МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»

Факультет информатики и вычислительной техники
Кафедра компьютерных технологий

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)
по направлению подготовки
09.04.03 «Прикладная информатика»
(направленность (профиль) «Информатизация предприятий и организаций»)

Разработка проекта подсистемы управления инцидентами информационной безопасности в онлайн-сервисе «АльфаДок»

Обучающий(ая)ся _____ 21.06.2019 / Е.А. Максимова
(подпись, дата) И.О. Фамилия

Руководитель
к.э.н, доцент _____ 21.06.2019 / А.Х. Александров
(подпись, дата) И.О. Фамилия

Заведующий кафедрой
д.п.н., профессор _____ 21.06.2019 / Т.А. Лавина
(подпись, дата) И.О. Фамилия

Работа выполнена на базе ООО «КСБ-СОФТ» г. Чебоксары ЧР

Чебоксары 2019

Аннотация

68 с., 34 рис., 21 табл., 2 прил.

Ключевые слова: информационная безопасность, информационные системы, инциденты информационной безопасности, АльфаДок.

Актуальность работы определяется увеличением потребности в системе, позволяющей вести учет несанкционированных действий, способной разрабатывать требуемую документацию в организации, а также позволяющей оповещать о данных действиях требуемые государственные органы.

Научная новизна состоит в анализе существующих решений по управлению инцидентами информационной безопасности, выделении положительных качеств каждого решения и сведения их в единую систему.

В результате проведенного анализа выявлены сильные и слабые стороны разрабатываемой подсистемы управления инцидентами информационной безопасности, спроектирована система, удовлетворяющая требованиям нормативно-правовых актов, государственным стандартам.

Annotation

68 p., 34 pc., 21 t., 2 app.

Keywords: information security, information systems, information security incidents, AlfaDoc.

The relevance of the work is determined by the increase in the need for a system that allows you to keep records of unauthorized actions, is able to develop the required documentation in the organization, and also allows you to notify public authorities about these actions.

The scientific novelty consists in analyzing the existing solutions for managing information security incidents, highlighting the positive qualities of each solution and putting them into a single system.

As a result of the analysis, the strengths and weaknesses of the information security incident management subsystem being developed are identified, and a system has been designed that meets the requirements of regulatory and legal acts and state standards.

Содержание

Введение

Специалистами компании «ООО «НПЦ «Кейсистемс-Безопасность» разработан онлайн-сервис «АльфаДок». Онлайн-сервис «АльфаДок» направлен на выполнение требований законодательства в области защиты персональных данных, государственных информационных систем и объектов критических информационных инфраструктур и позволяет организациям, использующим данный сервис быть постоянно готовыми к проверкам регуляторов, таких как, ФСБ России, Роскомнадзор и ФСТЭК России.

Законодательство Российской Федерации постоянно меняется, и операторы информационных систем обязаны поддерживать документацию организации в актуальном состоянии. Так, с выходом новых изменений в части ведения инцидентов информационной безопасности, операторы государственных информационных систем и объектов критической информационной инфраструктуры обязаны информировать федеральный орган исполнительной власти в области обеспечения безопасности о событиях безопасности, в результате которых нарушено или прекращено функционирование информационной системы и/или нарушена безопасность обрабатываемой в информационной системе информации (компьютерных инцидентах).

Объект исследования: онлайн-сервис «АльфаДок».

Предмет исследования: подсистема управления инцидентами информационной безопасности.

Актуальность работы определяется увеличением потребности в системе, позволяющей вести учет несанкционированных действий, способной разрабатывать требуемую документацию в организации, а также позволяющей оповещать о данных действиях требуемые государственные органы.

Целью работы является разработка проекта подсистемы управления инцидентами информационной безопасности в онлайн-сервисе «АльфаДок».

Задачами работы для достижения поставленной цели являются:

– изучить теоретический материал, нормативы и стандарты и обосновать необходимость разработки подсистемы управления инцидентами информационной безопасности в онлайн-сервисе «АльфаДок»;

– провести анализ существующих решений на рынке информационных технологий области информационной безопасности;

– разработать проект подсистемы управления инцидентами информационной безопасности в онлайн-сервисе «АльфаДок».

Практическая значимость работы состоит в возможности промышленного внедрения разработанной подсистемы управления инцидентами информационной

безопасности на предприятии.

Научная новизна состоит в анализе существующих решений по управлению инцидентами информационной безопасности, выделении положительных качеств каждого решения и сведения их в единую систему.

Работа состоит применительно из введения, трех действий глав ссылка, заключения и списка коммутатором использованной литературы, содержащего 28 наименований.

В первой главе рассматриваются требования действующего законодательства по защите информации, которые предъявляются к юридическим лицам, описываются задачи, которые необходимо выполнить организации для успешного прохождения проверок регуляторов информационной безопасности, также рассматриваются пути решения задач.

Во второй главе происходит сравнение подсистемы в онлайн-сервисе «АльфаДок» с конкурирующими организациями – аналогами сервиса, выявляются сильные и слабые стороны сервиса.

В третьей главе приводится описание разработки подсистемы управления инцидентами информационной безопасности в онлайн-сервисе «АльфаДок», а именно требования к подсистеме, разработка баз данных, проектирование пользовательского интерфейса.

1. Теоретические основы проектирования информационных систем управления инцидентами информационной безопасности

1.1 Основные понятия

Согласно международным регламентам, которые сертифицируют менеджмент информационных систем, инцидентом ИБ является любое событие непредсказуемого и нежелательного характера, которое может повлиять на бизнес-процессы организации/компании, могут скомпрометировать их или нарушить защищенность информационной безопасности. На практике к определению инцидента ИБ можно отнести разноплановые события, которые происходят в процессе работы с информацией, которая может существовать в электронном виде или на материальных носителях. К таким событиям можно отнести как оставление документов в свободном доступе для посторонних лиц, так и атаку хакеров. Оба эти инцидента ИБ в равной степени могут нанести какой-либо ущерб организации/компании.

К основным типам событий можно отнести:

– нарушение правил передачи данных при помощи почтовых или облачных сервисов, сети Интернет;

– программные или технические сбои в оборудовании;

– сбои в работе системного, прикладного обеспечения;

– нарушение правил обработки, передачи и хранения носителей персональных данных или защищаемой информации в любом виде (электронном, бумажном);

– несанкционированный доступ посторонних лиц к информации и ее носителям.

– внедрение вредоносных программ в информационной системе;

– действия по компрометации данных о защите информационной системы.

В компании подобные события должны быть классифицированы и отражены во внутренних регламентах, которые описывают порядок обеспечения информационной безопасности. Также в регламентах нужно установить порядок работы с событиями: описать, какие события относить к более или менее значимым, указать их иерархию. Большая часть событий может быть отнесена к малозаметным, на которые сотрудники организации не обращают должного внимания. В регламентах такие события необходимо описывать более подробно, с указанием мер по их выявлению.

При описании мер по выявлению событий необходимо учитывать, что частота появления инцидентов ИБ и их количество, являются показателем, говорящем о качестве работы системы защиты информации. Повторяющиеся инциденты ИБ являются тенденцией и говорят о намеренной атаке на информационные системы организации.

Тенденция может стать основанием для анализа системы защиты информации и дальнейшего его рассмотрения.

Регламенты по управлению инцидентами ИБ являются частью бизнес-процессов организации. Обозначая инцидент ИБ как нежелательное событие, необходимо иметь механизм по разделению событий на желательные и нежелательные. Кроме того, в регламенте необходимо описывать методы и способы классификаций событий, которые в документе могут быть прямо не обозначены.

В организации должны быть определены следующие условия работы:

– «события информационной безопасности (далее – события ИБ) необходимо своевременно обнаружить и качественно обработать, другими словами, идентифицировать событие в качестве возможного инцидента ИБ;

– выявленные инциденты ИБ должны оцениваться, и реагирование на них должно быть наиболее рациональным и эффективным;

– влияние инцидентов информационной безопасности на организацию должно быть минимизировано с помощью соответствующих мер по защите информационных ресурсов, которые являются частью процесса реагирования на инциденты, без вмешательства в непрерывность основной деятельности организации;

– необходимо быстро сделать выводы из инцидентов ИБ. Это должно быть сделано для того, чтобы увеличить шансы на предотвращение инцидентов информационной безопасности в будущем, чтобы понять, какие меры безопасности должны быть реализованы и использованы для улучшения общей системы управления информационной безопасностью» [9].

При проектировании системы управления инцидентами ИБ необходимо осуществить следующие процессы:

– «ручное или автоматизированное обнаружение и оповещение о возникновении событий ИБ;

– сбор информации, которая может быть связана с событиями ИБ, и проведение оценки этой информации с целью определения, какие события могут быть идентифицированы как инциденты ИБ;

– применение мер по реагированию на возникшие инциденты ИБ;

– для инцидентов ИБ, находящихся под контролем, выполнить менее действия, являющиеся менее важными или срочными (например, меры для полного восстановления процессов системы после инцидента ИБ);

– для инцидентов ИБ, не находящихся под контролем, выполнить «антикризисные» действия (например, вызвать пожарную помощь);

– оповестить персонал организации о наличии инцидентов ИБ и любые относящиеся к ним подробности, а также персоналу третьих организаций (это может включить в себя разглашение подробностей инцидента ИБ для дальнейшей оценки и/или принятия решений);

– соответствующую регистрацию всех действий и решений для будущего анализа;

– разрешение/закрытие инцидентов ИБ» [10].

После разрешения/закрытия инцидентов ИБ необходимо выполнить следующие действия по анализу состояния системы:

– провести дополнительную экспертизу (если это требуется);

– изучить выводы, сделанные из возникших инцидентов ИБ;

– определить требуемые защитные меры по улучшению для внедрения в систему защиты информации, полученные из выводов, извлеченных из возникших инцидентов ИБ;

– определить необходимые меры по совершенствованию системы информационной безопасности в целом с учетом выводов, полученных из анализа качества используемого подхода [10].

1.2 Цели и задачи управления инцидентами информационной безопасности

Целью управления инцидентами ИБ является обеспечение непрерывности процессов в ИС за счет минимизации возможных негативных последствий, вызванных инцидентами ИБ [13].

Задачами управления инцидентами ИБ являются:

– обнаружение событий ИБ и их дальнейшая обработка с целью выявления инцидентов ИБ;

– оценка инцидентов ИБ с целью выработки соответствующих мер реагирования;

– своевременное предотвращение возможных негативных воздействий и оперативное восстановление информационной инфраструктуры после инцидента ИБ;

– сокращение потерь Организации, инициированных инцидентами ИБ;

– выяснение причин возникновения инцидентов ИБ и снижение риска возникновения повторных инцидентов ИБ;

– внесение необходимых изменений в политики информационной безопасности с целью предотвращения подобных инцидентов ИБ в будущем [14].

1.3 Основные этапы процесса управления инцидентами информационной безопасности

Процесс управления инцидентами ИБ состоит из следующих этапов (рисунок 1.3.1):

– подготовка;

– использование;

– анализ и улучшение.

На этапе «Подготовка» в Организации:

– должны определяться и назначаться роли, которые принимают участие в процессе управления инцидентами ИБ;

– должны разрабатываться требуемые организационно-распорядительные документы;

– должны планироваться и исполняться события по обучению сотрудников.

Основные роли, которые должны участвовать в процессе управления инцидентами ИБ:

– Ответственные лица за регистрацию событий ИБ;

– Ответственные лица за управление инцидентами ИБ;

– Группа по реагированию на инциденты ИБ.

Этап «Использование» включает в себя мероприятия по обнаружению и оповещению о наступлении события ИБ, сбор информации о событии ИБ, его оценке и принятию решения по отнесению к инцидентам ИБ, реагированию на инцидент ИБ [11].

На этапе «Анализ и улучшение» оцениваются полнота и адекватность мер, принятых на этапе «Использование», определяются причины возникновения инцидента ИБ, вносятся необходимые изменения в процесс управления инцидентами ИБ в ИС[24].

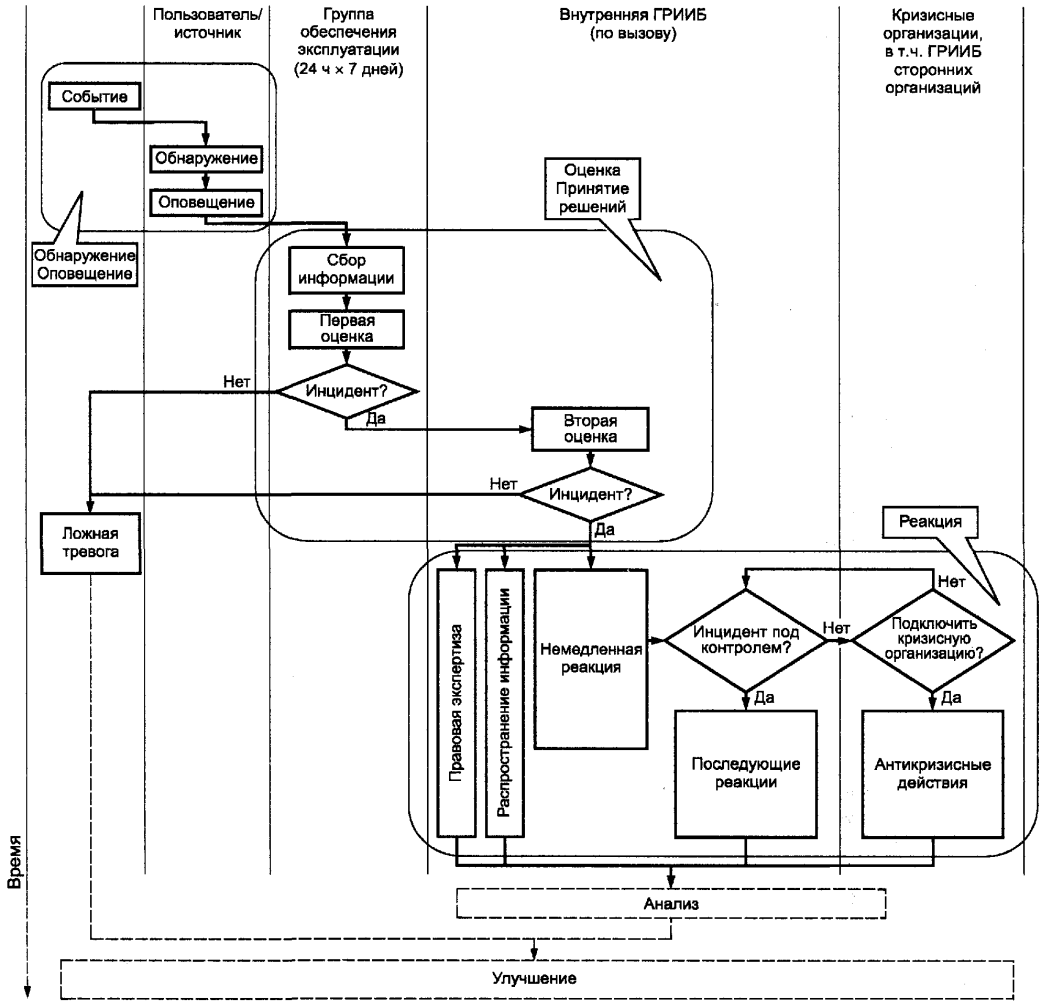

Рисунок 1.3.1 – Блок-схема последовательности операций обработки событий и инцидентов информационной безопасности

Основными процессами на этапе «Использование» являются:

– «обнаружение события ИБ и сообщение о событии одним из сотрудников персонала или самой системой;

– сбор данных о событии ИБ и проведение первичной оценки персоналом группы обеспечения эксплуатации организации для идентификации события в качестве инцидента ИБ;

– если событие представляет собой инцидент информационной безопасности для немедленного реагирования, а также необходимость юридической проверки;

– определение, находится ли инцидент ИБ под контролем;

– дальнейшая оценка и/или принятия решений;

– обеспечение достоверной регистрации всеми причастными лицами всех действий для дальнейшего анализа;

– обеспечение сбора и хранения доказательств в электронном виде и постоянный контроль за безопасным хранением этих доказательств, если это необходимо;

– поддержание режима контроля изменений, включая отслеживание инцидентов ИБ и обновления отчетов по инцидентам для поддержания актуальной базы данных событий/инцидентов ИБ» [10].

