесс управления инцидентами.

Во-вторых, необходимо реализовать управление техническими проблемами. Система позволяет регистрировать, классифицировать и отслеживать процессы решения технических проблем, например, таких как сбои оборудования.

В-третьих, система может собирать данные о происшествиях, анализировать их, выявлять тенденции и рекомендовать меры по повышению уровня информационной безопасности на предприятии. Таким образом, система будет проводить анализ производственной безопасности. Важно учитывать особенности системы управления инцидентами информационной безопасности в нефтегазовом секторе:

- в нефтегазовом секторе информационная безопасность имеет высокую степень критичности из-за значительного влияния на производственные процессы, экологию и безопасность персонала;
- предприятия нефтегазового сектора обычно имеют распределенные объекты и инфраструктуру, что требует комплексной системы управления инцидентами с учетом географического разброса;
- нефтегазовый сектор подвержен специфическим киберугрозам, таким как кибершпионаж, кибертерроризм, а также угрозы со стороны конкурентов

и экстремистских организаций;

- в нефтегазовом секторе существуют строгие регуляторные требования и стандарты в области информационной безопасности, что требует соответствия системы управления инцидентами соответствующим нормам;
- нефтегазовые предприятия имеют критическую инфраструктуру, такую как буровые вышки, трубопроводы, заводы и т.д., защита которой является приоритетом в системе управления инцидентами.

События, поступающие от различных технических средств защиты, например, системы мониторинга, системы обнаружения вторжений, брандмауэры и другие устройства безопасности, являются важными источниками информации о процессах, нарушениях и рисках ИБ. Эти события могут быть записями об активности пользователей, сетевом трафике, атаках, уязвимостях и других событиях, связанных с ИБ.

Технические средства защиты генерируют файлы с сохранением всех действий пользователей и журналы событий, которые содержат информацию о действиях и событиях, происходящих в сети и системах. Эти данные могут быть использованы для мониторинга и обнаружения инцидентов ИБ, а также для анализа и понимания текущего состояния безопасности предприятия. Анализ событий от технических средств защиты позволяет выявлять подозрительную активность, атаки, несанкционированный доступ, аномалии в поведении систем и другие потенциальные угрозы ИБ. Это помогает оперативно реагировать на инциденты, а также принимать меры по предотвращению будущих атак и улучшению общей безопасности систем и сетей.

Для эффективного использования информации от технических средств защиты, предприятия должны иметь соответствующие системы мониторинга, сбора и анализа логов. Такие системы позволяют обрабатывать большие объемы данных, фильтровать и классифицировать события, выявлять аномалии и осуществлять реагирование на возникающие угрозы ИБ. Предприятия также могут использовать средства автоматизации и машинного обучения для анализа событий от технических средств защиты. Это позволяет автоматизировать процессы обнаружения, анализа и реагирования на инциденты, улучшая скорость и эффективность реакции на угрозы ИБ.

Системы управления инцидентами выполняют следующие функции: собирают и анализируют информацию о событиях из разных источников; в реальном времени обнаруживают нарушения политик безопасности и атаки на инфраструктуру предприятия; мониторинг действий пользователей; автоматически оповещают о возникновении инцидентов; предоставляют инструменты для расследования инцидентов; формируют доказательную базу по инцидентам ИБ.

Регулярное использование системы управления инцидентами ИБ позволяет отладить процессы обнаружения и реагирования на инциденты, обеспечивает уменьшение потерь из-за реализации угроз ИБ, и в конечном итоге позволяет повысить уровень защищенности информации и ресурсов предприятия.

Системы сбора и корреляции событий (SIEM-системы) объединяют в себе возможности систем SIM и SEM. При этом системы SEM (Security Event Management) функционируют в режиме реального времени, и реализуют автоматический мониторинг событий, который включает сбор событий, оценку их корреляции, формирование предупреждающих сообщений. А системы SIM (Security Information Management) выполняют статистический анализ полученной информации.