Необходимо документировать все этапы разбирательства инцидента ИБ:

– документирование всех собранных доказательств;

– документирование действий, осуществляемых в ходе выполнения мер по устранению инцидента ИБ;

– документирование результатов анализа, проведенного в итоге исследования инцидента ИБ;

– документирование рекомендаций, сформулированных по результатам расследования инцидента ИБ.

Вся собранная информация, касающаяся событий или инцидентов ИБ, должна храниться в базе данных инцидентов ИБ, управляемой группой реагирования на инциденты ИБ. Информация, передаваемая во время каждого процесса, должна быть как можно более полной, чтобы обеспечить наиболее надежную основу для оценок и принятия решений, а также для предпринятых действий.

Преимущества наличия базы инцидентов ИБ:

– контроль реагирования на инциденты ИБ;

– сбор необходимой статистики и аналитики;

– накопление опыта, который может пригодиться при повторении инцидента ИБ.

После обнаружения события ИБ и сообщения о нем последующими действиями являются:

– «распределение ответственности за действия, связанные с управлением инцидентами, посредством соответствующей иерархии персонала, наряду с оценкой и принятием решений, а также за действия, связанные с персоналом, как связанные, так и не связанные с безопасностью;

– предоставление формальных процедур для каждого вовлеченного лица, включая анализ и исправление сделанного сообщения, оценку ущерба и уведомление соответствующего персонала;

– проведение тщательного документирования событий ИБ, а позднее, если событие будет отнесено к инциденту ИБ, то и для последующих действий в отношении инцидента ИБ и обновления базы данных событий/инцидентов ИБ» [11].

1.4 Проблемы управления инцидентами информационной безопасности

Основной проблемой в организациях при внедрении системы управления инцидентами ИБ является отсутствие подготовки персонала, нежелание полностью выполнять все рекомендации по определению событий информационной безопасности. Это может быть вызвано трудностями в восприятии информации, а также действиями, которые не могут быть прямо указаны в инструкциях персонала, или, наоборот, избыточностью информации в правилах.

Внедрение системы управления инцидентами. На практике большинство компаний не осознают необходимость внедрения такой системы. Часто для этого требуется аудит системы, который проводят специалисты ООО «НПЦ Кейсистемс-Безопасность». На этапе аудита определяются системные требования и необходимость внедрения системы управления инцидентами информационной безопасности.

Часто в организации не применяются способы и методы классификации инцидентов ИБ, вследствие чего сотрудники не знают, какое событие можно относить к инцидентам, а какое инцидентом не является.

Также сотрудники часто бывают не оповещены и не информированы о порядке действий и форме отчетности при возникновении инцидентов.

Помимо всего этого на предприятии могут быть не определены порядки и правила регистрации инцидентов ИБ – отсутствуют журналы по их регистрации, не соблюдаются правила и сроки их заполнения.

На предприятиях часто отсутствует четко зафиксированная документально процедура по описанию порядка устранения последствий и причин возникновения по каждому типу инцидентов ИБ. Данная процедура не должна мешать мероприятиям, которые направлены на расследование инцидентов ИБ, т.к. при устранении последствий возникновения инцидента может быть утеряна важная информация о возможных причинах его возникновения.

Разграничение прав пользователей, выявление ответственных за возникновение инцидентов ИБ, ведение журналы по регистрации инцидентов ИБ – всё это, являются определяющими действиями при расследовании каждого отдельного инцидента. В большинстве случаев на предприятиях данным процедурам не придают должного значения. Сразу же после устранения последствий инцидентов действий по выявлении виновных и ответственных не предпринимаются. Часто, в тех случаях, когда в результате возникновения инцидента предприятию был нанесен ущерб, применяется стандартная практика по взысканию с виновных, т.е. виновники определяются по неверным правилам.

В первую очередь необходимо проконтролировать порядок устранения инцидента. На этапе расследования от должностных лиц организации требуется:

– Определить причины, по которым возник инцидент ИБ.

– Определить виновных и ответственных лиц.

– Собрать и зарегистрировать доказательства.

– Установить причины и мотивы совершений инцидента.

Также одной из возможных проблем управления инцидентами ИБ в организации является оценка ущерба от инцидента ИБ. На данный момент не существует официальной методики определения ущерба. ФСТЭК России на конференциях обещает подготовить и опубликовать до конца года методику оценки ущерба и моделирования угроз для критических информационных инфраструктур. Но определять ущерб и строить модель угроз нужно уже сейчас. Многие компании, являющиеся субъектами КИИ, разрабатывают свои карты негативных бизнес-событий с экспертной оценкой их вероятности и размера последствий, но они не всегда являются успешными.

1.5 Выводы

На основании рассмотренного теоретического материала можно выделить следующие моменты.

Цели процесса управления инцидентами ИБ могут быть:

– обеспечить быструю идентификацию любых событий;

– обеспечить доступ к произошедшему событию информационной безопасности;

– обеспечить максимально быстрое устранение последствий появления инцидента информационной безопасности;

– извлечение уроков и анализ причин, позволяющих привести к повторному появлению инцидентов ИБ.

В организации необходимо составить план действий, состоящий из следующих действий:

– разработать и утвердить документы, которые должны описывать процедуру ведения инцидентов ИБ;

– определить лица, ответственные за осуществление процедуры контроля информационной безопасности и, в частности, управления инцидентами информационной безопасности;

– оповещать сотрудников организации о правильном порядке их действий при обнаружении событий информационной безопасности;

– создать единую базу данных, содержащую информацию по всем инцидентам информационной безопасности;

– вести документацию по хранению информации о безопасности информационных инцидентов.

После осуществления мер, направленных на устранение последствий от произошедшего инцидента ИБ, могут быть выявлены следующие выводы:

– проведена переоценка эффективности существующей системы защиты информации;

– выявлены уязвимости организации в части управления информационной безопасностью;

– выявление тенденций, позволяющих выявить системную проблему;

– необходимость дополнительного или повторного обучения работников организации;

– улучшения процесса управления инцидентами ИБ;

– выявление потребности в проведении аудита информационной безопасности.

2 Анализ имеющихся средств управления инцидентами информационной безопасности

Рост внимания к системам, управляющими инцидентами ИБ связан с некоторыми изменениями в области информационной безопасности на уровне изменений требований законодательства Российской Федерации. А именно: вступление в силу с 1 января 2018 года ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ и ряда связанных с ним нормативно-правовых актов, выпущенными такими регуляторами как ФСБ России и ФСТЭК России. Согласно данным документам необходимо создание Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). В большинстве случаев платформой по созданию таких центров оказываются SIEM-системы, но компания ООО «НПЦ «Кейсистемс-Безопасность» предлагает упростить данный процесс, используя облачное решение, в котором имеется подсистема управления инцидентами информационной безопасности.

На данный момент на рынке информационных технологий существует огромное количество компаний, предлагающие продукты по управлению инцидентами информационной безопасности в Российской Федерации. Все они предлагают различные услуги, которые имеют свой ряд достоинств и недостатков. Появление большого количества продуктов, управляющих инцидентами ИБ, порождает среди потенциальных покупателей проблему выбора.

Для сравнительного анализа были выделены следующие критерии сравнения систем по управлению инцидентами ИБ:

– Общая информация – основные показателей стратегии компании, по которым можно будет судить о зрелости предлагаемого решения (таблица 2.1).

– Соответствие направлению импортозамещения – позволит оценить ценность решения как компонента системы соответствия (таблица 2.2).

– Интеграционные возможности – наличие усовершенствованных подсистем управления уязвимостями, инцидентами позволит на начальном этапе эксплуатации ограничиться использованием одного продукта, избавив компанию приобретать за отдельную стоимость дополнительные продукты. А интеграция со сторонними продуктами в целях дополнения информации о событиях ИБ и поддерживаемых источниках событий указывают на открытость компании на рынке ИТ, умение подстраиваться под других игроков, говорит о развитости продукта (таблица 2.3).

– Дополнительные критерии – наличие отчетности, юзабилити, глубина погружения при навигации в рамках интерфейса системы. Все это влияет на оперативность при обработке событий ИБ и выявлении инцидентов ИБ (таблица 2.4, таблица 2.5).

– Архитектура решения – стандарт, масштабируемость, методы управления событиями и инцидентами ИБ и схема лицензирования (таблица 2.6).

– Функциональные особенности – наличие и составляющие параметров, подстраиваемых под конечных пользователей, гибкость настройки этих параметров. Данные параметры позволят оценить применимость решения к отдельной компании. А качество и количество предустановленных из коробки элементов, а также среднее время старта дадут представление о сроках внедрения до получения первых показателей эффективности (таблица 2.7, таблица 2.8).

При выборе продуктов для сравнения были учтены такие факторы, как популярность на рынке ИТ, происхождение производителя, реализованная функциональность.

В итоге были выбраны следующие продукты:

1. Онлайн-сервис «АльфаДок» («Кейсистемс-Безопасность»).
2. MaxPatrol SIEM 4.0 («Позитив текнолоджиз»).
3. RuSIEM («РУСИЕМ»).
4. СёрчИнформ SIEM 1.23 («СёрчИнформ»).
5. Онлайн-сервис «Докшел» («АйТи Мониторинг»).

Таблица 2.1 – Общая информация

Критерий оценки / Произ-водитель	**Онлайн-сервис «АльфаДок»**	**MaxPatrol SIEM 4.0**	**RuSIEM**	**СёрчИнформ SIEM 1.23**	**Онлайн-сервис «Докшелл»**
1	**2**	**3**	**4**	**5**	**6**
Название компании	ООО «НПЦ «Кейсистемс-Безопас-ность»	АО «Позитив текнолоджиз»	ООО «РУСИЕМ»	ООО «СёрчИн-форм»	АйТи Мониторинг
Штаб-квартира	г.Чебоксары	г.Москва	г.Москва	г.Москва	г.Краснодар
Веб-сайт	alfa-doc.ru	ptsecurity.com	usiem.com	searchinform.ru	docshell.ru
Целевой сегмент	Государствен ный сектор, малый бизнес	Все секторы, любой размер бизнеса	Государствен ный сектор, малый, любой размер бизнеса	Малый, крупный и средний бизнес. Все секторы	Государствен ный сектор, малый бизнес
Количество партнеров	98	Более 50	9	6 собствен-ных офисов	44

Продолжение таблицы 2.1

1	2	3	4	5	6
Полное название системы	Онлайн-сервис «АльфаДок»	MaxPatrol SIEM	RuSIEM, RuSIEM Analytics иRvSIEM free	СёрчИнформ SIEM	DocShell
Сроки внедрения	От 4 часов до 1 месяца	От 1 месяца	До 2-3 недель	От 6 часов до 8 дней	От 1 месяца
Стоимость	от 35 тыс.руб.	от 3 млн. руб.	300 тыс. руб.	1 млн. 460 тыс. руб	45 тыс. руб.

Таблица 2.2 – Соответствие направлению импортозамещения

Критерий оценки / Производитель	**Онлайн-сервис «АльфаДок»**	**MaxPatrol SIEM 4.0**	**RuSIEM**	**СёрчИнформ SIEM 1.23**	**Онлайн-сервис «Докшелл»**
Крупнейшее из известных внедрений	ООО ИК «Сибинтек»	ГК Росатом	ГБУ СО «Сахалинский областной центр информатизации»	«НефтеТранс Сервис»	ПАО «Газпром»
Языки интерфейса	Русский	Русский	Русский, английский	Русский	Русский
Лицензия ФСТЭК России	Есть	Есть	Нет	Есть	Есть
Наличие сертификата отечественного ПО	Регистрационный номер в реестре: 1207	Регистрационный номер в реестре: 1143	Регистрационный номер в реестре: 3808	Регистрационный номер в реестре: 4701	Регистрационный номер в реестре: 2276
Секторы экономики, в которых выполнены внедрения	Госсектор и оборона, здравоохранение, IT, ТЭК, пищевая промышленность, строительство, соц. сфера, торговля, транспорт, услуги, ресурсоснабжение	Финансы, госсектор, энергетика, промышленность, связь, торговля	Госсектор, промышленность, коммерческий сектор, процессинг, банки, интернет-коммерция, реклама	Госсектор и оборона, здравоохранение, IT, ТЭК, пищевая промышленность, строительство, сельское хозяйство, соц. сфера, торговля, транспорт, услуги, финансовый сектор, ресурсоснабжение	Госсектор, транспорт, ТЭК
Страны, в которых выполнены внедрения	Россия	Россия, СНГ, Азия, Ближний Восток	Россия, Канада, СНГ	Россия	Россия

Таблица 2.3 –Управление инцидентами, уязвимостями

Критерий оценки / Производитель	**Онлайн-сервис «АльфаДок»**	**MaxPatrol SIEM 4.0**	**RuSIEM**	**СёрчИнформ SIEM 1.23**	**Онлайн-сервис «Докшелл»**
Карточка инцидента	21 поле	19 полей	372 поля, настраиваемые пользователем	Более 50 полей (в зависимости от типа инцидента)	16 полей
Путь эскалации инцидента	Отправка email. Ручная эскалация в карточке инцидента, с возможностью изменения критичности, темы и описания	Автоматическая маршрутизация инцидента при наличии условий (сработавшего правила, критичности инцидента)	Эскалация вручную с возможностью изменения критичности, темы и описания	Автоматическая эскалация при формировании инцидента в зависимости от заданных критериев	Ручная эскалация в карточке инцидента, с возможностью изменения критичности, темы и описания
Оповещение об инциденте	Email	SMTP, скрипты	SMTP	Email	Нет
Принятие решений в рамках процесса обработки инцидентов	Ручное	Ручное	Ручное	Нет	Ручное
Интеграция с системами ServiceDesk	Да (в разработке)	Да	Да	Нет	Неизвестно
Авторегистрация уязвимостей (интеграция со сканерами)	Да. Автоматическое получение уязвимостей из базы БДУ ФСТЭК на основе введенных данных в системе	Отдельный собственный модуль, получение списков от сторонних сканеров уязвимостей, имеющих возможность выгрузки	Интеграция с некоторыми сканерами через API, файловые логи и syslog	Да. Обработка информации из файла отчетов сканера (txt, cvs, XML)	Нет
Настройка собственной модели определения критичности уязвимости	Да	Да	Да	Нет	Нет
Сортировка уязвимостей по различным критериям – в т. ч. критичности	Да	Нет	Да	Нет	Нет

Таблица 2.4– Визуализация и аналитика

Критерий оценки / Производитель	**Онлайн-сервис «АльфаДок»**	**MaxPatrol SIEM 4.0**	**RuSIEM**	**СёрчИнформ SIEM 1.23**	**Онлайн-сервис «Докшелл»**
Работа с фильтрами	Фильтрация по полям	Фильтрация по полям	Фильтрация по полям	Фильтрация по полям	Поиск по полям
Создание/изменение кастомизируемых панелей	Да	Да	Да	Да	Нет
Интерактивная работа с панелями	Да	Да	Да	Да	Да
Возможность формирования отчетов в виде документов, форматы экспорта отчетов в виде документов	PDF, XLSX, XLS, DOCX, CSV	PDF, XLSX, MHT, DOCX, CSV	PDF, XLSX, CSV	PDF, HTML, XML, XLS, XLSX, TXT	DOC
Формирование и рассылка отчетов по расписанию/по критерию	Формирование отчетов по событиям, инцидентам	Формирование отчетов по событиям, инцидентам, по расписанию	Формирование отчетов по событиям, инцидентам, по расписанию	Нет	Формирование отчетов по, активности, инцидентам
Встроенный конструктор отчетов (показатели и графики)	Встроенный конструктор, фильтрация, сложные отчеты через аналитику, подсчет среднего. Кастомизируется пользователем	Встроенного конструктора нет, фильтрация через генерацию отчета	Встроенный конструктор, фильтрация, сложные отчеты через аналитику, подсчет среднего. Кастомизируется пользователем	Да	Фильтрация через генерацию отчетов

Таблица 2.5 – Дополнительные параметры

Критерий оценки / Производитель	**Онлайн-сервис «АльфаДок»**	**MaxPatrol SIEM 4.0**	**RuSIEM**	**СёрчИнформ SIEM 1.23**	**Онлайн-сервис «Докшелл»**
Время существования	5 лет	4 года	4 года	5 лет	3 года
Схема продаж (партнерская /прямая/смешанная)	Смешанная	Партнерская	Смешанная	Прямые продажи	Смешанная
Прайс-лист	Закрытый	Закрытый	Закрытый	Закрытый	Закрытый

Таблица2.6 – Системная архитектура

Критерий оценки / Производитель	**Онлайн-сервис «АльфаДок»**	**MaxPatrol SIEM 4.0**	**RuSIEM**	**СёрчИнформ SIEM 1.23**	**Онлайн-сервис «Докшелл»**
Операционная система в основе решения	WindowsServer 2008, Ubuntu Server, Debian 7	Windows, Debian	Ubuntu x64	Windows	Ubuntu Server, Альт 8 СПСервер
СУБД	PostgreSQL	Elasticsearch	Elasticsearch, RuSIEM DB, postgresql, ClickHouse, neo4j	MongoDM	PostgreSQL
Наличие сформированных образов для платформ виртуализации	VMWare, Hyper-V	VMWare	VMWare, Hyper-V, KVM, QEMU	Нет	VMWare, Hyper-V, KVM, Hyper-V
Возможность хранения данных на внешних носителях	Да (импорт в XML)	Да	Да	Да	Да
Минимальное количество серверов для разворачивания системы	0 (1 – для развертывания системы на мощностях Заказчика)	1	1	1	1
Тип консоли администратора	Веб-консоль, толстый клиент	Веб-консоль	Веб-консоль	Толстый клиент	Веб-консоль, толстый клиент

Таблица 2.7– Защищенность системы

Критерий оценки / Производитель	**Онлайн-сервис «АльфаДок»**	**MaxPatrol SIEM 4.0**	**RuSIEM**	**СёрчИнформ SIEM 1.23**	**Онлайн-сервис «Докшелл»**
1	**2**	**3**	**4**	**5**	**6**
Ролевая модель	Настраиваемая (на этапе тестирования)	RBAC	Настраиваемая	Да	Да
Аутентификация (интеграция с другими системами)	Active Directory, локальная	LDAP	Локально, LDAP, гибридная (локально и LDAP)	Локальная, LDAP, AD	Нет
Журналирование изменений объектов – инициированных пользователями	Логирование действий пользователей, логирование функционирования системы	Да	Да	Логирование действий пользователей, логирование функционирования системы	Да

Продолжение таблицы 2.7

1	2	3	4	5	6
Безопасные протоколы передачи данных между компонентами системы	Защита канала между сервером и толстыми клиентами	TLS/SSL	TLS	Защита канала между сервером и толстыми клиентами	Защита канала между сервером и толстыми клиентами

Таблица 2.8 – Техническая поддержка и обновления

Критерий оценки / Производитель	**Онлайн-сервис «АльфаДок»**	**MaxPatrol SIEM 4.0**	**RuSIEM**	**СёрчИнформ SIEM 1.23**	**Онлайн-сервис «Докшелл»**
Язык поддержки	Русский	Русский	Русский, английский	Русский, английский	Русский
Поддержка по e-mail	Да	Да	Да	Да	Да
Поддержка по телефону	Да	Да	Да	Да	Да
Период обслуживания	Согласно условиям договора	Зависит от типа SLA: 8x5 или 24x7	Зависит от типа SLA: 8x5 или 24x7	Согласно условиям договора	Согласно условиям договора
Наличие доступной технической документации на сайте или по запросу	Доступна по запросу у менеджера, поставляется с продуктом	На портале технической поддержки, поставляется с продуктом	Присутствует, размещена на сайте	Доступна по запросу у менеджера	Доступна по запросу у менеджера
Обновление предустановленных компонентов (дашборды, отчеты, правила корреляции)	1 раз в 2-3 недели	На партнерском портале может выдаваться по запросу	1-2 раза в неделю и чаще	7-12 раз в год	1 раз в месяц

Сравниваемые системы, такие как, MaxPatrol, СёрчИнформ SIEM, являются в больше части SIEM-системами, которые подходят для крупных организаций. В отличие от них, «АльфаДок» и «Докшел» подходят для рынка

2.1 Сравнение подсистемы управления в онлайн-сервисе «АльфаДок» с подсистемой онлайн-сервиса «Докшелл»

Страница подсистемы ведения инцидентов онлайн-сервиса представлена на рисунке 2.1.1 [28]:

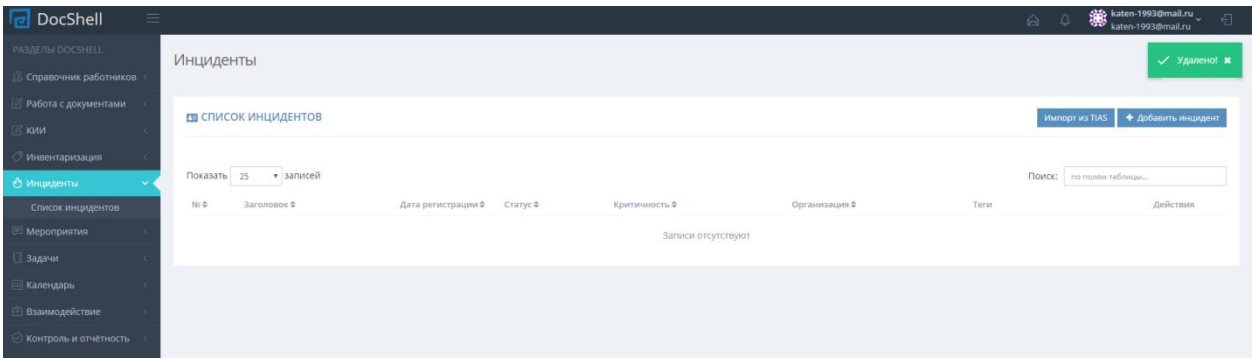

Рисунок 2.1.1 – Основная страница ведения инцидентов онлайн-сервиса «Докшелл»

Страница добавления события представляет собой одну страницу со всеми входными параметрами (рисунок 2.1.2). Можно указать тип инцидента, теги, по которым можно найти инцидент, место, где инцидент произошел, его описание, дату самого инцидента и дату его плановой регистрации.

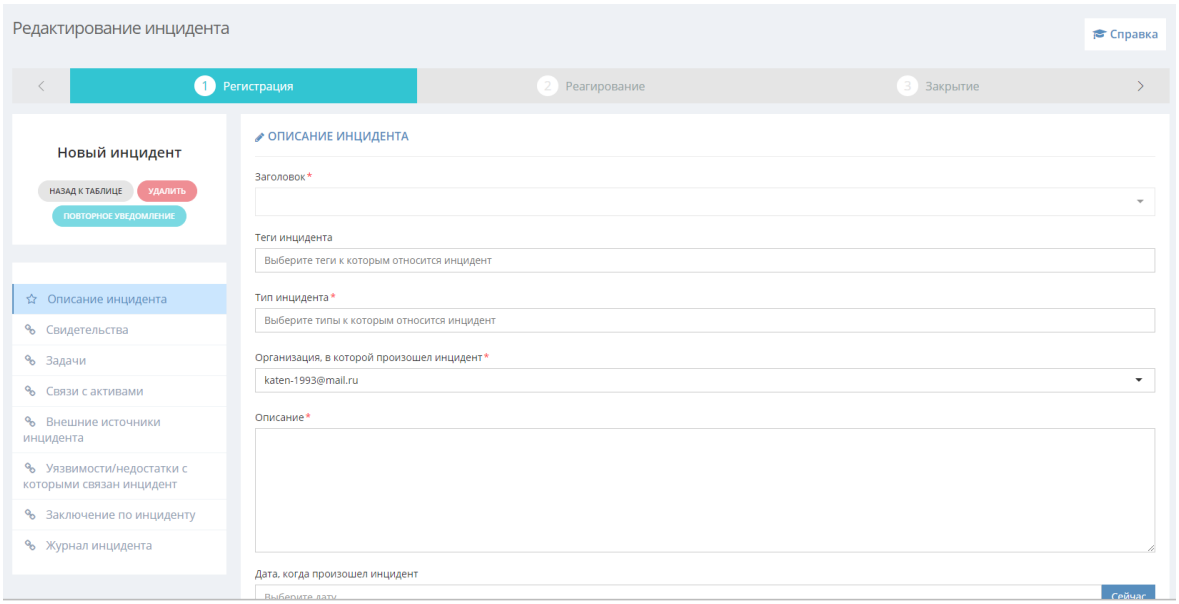

Рисунок 2.1.2 – Карточка инцидента онлайн-сервиса «Докшелл»

Инциденту можно сразу же назначить группу быстрого реагирования из списка сотрудников (в данной системе группа сотрудников называется «Группа информирования»). Также, как и в онлайн-сервисе «АльфаДок» можно указать уровень критичности. Уровень конфиденциальности присутствует в системе «Докшелл», отсутствует в системе «АльфаДок». Наглядно можно увидеть эти параметры на рисунке 2.1.3.