Таким образом, предлагается построить модель архитектуры системы управления инцидентами информационной безопасности с учетом особенностей функционирования предприятий в нефтегазовом секторе (рис. 2):

1. Управление критической инфраструктурой обеспечивается включением подсистемы мониторинга промышленного оборудования. Интеграция средств мониторинга и обнаружения угроз с системами управления промышленным оборудованием

для обеспечения безопасности критической инфраструктуры;

2. Автоматизированные и автоматические системы обнаружения утечек газа и нефти. Использование сенсоров и систем мониторинга для обнаружения утечек газа, нефти или других опасных веществ, что может предотвратить аварии и инциденты;

3. Защита от киберфизических атак требует интеграции систем безопасности и автоматизации, что обеспечит защиту не только в цифровой среде, но и в физическом пространстве, включая интеграцию систем безопасности с системами управления производством;

4. Управление рисками обеспечивается включением в архитектуру подсистемы оценки специфичных для отрасли уникальных угроз и уязвимостей в нефтегазовом секторе;

5. Мониторинг геополитических рисков позволяет провести анализ и мониторинг внешних угроз, включая геополитические факторы, которые могут повлиять на безопасность операций в нефтегазовом секторе.

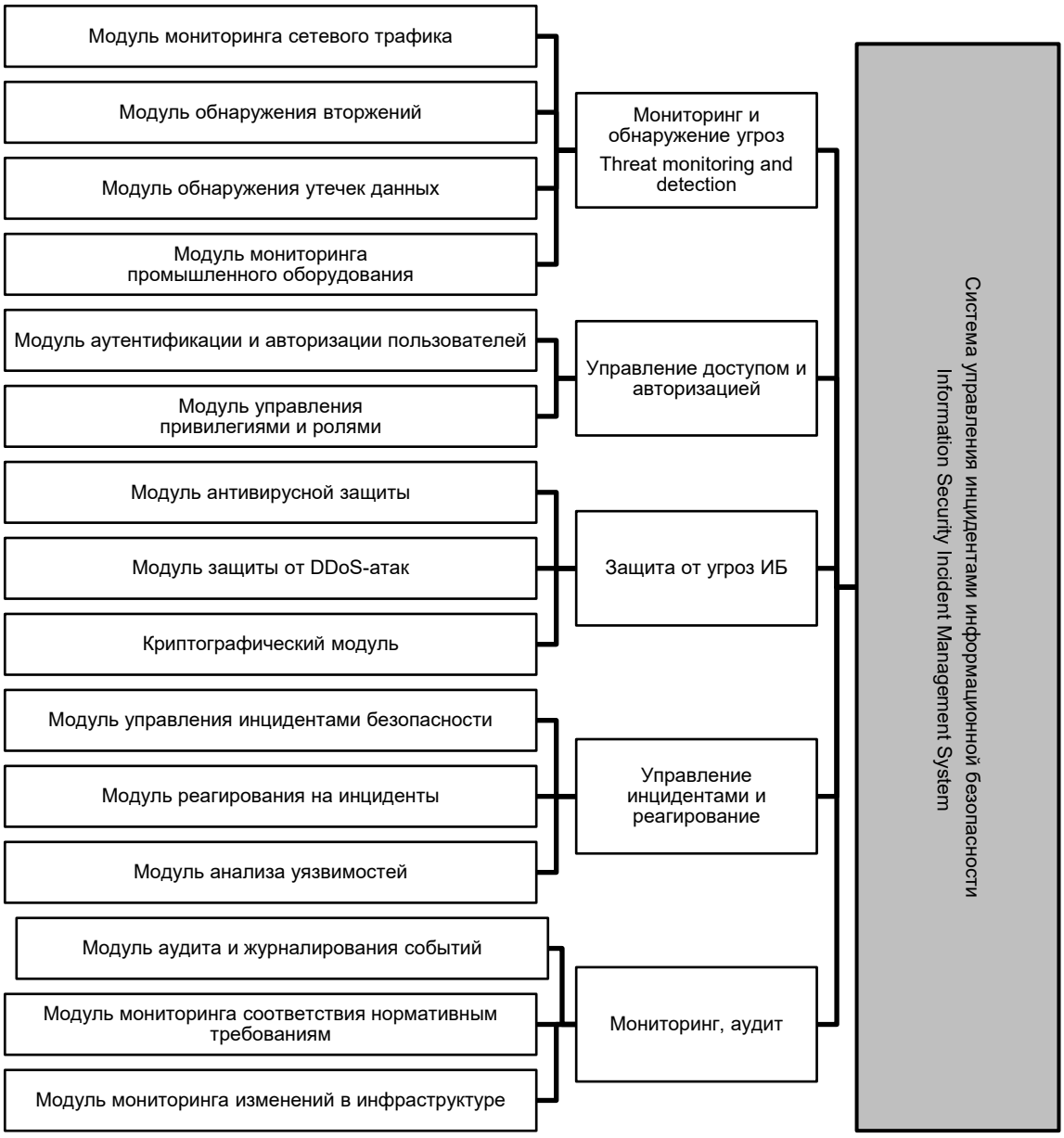

Рис. 2. Архитектура системы управления инцидентами информационной безопасности
Fig. 2. Architecture of the information security incident management system

Предлагаемая архитектура системы управления инцидентами информационной безопасности для предприятий нефтегазовой включает следующие подсистемы: монито-

ринга и обнаружения угроз; управления доступом и авторизацией; защиты от угроз информационной безопасности; управления инцидентами и реагирования; мониторинга и аудита.

Состав каждой подсистемы, содержащейся в предлагаемой системе управления инцидентами информационной безопасности, приведен на рис. 2.

Вывод. Внедрение автоматизации и управления инцидентами ИБ в предприятия нефтегазового сектора позволяет быстро обнаруживать и реагировать на инциденты, минимизируя возможные негативные последствия.

Эффективность процесса управления инцидентами в нефтегазовом секторе определяется следующими показателями:

- предотвращение простоев и снижение эффективности работы за счет значительного уменьшения отрицательного влияния инцидентов на производственные процессы;
- эффективное управление инцидентами путем принятия обоснованных управленческих решений;
- повышение уровня защищенности информации.

Процесс управления инцидентами позволяет предприятию нефтегазового сектора оперативно выявлять, классифицировать и реагировать на инциденты, минимизируя потенциальные убытки, обеспечивает возможность выявления узких мест в безопасности производственных процессов и снижения влияния человеческого фактора.

Библиографический список:

1. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Введ. 01.02.2008. – М.: Стандартинформ, 2008, 31 с.
2. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Введ. 01.02.2008. – М.: Стандартинформ, 2009, 50 с.
3. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Введ. 18.12.2008. – М.: Стандартинформ, 2018, 20 с.
4. ГОСТ Р 59709-2022. Защита информации. Управление компьютерными инцидентами. Термины и определения. – Введ. 29.11.2022. – М.: Российский институт стандартизации, 2022, 20 с.
5. Гарбузов Г. Проведение расследований инцидентов ИБ: организационные и правовые аспект // Информационная безопасность: [сайт]. URL: https://lib.itsec.ru/articles2/control/provedenie-rassledovaniy-incidentov-ib (дата обращения: 02.09.2023).
6. Писаренко И. Выявление инцидентов информационной безопасности // Информационная безопасность: [сайт]. URL: http://lib.itsec.ru/articles2/control/vyyavlenie-incidentov-informacionnoy-bezopasnosti (дата обращения: 02.09.2023).
7. Семишкур, А.Р. Формирование системы требований по обеспечению информационной безопасности на объектах критической информационной инфраструктуры в кооперации Российской Федерации и Китайской Народной Республики на примере газопровода «Сила Сибири» / А.Р. Семишкур, И.И. Лившиц // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 2. – С. 142-152. – DOI 10.21822/2073-6185-2023-50-2-142-152. – EDN TUUTVD.
8. Артамонов, Г.М. Проблемы управления рисками в сфере информационной безопасности / Г.М. Артамонов, В.В. Маслов, С.А. Резниченко // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 2. – С. 25-34. – DOI 10.21822/2073-6185-2023-50-2-25-34. – EDN WFXCEJ.
9. Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов. — М.: РИА «Стандарты и качество», 2008. - 408 с. - ISBN 978-5-94938-063-5