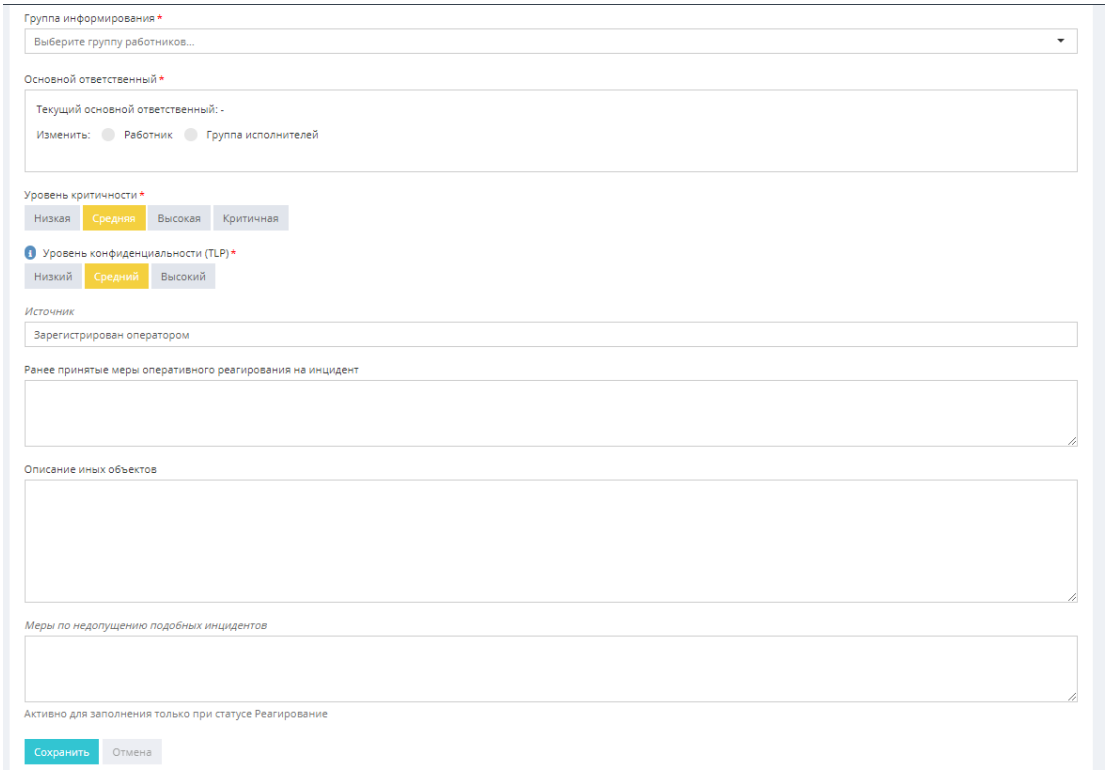

Рисунок 2.1.3 – Карточка инцидента онлайн-сервиса «Докшелл»

В системе «АльфаДок» меры по решению инцидента можно выбрать из списка, а также, меры фильтруются по типу инцидента, что значительно упрощает работу пользователю и не позволяет выбрать неверное значение. В системе «Докшелл» меры прописываются только вручную, аналитика отсутствует.

Также, как в системе «АльфаДок», можно прикрепить дополнительные файлы доказательства произошедшего инцидента (рисунок 2.1.4):

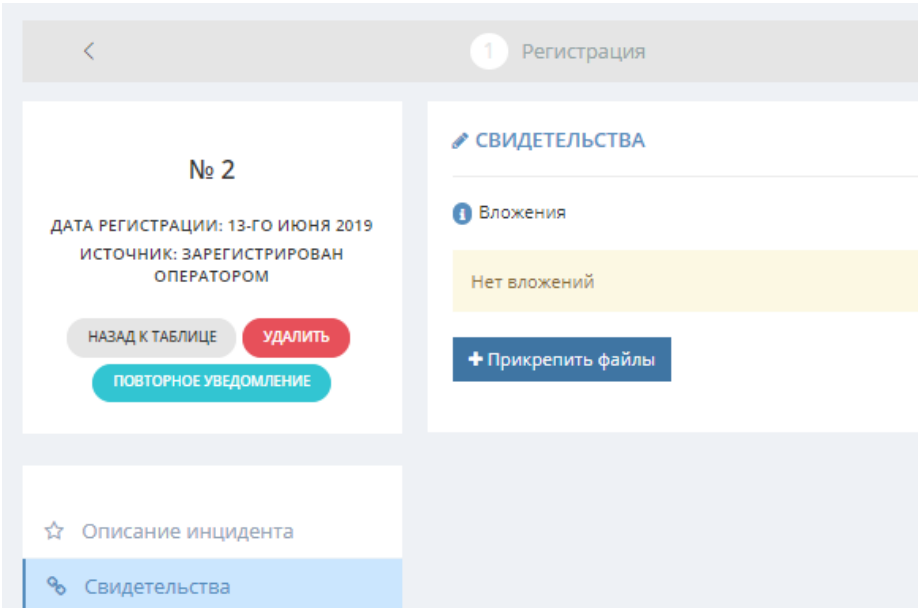

Рисунок 2.1.4 – Вложения для доказательства инцидента в онлайн-сервисе «Докшелл»

Также можно создать задачи по инциденту (рисунок 2.1.5). Для задачи можно указать тему, дату завершения, исполнитель задачи, статус, приоритет. Помимо этого, задачу можно нельзя связать с иным инцидентом. Задача создается в пределах одного инцидента. Хорошим решением является возможность добавить к задаче файл, данного функционала нет в системе «АльфаДок».

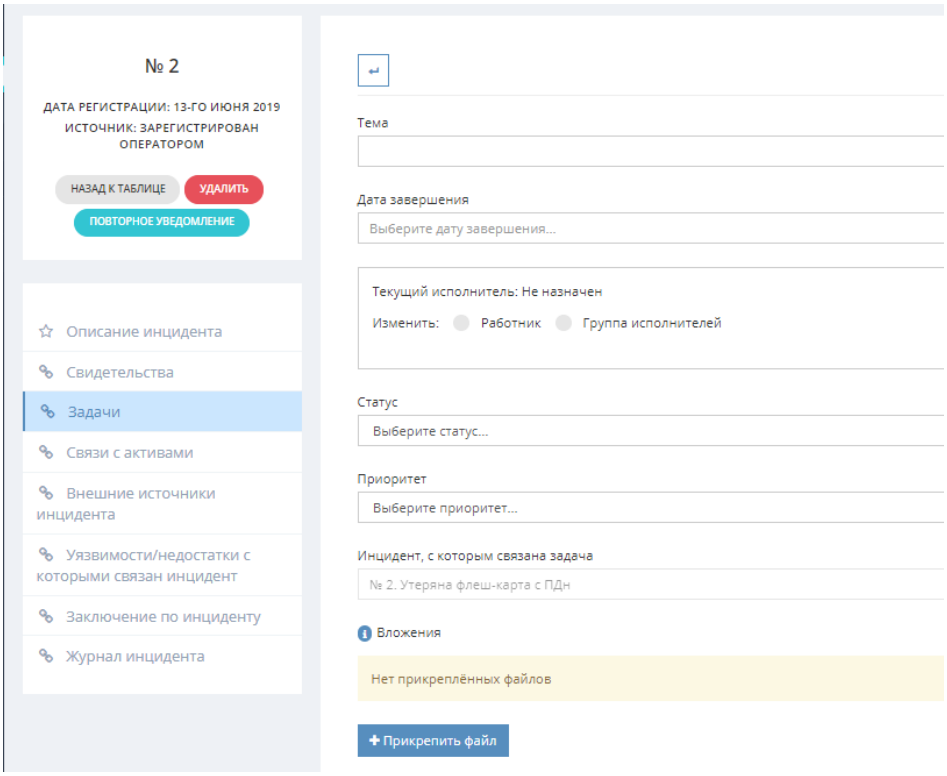

Рисунок 2.1.5 – Задачи, связанные с инцидентом в онлайн-сервисе «Докшелл»

Несомненным плюсом системы «Докшелл» является связь с активами организации (рисунок 2.1.6). В системе «АльфаДок» данный функционал отсутствует.

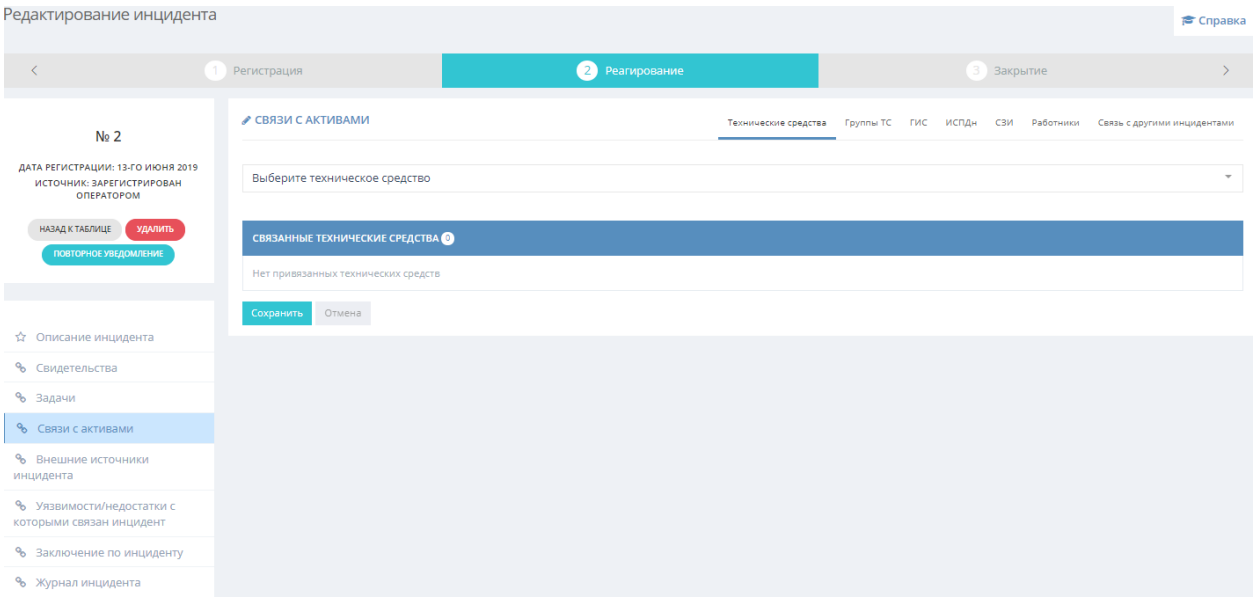

Рисунок 2.1.6 – Связи инцидента с активами в онлайн-сервисе «Докшелл»

Помимо связи с активами большим плюсом является связь с уязвимостями системы (рисунок 2.1.7). В системе «АльфаДок» подсистема «Уязвимости» также присутствует, но связь на данном этапе разработке с уязвимостями не устанавливается. Но минусом данной системы является отсутствие библиотеки уязвимостей, которые есть в «АльфаДок» и, которые постоянно обновляются из банка данных уязвимостей.

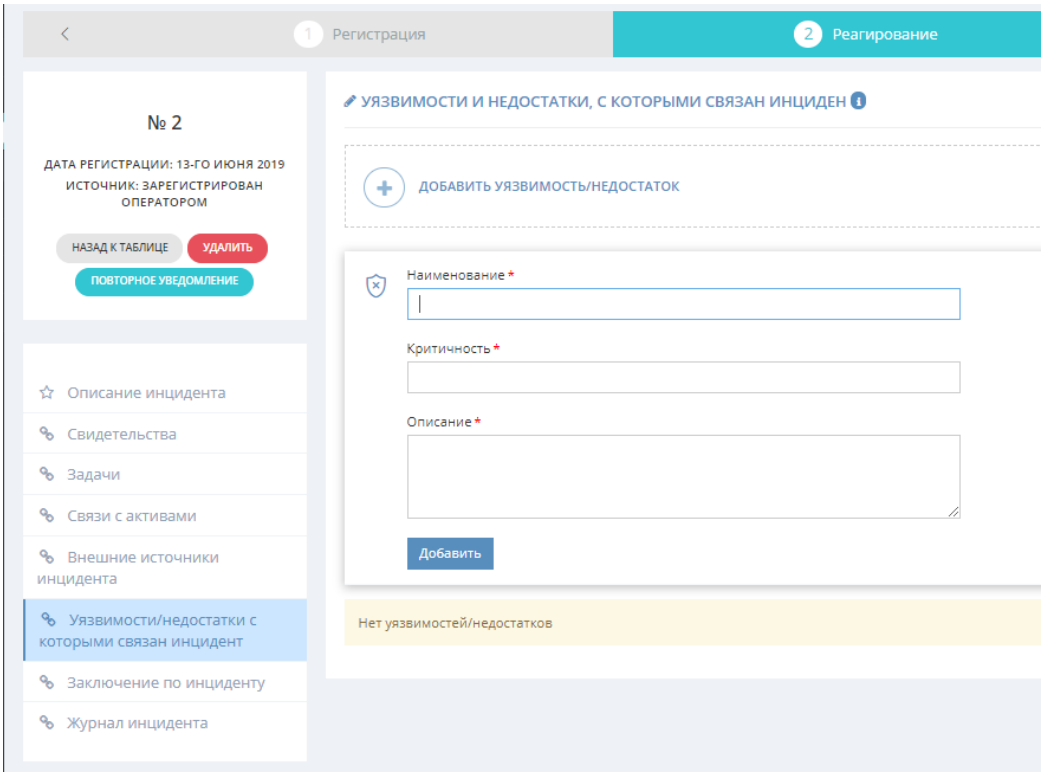

Рисунок 2.1.7 – Уязвимости, связанные с инцидентом, в онлайн-сервисе «Докшелл»

Также в системе «Докшелл» присутствует журнал инцидента (рисунок 2.1.8). Данное требование исходит от правовых регуляторов. Выгрузить печатную форму журнала не удается, т.к. в бесплатной версии системы такая возможность отсутствует.