References:

1. GOST R ISO/IEC 27001-2006. Information technology. Methods and means of ensuring security. Information security management systems. *Requirements.* Enter. 02/01/2008. M.: Standartinform, 2008; 31(In Russ)..
2. GOST R ISO/IEC TO 18044-2007. Information technology. Methods and means of ensuring security. Information security incident management. Enter. 02/01/2008. M.: Standartinform, 2009;50. (In Russ).

3. GOST R 53114-2008. Data protection. Ensuring information security in the organization. Basic terms and definitions. – Enter. 12/18/2008. – M.: Standartinform, 2018;20. (In Russ).
4. GOST R 59709-2022. Data protection. Computer incident management. Terms and Definitions. – Enter. 11/29/2022. – M.: Russian Institute of Standardization, 2022; 20. (In Russ).
5. Garbuzov G. Conducting investigations of information security incidents: organizational and legal aspects Information security: [site]. URL: https://lib.itsec.ru/articles2/control/provedenie-rassledovaniy-incidentov-ib (access date: 09/02/2023). (In Russ).
6. Pisarenko I. Identification of information security incidents // Information security: [site]. URL: http://lib.itsec.ru/articles2/control/vyyavlenie-incidentov-informacionnoy-bezopasnosti (access date: 09/02/2023). (In Russ).
7. Semishkur, A.R. Formation of a system of requirements for ensuring information security at critical information infrastructure facilities in cooperation between the Russian Federation and the People's Republic of China using the example of the "Power of Siberia" gas pipeline / A.R. Semishkur, I.I. Livshits. *Herald Daghestan State Technical University. Technical Sciences.* 2023;50(2):142-152. –DOI 10.21822/2073-6185-2023-50-2-142-152. – EDN TUUTVD. (In Russ).
8. Artamonov, G.M. Problems of risk management in the field of information security / G.M. Artamonov, V.V. Maslov, S.A. Reznichenko. *Herald of the Dagestan State Technical University. Technical Sciences.* 2023; 50(2): 25-34. – DOI 10.21822/2073-6185-2023-50-2-25-34. – EDN WFXCEJ. (In Russ).
9. Repin V.V., Eliferov V.G. Process approach to management. Business process modeling. - M.: RIA "*Standards and Quality",* 2008; 408 — ISBN 978-5-94938-063-5(In Russ).

Сведения об авторах:

Цветкова Ольга Леонидовна, кандидат технических наук, доцент, доцент, кафедра вычислительных системы и информационной безопасности; olga_cvetkova@mail.ru. ORCID: 0000-0003-4071-6313

Айдинян Андрей Размикович, кандидат технических наук, доцент, доцент, кафедра вычислительных системы и информационной безопасности; 79081891239@yandex.ru; andstyle@mail.ru

Information about the authors:

Olga L. Tsvetkova, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., Department of Computer Systems and Information Security, olga_cvetkova@mail.ru. ORCID: 0000-0003-4071-6313

Andrey R. Aidinyan, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., Department of Computing Systems and Information Security, 79081891239@yandex.ru; andstyle@mail.ru ORCID: 0000-0001-9455-4079

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 19.02.2024.

Одобрена после рецензирования/ Reviced 22.03.2024.

Принята в печать/ Accepted for publication 22.03.2024.