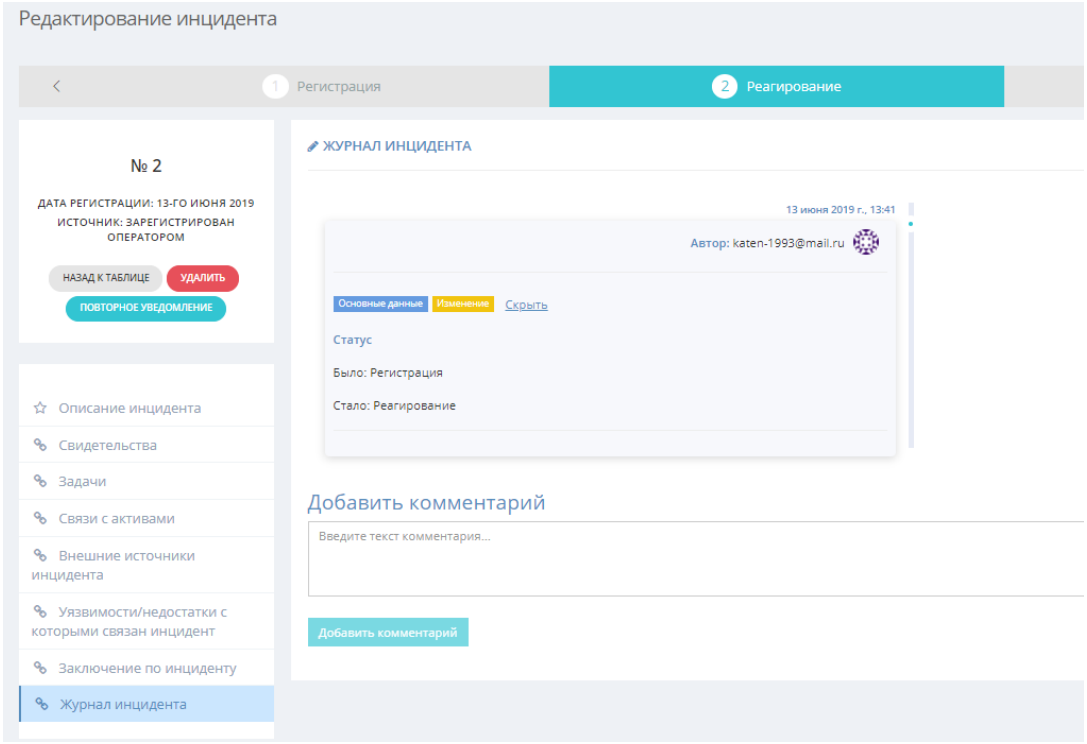

Рисунок 2.1.8 – Журнал инцидента онлайн-сервиса «Докшелл»

2.2 Выводы

Таким образом, подсистема управления инцидентами информационной безопасности по сравнению с SIEM-системами имеет ряд недостатков, такие как: недостаточность аналитики и настраиваемых полей. Также «АльфаДок» имеет достаточно большой, но не полный список выгрузки форматов документов, но при этом в системе используются часто используемые в организациях форматы.

Также система «АльфаДок» не имеет интеграции с антивирусными средствами защиты, со средствами защиты от несанкционированного доступа. При выявлении данной потребности среди пользователей реализация данного функционала возможна в будущем.

Достоинствами подсистемы является возможность демонстрации статистики в разных разрезах, а также достаточное количество информативных дашбордов.

Также большим плюсом можно выделить низкую стоимость онлайн-сервиса «АльфаДок», что делает ее доступной для множества бюджетных организаций, имеющих низкий годовой бюджет. Еще одним из достоинств является постоянная поддержка пользователей и обширная база знаний. Клиенты, обладающие низкими знаниями в данной сфере, с легкостью смогут получить необходимый комплект документов.

3. Проектирование подсистемы управления инцидентами информационной безопасности

3.1 Постановка задачи

В настоящее время в каждой ИТ-компании существует необходимость защиты от различных видов угроз информационной безопасности. Исходя из требований, указанных в международном стандарте ISO 27001: 2005, система управления инцидентами является одним из основных компонентов системы управления информационной безопасностью. Очевидно, что без своевременного обнаружения и реагирования на инциденты информационной безопасности работа системы управления информационной безопасностью становится неэффективной. С развитием информационных технологий появляются новые угрозы и, следовательно, новые инциденты информационной безопасности, а это означает, что система защиты нуждается в модернизации.

Анализ инцидентов позволяет определить слабые и устаревшие места в системе защиты, которая не может отвечать современным рискам и угрозам информационной безопасности и на основе этих данных модернизировать систему управления информационной безопасностью.

Согласно требованиями нормативно-правовых актов, а именно, приказов Федеральной службы по техническому и экспортному контролю, необходимо информировать органы исполнительной власти и случившихся инцидентах в организации, если, в организации обрабатываться ПДн или защищаемая информация [3,4].

Работа с инцидентами, которые могут негативно отразится на работе информационной системы и / или возникновению угроз безопасности персональных данных, это часть мер, необходимых для обеспечения безопасности персональных данных и защищаемой информации, содержащейся в государственных информационных системах, с учетом актуальных угроз безопасности информации и используемых информационных технологий [24].

Целью данной работы для компаний, использующий онлайн-сервис «АльфаДок», является снижение затрат на подготовку необходимой отчетности за счет ее автоматизации, и помимо этого повышение уровня практической безопасности организации.

Данный функционал можно реализовать в онлайн-сервисе «АльфаДок», который оказывает помощь в выполнении требований законодательства РФ по защите персональных данных, государственных информационных систем, и быть постоянно готовыми к проверкам регуляторов.

В сервисе осуществляется разработка профессиональной документации по защите персональных данных и информации в ГИС (МИС), электронных журналов, технической документации. Постоянная готовность к проверкам Роскомнадзора, а также ФСБ и ФСТЭК России (при выполнении технических мероприятий) позволит избежать штрафов и репутационных рисков. Система содержит обширную базу знаний, поможет разобраться в тонкостях законодательства и корректно внести данные.

Также в системе можно вести контроль подведомственных учреждений: контроль разработки документации, готовности учреждений к проверкам, сбор сведений об информационных системах, применяемых средствах защиты и многое другое [26].

3.2 Описание бизнес-процесса

Для описания бизнес-процессов управления инцидентами ИБ, используя Business Studio, было осуществлено моделирование функциональных диаграмм, основанных на технологии моделирования IDEF0 (рисунок 3.2.1).

Рисунок 3.2.1 – Контекстная диаграмма модели управления инцидентами ИБ

Процесс управления инцидентами ИБ в организации представлен в виде взаимодействия системы с окружающей средой и описывается в понятиях входа, выхода, механизмов и управления [23]. В таблице 3.2.1 представлено подробное описание значения стрелок контекстной диаграммы:

Таблица 3.2.1 –Значения стрелок контекстной диаграммы

Назначение стрелки	Название стрелки	Описание
ВХОД	Инциденты ИБ	Все сведения об инциденте ИБ
	События ИБ	Все сведения о событияхИБ
ВЫХОД	Отчеты об инцидентах ИБ	Сводные таблицы об инцидентах ИБ организации, генерируемые онлайн-сервисом «АльфаДок»
	Отчеты о событиях ИБ	Сводные таблицы событий ИБ, генерируемые системой «АльфаДок» на основе данных, вводимых сотрудниками организации, которые были задействованы в произошедшем событии ИБ
	Принятые меры	Действия, осуществленные в организации для устранения/предотвращения инцидентов ИБ
УПРАВЛЕНИЕ	Регламент реагирования на инциденты ИБ	«…документ, в котором указаны действия сотрудников организации при возникновении инцидента ИБ» [23]
	Устав организации	Содержит правила, определяющие порядок функционирования организации
	Приказ ФСТЭК России от 18 февраля 2013 г. № 21	Содержит основные требования по защитеперсональных данных
	Приказ ФСТЭК России от 11 февраля 2013 г. № 17	Содержит основные требования по защите информации, содержащейся в государственных информационных системах
	Международные, национальные и отраслевые стандарты в области ИБ	Содержат рекомендательные действия и правила по реагированию на инциденты ИБ в информационных системах
МЕХАНИЗМ	Операторы, осуществляющие обработку ПДн	«…государственный, муниципальный орган, юридическое или физическое лицо, организующее и/или осуществляющее обработку ПДн, а также определяющее цели и содержание обработки персональных данных» [1]
	Операторы государственных информационных систем	«…государственный, муниципальный орган, юридическое или физическое лицо, организующее и/или осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных» [2]
	Ответственный за выявление инцидентов ИБ и реагирование на них	Сотрудник организации/предприятия, который несет ответственность за выявление инцидентов в организации и реагирование на них
	Сотрудники	Сотрудники организации, которые могут иметь косвенное или прямое отношение к инциденту ИБ
	Комиссия по расследованию инцидентов ИБ	Сотрудники, выполняющие дополнительное расследования инцидента ИБ
	Ресурсы	Программное и аппаратное обеспечение, необходимое для выполнения бизнес-процесса

Основными этапами управления инцидентами ИБ являются:

– Выявление лиц, ответственных за выявление инцидентов и реагирование на них – в организации, обрабатывающей ПДн, и другой информации, которая не содержит сведений, составляющих государственную тайну, необходимо определить ответственного

лица, которое будет принимать решения при возникновении инцидентов. Чаще всего в этот список входят лица, ответственные за обеспечение безопасности защищаемой информации, а также специалисты по информационным технологиям (программисты, системные администраторы и т. д.). Процесс определения лиц, ответственных за выявление и реагирование на инциденты, основан на списке сотрудников.

– Обнаружение, идентификация и регистрация инцидентов – сотрудник организации, при обнаружении события ИБ оповещает Ответственногоза выявление инцидентов и реагирование на них (далее – Ответственный) посредством звонка, отправки сообщения по почте, регистрации события в системе и т.д. После регистрации события ИБ сотрудником или самим Ответственным, проводится исследование и событие ИБ либо определяется как инцидент ИБ и регистрируется в системе, либо, если инцидентом не является, в системе не регистрируется [23].

– Анализ инцидентов информационной безопасности – этот этап включает в себя процесс расследования и получения дополнительной информации об инциденте информационной безопасности. Ответственное лицо определяет тип инцидента из Справочника инцидентов ИБ, назначает приоритет и статус. При необходимости проводится юридическая экспертиза [23].

– Принятие мер по устранению последствий инцидентов ИБ – после проведения подробного анализа необходимо принятие мер по устранению инцидента и его последствий. Меры могут выполняться как самим Ответственным, так и другими сотрудниками организации. При невозможности разрешения инцидента, проводится его эскалация и назначается Комиссия по расследованию инцидентов ИБ для принятия последующих мер[23].

– Планирование и принятие мер по предотвращению повторного возникновения инцидента ИБ – чтобы снизить затраты и риски повторного возникновения инцидентав последующем, необходимо спланировать и принять соответствующие меры.

Этапы управления инцидентами ИБ графически показаны на рисунке 3.2.2.

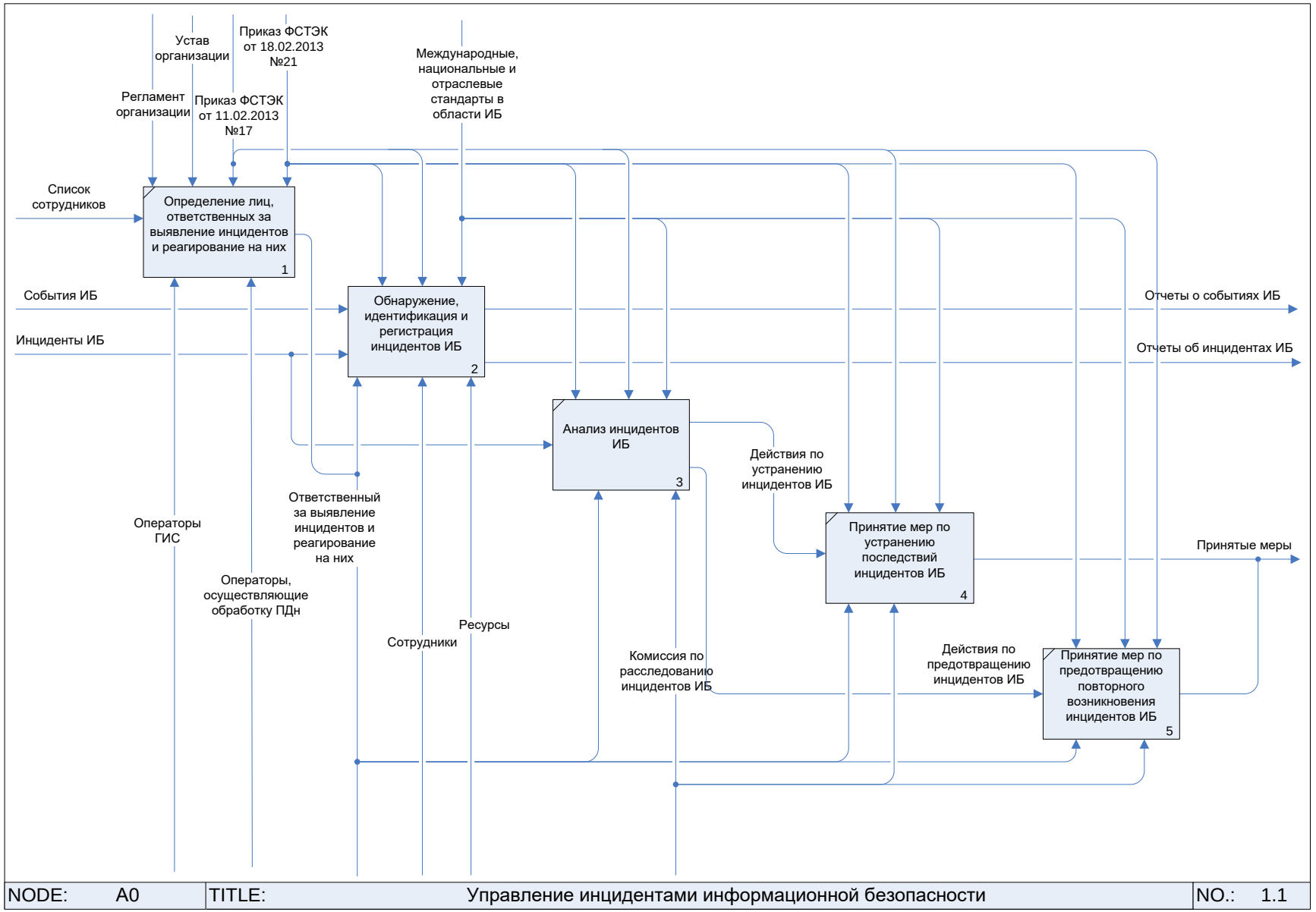

Рисунок 3.2.2 – Декомпозиция процесса управления инцидентами ИБ

Рассмотрим типовой процесс управление инцидентами ИБ в организации с использованиемонлайн-сервиса «АльфаДок».

После того, как в организации произошло событие, не свойственное информационной системе, сотрудник информационной безопасности, авторизованный в системе «АльфаДок», вводит информацию об этом событии. Для регистрации событий необходимо выбрать тип из справочникасобытий информационной безопасности, описать подробные данные, предоставить информацию о событиях и времени событий, определить самостоятельно уровень критичности, описать элементы информационной системы, на которые повлияли эти события. Также возможно прикрепить снимок экрана, дополнительные файлы системы,если событие произошло на рабочем месте сотрудника.

После внесения необходимых данных, онлайн-сервис «АльфаДок»генерирует и отправляет уведомление наадрес почтового ящика Ответственногоо том, что созданособытие ИБ.

Получив уведомление, Ответственное лицо проводит разбирательство по событию инцидента и определяет, является ли это событие инцидентом информационной безопасности. Если в ходе расследования выясняется, что событие не является инцидентом информационной безопасности, то запрос сотрудника закрывается, в системе со статусом события «Закрыто». Если событие оказывается инцидентом ИБ, Ответственное лицо делает такую отметку и, при необходимости, вносит дополнительную информацию в системе. Затем создается запись в реестре инцидентов информационной безопасности. В случае если зарегистрированный инцидент ИБ был классифицирован как «Критический» или «Высокий», Ответственное лицо обязано немедленно уведомить ИБ, ответственное за обеспечение безопасности защищенной информации, по электронной почте или другим средствам связи для последующего анализа этого инцидента.

Лицо, ответственное за обеспечение безопасности защищенной информации, должно провести внеплановый анализ идентифицированного инцидента ИБ и, при необходимости, инициировать процедуру внутреннего расследования и уведомить высшее руководство об инциденте ИБ.

Для устранения инцидента ИБ и / или его последствий Ответственное лицо составляет список действий, которые необходимо предпринять. Действия регистрируются в системе, после чего отправляется уведомление лицам, имеющим отношение к инциденту ИБ. При необходимости Ответственный может передать расследование инцидента ИБ в Комиссию по расследованию ИБ, которая, в свою очередь, составляет собственный перечень необходимых мер. Действия могут быть выполнены Ответственным, сотрудниками организации или, при обращении, сторонними организациями.

После того, как инцидент взят на контроль, в системе сотрудником, создавшим событие, которое было отмечено как инцидент ИБ, ставится отметка о закрытии инцидента ИБ, инциденту присваивается статус «Закрыто».

Для предотвращения повторного возникновения инцидента ИБ в будущем, Ответственный планирует соответствующий перечень мер, которые необходимо принять в организации.

Вышеописанный типовой процесс показан на рисунке 3.2.3:

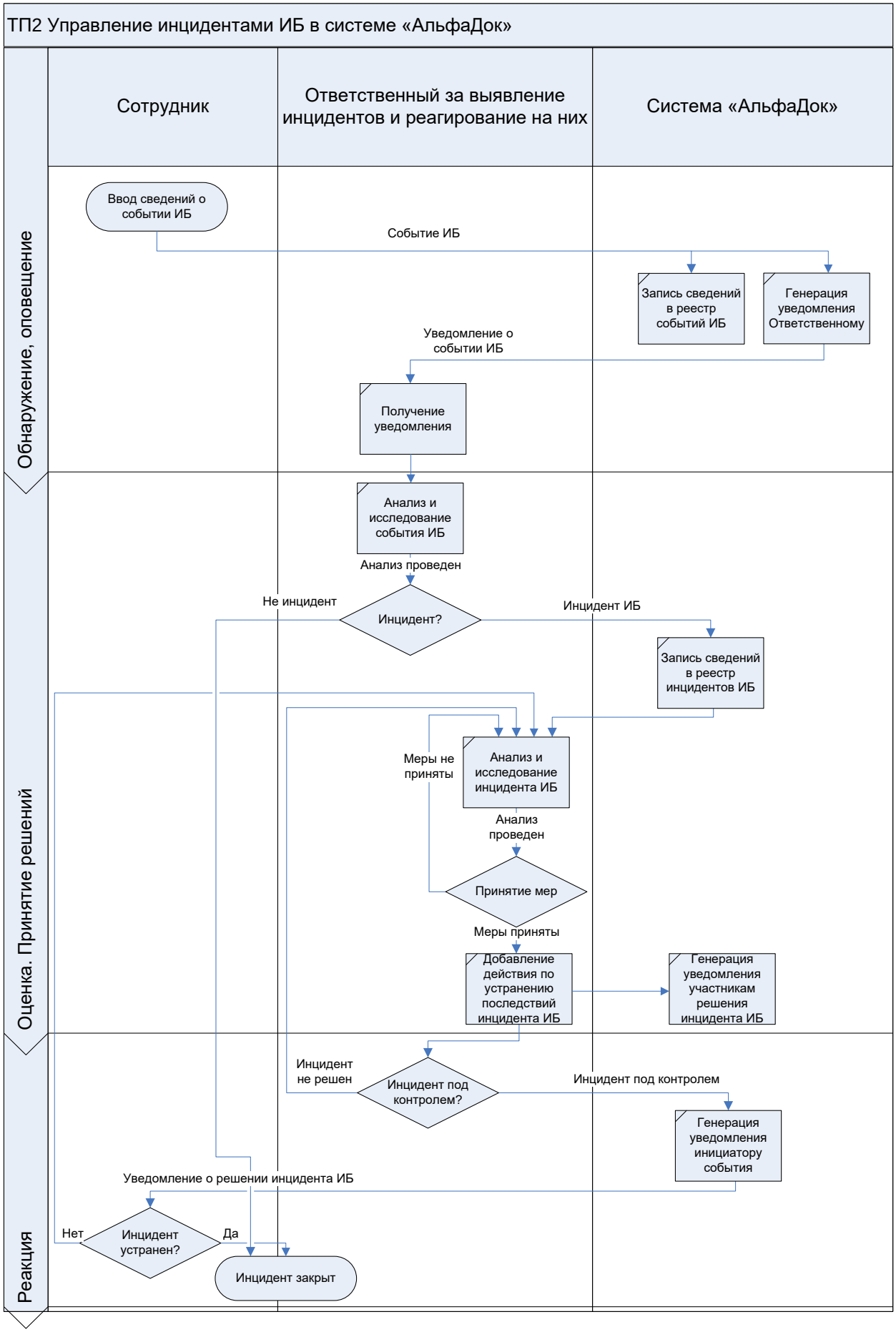

Рисунок 3.2.3 – Диаграмма последовательности действий в нотации «Процедура»

3.3 Выявление заинтересованных сторон

Необходимость выявления заинтересованных сторон, участников проекта заключается в том, что у каждого участника есть свои интересы, которые так или иначе могут влиять на планируемые изменения в системе. Важно учитывать все потребности, чтобы избежать конфликтов и найти компромисс в дизайне системы. Таблица 3.3.1 описывает заинтересованные стороны проекта.

Таблица 3.3.1 – Заинтересованные стороны проекта

№ п/п	Заинтересованная сторона	Представитель	Интересы	Влияние	Обязательства
1	2	3	4	5	6
1.	Компания разработчик	Руководитель организации	Привлечение большего числа клиентов	Имеет возможность предоставить дополнительные ресурсы для достижения цели	Разработка системы в соответствии с требованиями законодательства Российской Федерации и со стандартами информационной безопасности
2.	Головная организация	Руководитель головной организации	Выполнение требований приказов ФСТЭК № 21 от 18 февраля 2013 г. и № 17 от 13 февраля 2013 г.; Защита прав организации		Ведение статистики инцидентов ИБ; Осуществление контроля над подведомственными организациями по ведению документации по инцидентам ИБ
3.	Подведомственная организация	Руководитель подведомственной организации	Выполнение требований приказов ФСТЭК № 21 от 18 февраля 2013 г. и № 17 от 13 февраля 2013 г.; Выполнение требований головной организации; Защита прав организации		Ведение статистики инцидентов ИБ; Ведение документации по инцидентам ИБ
4.	Подведомственная организация	Ответственный за выявление инцидентов и реагирование на них	Сокращение нагрузки при сборе информации об инциденте ИБ; сокращение нагрузки при составлении отчета о событии / инциденте ИБ	Будущий непосредственный пользователь системы	Осуществление ввода сведений о событии / инциденте ИБ; Осуществление контроля над инцидентами ИБ

Продолжение таблицы 3.3.1

1	2	3	4	5	6
5.	Подведомственная организация	Ответственный за обеспечение безопасности защищаемой информации	Сокращение нагрузки при сборе информации об инциденте ИБ; сокращение нагрузки при составлении отчета о событии/ инциденте ИБ	Будущий непосредственный пользователь системы	Расследование инцидента ИБ Осуществление настройки и сопровождения всех программных и технических средств защиты ИС
6.	Подведомственная организация	Сотрудник подведомственной организации	Сокращение нагрузки при составлении отчета о событии/инциденте ИБ	Будущий непосредственный пользователь системы	Осуществление ввода сведений о событии /инциденте ИБ

Далее мы рассмотрим функции пользователей в системе, когда они распределены по ролям и их взаимодействие друг с другом.

В результате анализа заинтересованных сторон можно выделить следующее распределение по ролям:

1) Сотрудник подведомственной организации;

2) Ответственный за выявление инцидентов и реагирование на них;

3) Ответственный за обеспечение безопасности защищаемой информации;

4) Сотрудник головной организации.

Сотрудник подчиненной организации выполняет ввод первичной информации в систему: он вводит информацию о времени и месте события ИБ, при каких обстоятельствах это произошло, с возможным дополнительным описанием. Используя онлайн-сервис «АльфаДок», взаимодействие с Ответственным осуществляется посредством уведомления о создании нового события информационной безопасности.

Лицо, ответственное за выявление инцидентов, после сбора информации дополняет информацию, идентифицирующую тип инцидента ИБ. При необходимости ответственным лицам назначаются задачи, которые должны выполнять сотрудники организации для реализации мер, предпринятых для устранения / предотвращения инцидента ИБ и его последствий. Ответственное лицо может назначить комиссию по расследованию инцидентов ИБ из числа сотрудников организации или иных уполномоченных лиц.

По внесенным записям в реестр событий и инцидентов ИБможно вести статистическая информация, которую при необходимости может просмотреть Сотрудник головной организации. Например, ведениеучета инцидентов ИБ, произошедших в

организации за определенный период или ход выполнения мер, принятых для его устранения.

3.4 Требования к подсистеме

В сервисном режиме подсистема должна обеспечивать следующую работу:

– регистрацию событий и инцидентов ИБ;

– возможность формированияотчетовсобытий и инцидентовИБ;

– возможность формированияграфического отображения статистики по инцидентамИБ в организации;

– оповещение ответственных лиц по происшествию события ИБ.

Ролевая модель должна отражать потребности и полномочия различных пользователей.

В части регистрации запросов подсистемадолжна обеспечивать:

– один общий пункт приема и регистрации всех запросов и обращений пользователей, связанных с появлением событий ИБ на их автоматизированных рабочих местах (далее – запросы), в общей базе данных, в которой хранится вся информация о всех запросах;

– регистрацию запроса с помощью веб-приложения в системе;

– отображениеинформации об уже открытых запросах текущего пользователя при создании нового запроса;

– регистрацию заявок по электронной почте. Адреса назначенных почтовых ящиков должны задаваться в настройках системы;

– регистрацию запросов с использованием специального программного обеспечения, которое отслеживает действия пользователя на автоматизированном рабочем месте пользователя;

– собственный веб-интерфейс и средства интеграции с внешним личным аккаунтом, которые позволяют пользователям регистрировать запросы, просматривать данные по их запросам, подтверждать завершение своих запросов;

– использование справочников событий и инцидентов ИБ для качественного заполнения и изменения записей запросов в базе данных при помощи карточек запросов:

- идентификация пользователя, регистрирующего запрос;
- идентификация возможных для пользователя услуг;
- идентификация текущих обращений пользователя;

– категоризацию и определение других необходимых параметров, обеспечивающих управление запросами, в частности:

- функциональное воздействие;
- информационное воздействие;
- приоритет запроса;
- статус запроса;
- регламентный срок обработки запроса;

– возможность ввода дополнительных параметров для более подробного описания запроса с возможностью определения обязанности их заполнения при регистрации (и при последующей обработке запросов);

– возможностьнастраивать порядок запросов;

– возможность прикреплять к запросу файлы различных форматов.

В части закрытия запросов подсистема должна обеспечивать:

– при закрытии запроса подсистема должна предоставлять возможность ввода возможного решения:

- запрос подтверждения от пользователя, что запрос решен;
- ввод описания с помощью добавления текста;
- выбора описания результата решения из списка описаний типичных решений;
- выбора описания результата решения;
- создание задач на устранение инцидента ИБ;

– автоматическое оповещение пользователей о завершении обработки их запросов с возможностью подтверждения или опровержения успеха решения непосредственно в подсистеме управления инцидентами ИБ;

– если невозможно получить подтверждение от пользователя, подсистема должна автоматически закрыть запрос через определенный промежуток времени. Запрос на автоматическое закрытие на определенное время, чтобы повторить попытку получения подтверждения.

В части прохождения запросов подсистемадолжна предоставлять:

– средства для внесения дополнительной информации и изменения приоритета запроса на протяжении всего жизненного цикла запроса (после его первичной регистрации до момента закрытия) [18];

– ручную и автоматическую передачу запроса для его решения в персональную ответственность Ответственному за обеспечение безопасности защищаемой информации;

– информацию об уже имеющихся запросах, известных проблемах, которые подобны (аналогичны) вновь поступившим, и способах их решения;

– средства отслеживания детальной истории событий по каждому запросу;

– графическое представление жизненных циклов запросов в виде диаграмм на экранных формах запросов;

– средства ведения списка комментариев по запросу, в общих чертах (видимых, в том числе и для самого пользователя).

В части контроля выполнения регламентов по запросам подсистемадолжна обеспечивать:

– обслуживание запросов, определение максимального времени устранения запроса, с учетом приоритета обратившегося сотрудника;

– контроль времени начала и завершения работ по каждому запросу;

– учет общего времени обработки запроса в сервисе «АльфаДок»;

– учет времени обработки в каждом из состояний и каждым из ответственных специалистов;

– рассылку уведомлений по электронной почте и в сервисе «АльфаДок», в соответствии со сделанными настройками (по событиям, по регламентным срокам).

3.5 Проектирование и построение базы данных

Для проектирования базы данных был выбран пакет MS SQL Server 2014. Пакет MS SQL Server 2014позволяет в полной мере для базы данных описать всю ее логическую структуру.

«…Система программирования MS SQL Server 2014 относится к классу суперкомандных систем. Единицей действий являются команды, которые выполняются в режиме интерпретации, как только они поступают на сервер. Основой этой системы является проблемно-ориентированный структурированный язык» [21].

SQL Server предоставляет набор системных типов данных. Данные могут храниться в объекте: целые числа, символы, данные типа денег, двоичные строки и т. д. [21].

Описание функций базы данных:

1) Подсистемадолжна регистрировать и хранить события информационной безопасности, произошедшие в организации.

2) Подсистемадолжна регистрировать и хранить информацию о том, какой сотрудниккакое событие ИБ создал.

3) Подсистемадолжна хранить всю отчетность по событиям и инцидентам ИБ.

4) Подсистемадолжна регистрировать и хранить информацию о том, какой сотрудник, какую задачу выполняет.

5) Подсистемауправляет приоритетамисобытий и инцидентов ИБ.

6) Подсистемауправляет списком сотрудников с указанием должностей и отделов, в которых они состоят.

7) Подсистемахранит информацию о типах событий и инцидентов ИБ, причинах возникновения, описании, последствиях инцидентов ИБ.

8) Подсистема хранит информацию о действиях, необходимых для устранения инцидента ИБ.

Из перечня функций базы данных составим перечень сущностей.В ходе проведения инфологического моделирования в области данных было выявлено четыре сущности:

1) ИнцидентыИБ;
2) Сотрудники;
3) Комиссия;
4) Действия.

Сформируем перечень атрибутов и первичные ключи для каждой сущности и занесем их в таблицу 3.5.1, где PK–Primary key, FK–Foreign key:

Таблица 3.5.1 – Основные объекты проектируемой базы данных

Сущность	**Атрибуты**
1	**2**
Инциденты ИБ	Код события/инцидента ИБ
	Номер события ИБ
	ФИО инициатора
	Состояние события ИБ
	Тип события/инцидента ИБ
	Признак инцидента
	Приоритет события ИБ
	Дата и время возникновения события/инцидента ИБ
	Дата и время выявления события/инцидента ИБ
	Дата и время завершения разбирательства
	Информационная система
	Территориальные подразделения
	Информационное воздействие
	Функциональное воздействие
	Тип угрозы
	Наименование угрозы
	Описание инцидента ИБ
	Причины инцидента ИБ
	Понесенные убытки
	Источник информации
	Последствия
	Файл события ИБ
	Дополнительно

Продолжение таблицы 3.5.1

1	2
Сотрудники	Код сотрудника
	ФИО
	Структурное подразделение
	Должность
	Номер телефона
Комиссия	Код комиссии
	ФИО
	Должность
	Роли членов комиссии
Действия	Код действия
	Наименование действия
	Описание действия
	Исполнитель
	Дата выполнения
	Статус действия
	Фактическая дата выполнения
	Код инцидента

Представим модель сущность-связь для разрабатываемой подсистемы (рисунок 3.5.1):

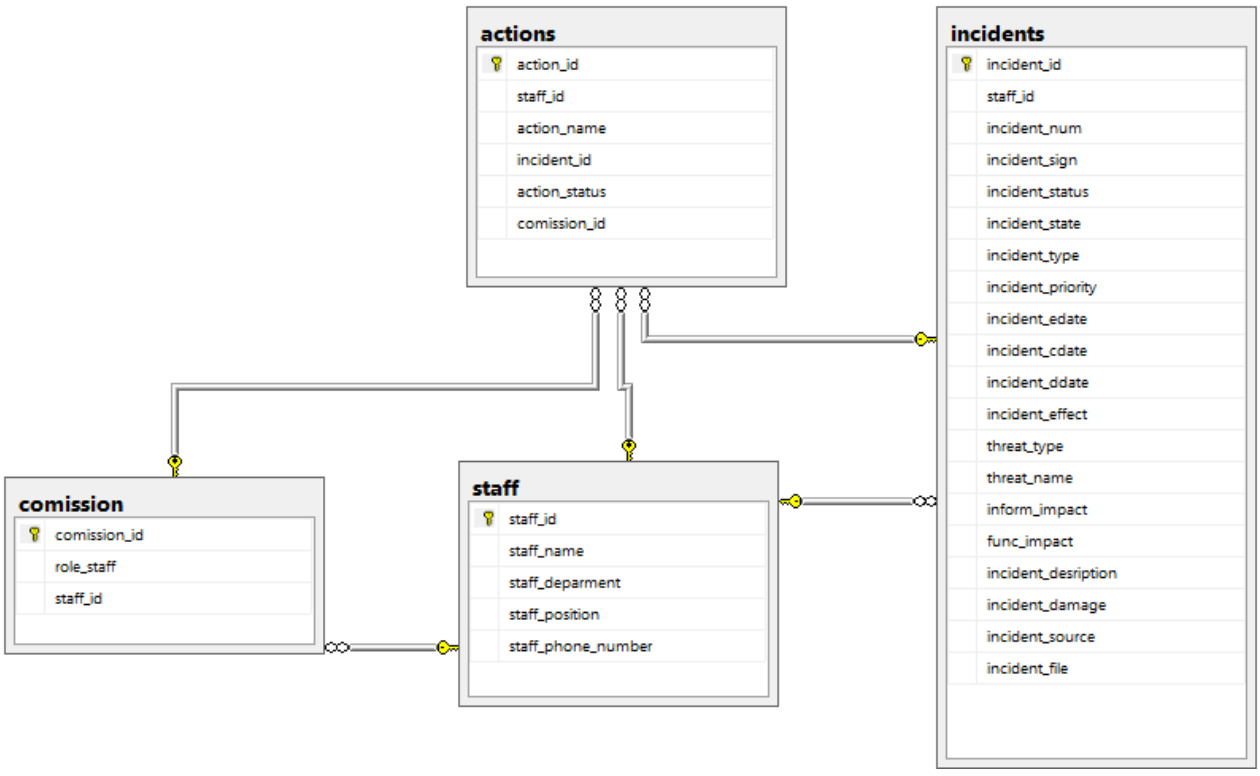

Рисунок 3.5.1 – ER-диаграмма базы данных

Перейдем к физической реализации структуры баз данных для СУБД MS SQL Server 2014.

Определим физические характеристики хранимых записей: типа значений и требуемого объема для хранения значений в памяти.Описание данных, хранимых в таблицах удаленной базы данных SQL Server, можно представить в виде таблиц 3.5.2 – 3.5.5:

Таблица 3.5.2 – Структура таблицы «Инциденты» (incidents)

Название поля	Описание	Тип поля	Дополнительно
1	2	3	4
incident_id	Код события/инцидента ИБ	int	Первичный ключ
staff_id	Код сотрудника	int	Внешний ключ
incident_num	Порядковый номерсобытия /инцидента ИБ	int	Присваивается автоматически
incident_sign	Признак инцидента	bit	Да/Нет
incident_state	Состояние, показывающее, на какой стадии находится рассмотрение события ИБ. Выбирается из списка заданных значений	varchar(15)	Выпадающий список
incident_status	Статус инцидента ИБ. Выбирается из списка заданных значений		Выпадающий список
incident_type	Тип события/инцидента ИБ. Выбирается из списка заданных значений	varchar(40)	Выпадающий список
incident_priority	Приоритет инцидента ИБ, определяющий порядок рассмотрения данного инцидента	varchar(10)	Определяется автоматически
incident_edate	Дата возникновения события/инцидента ИБ	date	
incident_ddate	Дата выявления события/инцидента ИБ	date	
incident_cdate	Дата завершения разбирательства по инциденту ИБ	date	
incident_effects	Последствия, повлекшие возникший инцидент ИБ. Выбирается из списка заданных значений. Возможен самостоятельный ввод	text	Выпадающий список
inform_impact	Информационное воздействие, оказанное на деятельность организации	varchar	Выпадающий список
func_impact	Функциональное воздействие, оказанное на деятельность организации	varchar	Выпадающий список
threat_type	Тип угрозы. Выбирается из списка заданных значений	varchar	Выпадающий список
threat_name	Наименование угрозы. Выбирается из списка заданных значений	varchar	Выпадающий список

Продолжение таблицы 3.5.2

1	2	3	4
incident_description	Описание инцидента ИБ. Выбирается из списка заданных значений. Возможен самостоятельный ввод	varchar	Выпадающий список
incident_reason	Причины инцидента ИБ. Выбирается из списка заданных значений. Возможен самостоятельный ввод	varchar	Выпадающий список
incident_damages	Понесенные убытки в рублях	int	
source_inform	Источник информации. Показывает, от кого получена информация об инциденте. Выбирается из списка заданных значений. Возможен самостоятельный ввод	varchar	Выпадающий список
incident_file	Файл, содержащий дополнительные сведения о событии/инциденте ИБ, например, снимки экрана, log-файлы	varbinary(max)	

Таблица 3.5.3 – Структура таблицы «Сотрудники» (staff)

Название поля	Описание	Тип поля	Дополнительно
staff_id	Код сотрудника	int	Первичный ключ
staff_name	Фамилия, имя, отчество сотрудника	varchar(60)	
staff_department	Структурноеподразделение	varchar(20)	
staff_position	Должность	varchar(20)	
staff_phone_number	Номертелефона	char(14)	

Таблица 3.5.4 – Структура таблицы «Комиссия» (comission)

Название поля	Описание	Тип поля	Дополнительно
commission_id	Код комиссии	int	Первичный ключ
staff_id	Код сотрудника	int	Внешний ключ
role_staff	Определение роли сотрудника в комиссии. Выбирается из списка заданных значений	varchar(20)	Определяется переключателем

Таблица 3.5.5 – Структура таблицы «Действия» (actions)

Название поля	Описание	Тип поля	Дополнительно
action_id	Код меры	int	Первичный ключ
action_name	Наименованиедействия по устранению последствий инцидента ИБ. Выбирается из списка заданных значений. Возможен самостоятельный ввод	varchar(50)	Выпадающий список
action_description	Описание действия, которые необходимо выполнить	varchar	
incidents_id	Код инцидента	int	Внешний ключ

Продолжение таблицы 3.5.5

1	2	3	4
action_status	Статус, показывающий, на какой стадии находится принятие мер Выбирается из списка заданных значений	varchar(20)	
action_date	Дата выполнения действия	date	
action_fdate	Фактическая дата выполнения действия	date	
action_result	Результат выполнения действия исполнителем	varchar	
staff_id	Код сотрудника	int	Внешний ключ
commission_id	Код комиссии	int	Внешний ключ

Проверочные ограничения:

1) статус события/инцидента ИБ может определяться как новый, в работе, запрос информации, разбирательство не требуется, решено, закрыт;

2) состояние события/инцидента ИБ может определяться как действительный, ошибка, подозрение;

3) для типизации инцидентов ИБ используется справочник «Типы инцидентов» (таблица 3.5.9);

4) приоритет события/инцидента ИБ может определяться как низкий, средний, высокий, критический (таблица 3.5.8);

5) последствия выбираются из списка заданных в справочнике значений;

6) информационное воздействиезаполняется значениями из справочника «Информационное воздействие» (таблица 3.5.6);

7) функциональное воздействиезаполняется значениями из справочника «Функциональное воздействие» (таблица 3.5.7);

8) описание инцидентов заполняется значениями из справочника «Описание инцидентов» (таблица 3.5.9);

9) для указания причин инцидентов используется справочник «Причины инцидентов»;

10) тип угрозы может принимать следующие значения: намеренная, случайная, ошибка, неизвестно;

11) наименование и класс угрозы описаны в справочнике «Угрозы» (таблица 3.5.10);

12) статус действий может принимать значения: новый, в работе,решено, закрыт;

13) для определения действий, необходимых для устранения последствий инцидента ИБ используется справочник «Принятые действия» (таблица 3.5.11);

14) роли сотрудников в комиссии могут быть следующие: председатель, член комиссии. Председатель в комиссии может быть только один.

Типы событий/инцидентов ИБ (справочник «Типы инцидентов»):

– DDoS-атака;
– внедрение вредоносного кода;
– вредоносная ссылка;
– компрометация учетных записей / паролей;
– кража/утеря оборудования;
– нарушение организационного характера;
– нарушение правил работы с ПДн;
– несанкционированная активность;
– несанкционированный доступ к онлайн-серверам или взлом;
– несанкционированный доступ к информации;
– несанкционированная печать ПДн /защищаемой информации;
– несанкционированное копирование ПДн /защищаемой информации;
– несанкционированный доступ к ПДн /защищаемой информации со стороны сотрудника организации;
– несанкционированный доступ к ПДн/защищаемой информации сотрудникомдругой организации;
– утечкаПДн /защищаемой информации;
– опубликование конфиденциальной информации;
– проникновение посторонних лиц на территорию организации;
– перебор паролей;
– сканирование ресурсов;
– фишинговая страница;
– эксплуатация уязвимостей ПО.

Последствия реализации инцидента ИБ:

– искажение информации/ПДн;
– нарушение доступности ИС;
– нарушение доступности информации/ПДн;
– уничтожение информации/ПДн;
– хищение информации/ПДн.

Таблица 3.5.6 – Справочник «Информационное воздействие

№ п/п	Уровень	Описание
1.	Нет воздействия	Никакая информация не была, изменена, удалена или скомпрометирована
2.	Компрометация персональных данных	Персональные данные клиентов, сотрудников и т.д. были скомпрометированы
3.	Нарушение конфиденциальности	Была нарушена конфиденциальность чувствительной для организации информации (например, информации о системе защиты критической информационной инфраструктуры)
4.	Потеря целостности	Чувствительная или конфиденциальная информации, была изменена или удалена

Таблица 3.5.7 – Справочник «Функциональное воздействие

№ п/п	Уровень	Описание
1.	Несуществующий	Нет воздействия на способность организации обеспечить все услуги всем пользователям
2.	Низкий	Минимальный эффект; организация все еще можете обеспечить все критические услуги всем пользователям, но со сниженной эффективностью
3.	Средний	Организация потеряла способность обеспечить критичные услуги для части пользователей системы
4.	Высокий	Организация не в состоянии предоставить некоторые важные услуги для всех пользователей

Таблица 3.5.8 – Приоритезация событий/инцидентов информационной безопасности

Функциональное воздействие					
	Высокий	Высокий	Критический	Критический	Критический
	Средний	Средний	Высокий	Высокий	Высокий
	Низкий	Низкий	Высокий	Высокий	Высокий
	Несуществующий	Низкий	Средний	Средний	Средний
		Нет воздействия	Компрометация ПДн	Нарушение конфиденциальности	Потеря целостности
		Информационное воздействие			

Таблица 3.5.9 – Описание инцидентов информационной безопасности

№ п/п	Описание инцидента информационной безопасности
1	**2**
1.Текущие нарушения	
1.1	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т. д.) Более трех раз подряд (за раз)
1.2	Периодические попытки неуспешного доступа к объектам: компьютерам, принтерам, файлам, документам
1.3	Несанкционированноеизменение времени на автоматизированном рабочемместе или на других элементах информационной системы Организации
1.4	Выполнение производственных обязанностей с использованием компьютернойтехники в нерабочее время
1.5	Оставление работающего компьютерного оборудования без блокирования экрана в нерабочее время
1.6	Перезагрузка рабочей станции в случае неисправности (одноразовая), включая аварийную перезагрузку, путем нажатия кнопки «горячего» сброса или полного отключения питания
1.7	Неправильное использование элементов информационной инфраструктуры организации (печать, интернет-сервисы, электронная почта и т. Д.)
2.Значимые нарушения	
2.1	Многократная при регистрации в информационной системе: ввод неправильных идентификационных регистрационных данных (пароля, имени пользователя) более трех раз подряд
2.2	Неоднократное оставление работающего компьютерного оборудования без запущенного хранителя экрана в нерабочее время
2.3	Утрата носителя конфиденциальной информации
2.4	Утрата носителя информации с резервной копией параметров информационной системы
2.5	Многократная неудачная попытка регистрации в информационной системе под чужими идентификационными данными (именем пользователя, паролем)
2.6	Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.)
2.7	Незапланированная очистка журналов событий безопасности информационных систем Организации
2.8	Несанкционированное подключение неучтенных внутренних и/или внешних устройств и носителей информации
2.9	Несанкционированное изменение аппаратной конфигурации компьютерной техники
2.10	Несанкционированное копирование информации (файлов) на носителей информации или иные внешние носители информации, а также несанкционированная передача подобной информации с использованием сервисов электронной почты, быстрых сообщений и иных сервисов Интернет
2.11	Несанкционированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах Организации
2.12	Попытка получения привилегированного доступа к автоматизированному рабочемуместу или к другим информационным ресурсам Организации (повышение уровня прав доступа, получение прав на отладку программ и т.п.)

Продолжение таблицы 3.5.9

1	2
2.12	Неумышленное заражение программного обеспечения автоматизированных рабочих мест и серверов вирусами
2.13	Несанкционированное использование сканеров
2.14	Несанкционированное использование анализаторов протоколов (снифферов)
2.15	Несанкционированный просмотр, печать, передача сторонним лицам защищаемой информации
2.16	Несанкционированное проведение обновления версий системного и прикладного программного обеспечения
3.Нарушения, имеющие признаки преступления	
3.1	Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры Организации
3.2	Несанкционированное изменение конфигурации элементов информационной инфраструктуры Организации
3.3	Утрата резервных копий
3.4	Утечка конфиденциальной информации (баз данных информационных систем и др.)
3.5	Подозрение в умышленном нарушении работоспособности информационной сети Организации, элементов информационной инфраструктуры Организации, системного и прикладного программного обеспечения
3.6	Юридически необоснованная передача (распространение) конфиденциальной информации
3.7	Несанкционированное внесение изменений в базы данных информационных систем Организации
3.8	Несанкционированное уничтожение конфиденциальной информации
3.9	Проведение обновления версии информационных систем Организации (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации
3.10	Намеренное заражение информационных систем Организации вредоносным кодом

Причины возникновения инцидента (справочник «Причины инцидентов»):

– воздействие вредоносного кода;

– запыленность помещений, в которых расположены оборудования/линии связи;

– использование неисправного оборудования/средств защиты информации /линий электросвязи;

– наличие брака в оборудовании/средствах связи;

– наличие водопроводных коммуникаций в помещения, в которых размещено оборудование/линии электросвязи;

– не установлено;

– неправильное хранение носителей защищаемой информации/ПДн;

– несоблюдение установленных правил обеспечения информационной безопасности со стороны ответственных за это лиц;

– случайное (непредумышленное) нарушение сотрудником организации;

– неэффективность используемых средств защиты информации;
– низкое качество предоставляемой энергии;
– ненадлежащая утилизация носителей защищаемой информации/ПДн;
– умышленные действия внешних нарушителей;
– умышленное нарушение сотрудником организации.

Таблица 3.5.10 – Информация об угрозе нарушения ИБ (справочник «Угрозы»)

Наименование угрозы	**Класс угрозы**	
1	**2**	
Вредоносное программное обеспечение	Индикаторы компрометации (IOC) (в случае наличия)	В формате Yara (если есть)
		В формате Open IOC (если есть)
		В формате XML (если есть)
		Иные форматы
	Антивирусные решения, детектирующие ВПО	Достаточно указать, детектирует ли установленное у участника обмена антивирусное
	Присутствуют ли данные IOC в бюллетенях Центра мониторинга и реагирования на компьютерные атаки	Да (указать идентификатор рассылки)/Нет
Эксплуатация уязвимости	Идентификатор уязвимости	Стандартизированный
	Описание методики эксплуатации (если есть)	Допускается ссылка на POC (proof of concept) уязвимости
DDoS	Атакующие IP адреса	
	Тип атаки	
	Прогнозируемое усиление (если есть)	
	Прогнозируемая мощность (если есть)	
Центр управления бот-сети	IP-адрес или доменное имя	
	Тип и общие сведения о бот-сети	
	Каким образом выявлен	
Фишинг	IP-адрес или доменное имя ресурса	
	Дата обнаружения ресурса	
	Технические заголовки письма (если есть)	
	Текст письма (если есть)	
Вредоносный ресурс	IP-адрес или доменное имя ресурса	
	Дата обнаружения ресурса	
	Причины, почему ресурс подозревается вредоносным	
Хищение	Объект хищения	
	Сумма хищения (если есть)	
Мошенничество	-	
Саботаж/физический ущерб	Объект, которому нанесли ущерб	
	Сумма ущерба (если есть)	
Спам	-	

Таблица 3.5.11 – Справочник «Принятые действия»

№ п/п	**Наименование действия**
1	**2**
1. Взаимодействие с третьими лицами	
1.1	Обращение в правоохранительные органы

Продолжение таблицы 3.5.11

1	2
1.2	Оповещение провайдера телекоммуникационных услуг
1.3	Привлечение сторонней организации для проведения расследования инцидента ИБ
1	**2**
2. Восстановительные действия	
2.1	Восстановление системы/данных из резервных копий
2.2	Замена вышедшего из строя оборудования
2.3	Перезапуск (перезагрузка) общесистемного прикладного программного обеспечения
2.4	Переключение на резервные мощности (ЦОД/сервер/канал связи и т.д.)
2.5	Переустановка скомпрометированных систем из надежных источников
3.Действия по сбору дополнительных сведений	
3.1	Дополнительный мониторинг активности пользователей / операций
3.2	Проведение анализа уязвимостей
3.3	Проведение антивирусной проверки
3.4	Проведение служебного расследования
3.5	Сбор лог-файлов и других свидетельств инцидента
4. Корректирующие действия	
4.1	Аварийное выключение прикладных систем
4.2	Блокирование скомпрометированных учетных записей
4.3	Корректировка настроек коммутационного оборудования
4.4	Корректировка настроек общесистемного и прикладного программного обеспечения
4.5	Корректировка средств защиты информации
4.6	Обновление общесистемного и прикладного программного обеспечения
4.7	Обновление программного обеспечения средств защиты информации
4.8	Смена аутентификационной информации (пароли, ключи доступа)
5. Общеорганизационные действия	
5.1	Проведение служебного расследования
5.2	Проведение повторного инструктажа сотрудников организации по обеспечению информационной безопасности в организации
5.3	Уведомление высшего руководства организации
5.4	Удаленная очистка содержимого мобильного устройства сотрудника
5.5	Удаленная очистка содержимого персонального компьютера сотрудника
5.6	Уничтожение информации/носителей информации
5.7	Эвакуация персонала

СоздадимбазуданныхDB_Incidents, содержащуюописанныевышетаблицы:staff, commission, tasks, incidents, actions.

```
useDB_Incidents
CREATETABLEstaff(
	staff_idINTPRIMARYKEY,
	staff_nameVARCHAR(60)		NOTNULL,
	staff_deparmentVARCHAR(20)	NOTNULL,
	staff_positionVARCHAR(20)	NOTNULL,
	staff_phone_numberCHAR(14)	NOTNULL)
CREATETABLEcomission(
	comission_idINTPRIMARYKEY,
	role_staffVARCHAR		NOTNULL
		CHECK (role_staffLIKE'Председатель'ORrole_staffLIKE'Членкомиссии'),
	staff_idINTFOREIGNKEYREFERENCES staff(staff_id))
CREATETABLEincidents(
	incident_idINTPRIMARYKEY,
	staff_idINTFOREIGNKEYREFERENCES staff(staff_id),
	incident_numINT			NOTNULL,
	incident_signBIT		NULL,
```

```
        incident_statusVARCHAR              NOTNULL,
               CHECK (incident_statusLIKE'Новый'ORincident_statusLIKE'Вработе'OR
        incident_statusLIKE'Запросинформации'
               ORincident_statusLIKE'Решено'OR          incident_statusLIKE'Закрыт'),
        incident_stateVARCHAR               NULL,
               CHECK (incident_stateLIKE'Действительный'ORincident_stateLIKE'Попытка'
               ORincident_stateLIKE'Подозрение'),
        incident_typeVARCHAR        NOTNULL,
        incident_priorityVARCHAR            NOTNULL
               CHECK (incident_priorityLIKE'Низкий'ORincident_priority
               LIKE'Средний'ORincident_priorityLIKE'Высокий'ORincident_priority
               LIKE'Критический'),
        incident_edateDATETIME              NOTNULL,
        incident_cdateDATETIME              NOTNULL,
        incident_ddateDATETIME              NULL,
        incident_effectVARCHAR              NULL,
        threat_typeVARCHAR                  NULL,
               CHECK (threat_typeLIKE'Намеренная'ORthreat_typeLIKE'Случайная'OR
               threat_typeLIKE'Ошибка'ORthreat_typeLIKE'Неизвестно'),
        threat_nameVARCHAR                  NULL
               CHECK (threat_nameLIKE'ВредоносноеПО'ORthreat_name
               LIKE'Эксплуатацияуязвимости'ORthreat_nameLIKE'DDoS'ORthreat_name
               LIKE'Центруправлениябот-сети'ORthreat_nameLIKE'Фишинг'
               ORthreat_nameLIKE'Вредоносныйресурс'ORthreat_nameLIKE'Спам'
               ORthreat_nameLIKE'Другое'),
        inform_impactVARCHAR        NOTNULL
               CHECK (inform_impactLIKE'Нетвоздействия'ORinform_impact
               LIKE'КомпрометацияПДн'ORinform_impactLIKE'Нарушениеконфиденциальности'
        ORinform_impactLIKE'Потеряцелостности'),
        func_impactVARCHAR                  NOTNULL
               CHECK (func_impactLIKE'Несуществующий'ORfunc_impactLIKE'Низкий'OR
        func_impactLIKE'Средний'ORfunc_impactLIKE'Высокий'),
        incident_desriptionVARCHAR          NULL,
        incident_damageINT                  NULL,
        incident_sourceVARCHAR              NULL,
        incident_fileVARBINARY              NULL)
CREATETABLEactions(
        action_idINTPRIMARYKEY,
        staff_idINTFOREIGNKEYREFERENCES staff(staff_id),
        action_nameVARCHAR(20)              NOTNULL,
        incident_idINTFOREIGNKEYREFERENCES incidents(incident_id),
        action_statusVARCHAR        NOTNULL,
               CHECK (action_statusLIKE'Новый'ORaction_statusLIKE'Вработе'OR
        action_statusLIKE'Выполнено'),
        comission_idINTFOREIGNKEYREFERENCEScomission(comission_id))
```

Для наглядности заполним таблицы данными с помощью запроса. Заполнимполятаблицы«Сотрудники»:

```
useDB_Incidents
insertintostaffValues
(001,'Иванов Иван Иванович','ОтделИТ','Инженер ИБ',325),
(002,'Николаев Алексей Васильевич','Отделмаркетинга','Начальник ОМ',105),
(003,'Петров Павел Борисович','Отдел маркетинга','Специалист',324),
(004,'Максимов Денис Вадимович','ОтделИТ','Начальник отдела ИТ',100),
(005,'Курочкин Леонид Александрович','ОтделИТ','Инженер ИБ',103)
```

Заполненная таблица выглядит следующим образом (рисунок 3.5.2):

staff_id	staff_name	staff_deparment	staff_position	staff_phone_n...
1	Иванов Иван Иванович	Отдел ИТ	Инженер ИБ	325
2	Николаев Алексей Васи...	Отдел маркетинга	Начальник ОМ	105
3	Петров Павел Борисович	Отдел маркетинга	Специалист	324
4	Максимов Денис Вадим...	Отдел ИТ	Начальник отдела ИТ	100
5	Курочкин Леонид Алекс...	Отдел ИТ	Инженер ИБ	103
NULL	*NULL*	*NULL*	*NULL*	*NULL*

Рисунок3.5.2– Заполненнаятаблица «Сотрудники»

Заполнимполятаблицыcommissionспомощьюзапроса:

```
useDB_Incidents
insertintocomissionValues
(100,'Председатель',004),
(101,'Членкомиссии',001),
(102,'Член комиссии',005)
```

Заполненная таблица выглядит следующим образом (рисунок 3.5.3):

comission_id	role_staff	staff_id
100	Председатель	4
101	Член комиссии	1
102	Член комиссии	5
NULL	*NULL*	*NULL*

Рисунок 3.5.3– Заполненная таблица «Комиссия»

Заполним поля таблицы «Инциденты» с помощью запроса:

```
useDB_Incidents
insertintoincidentsValues
(200,001,1,1,'Закрыт','Действительный','внедрение вредоносного кода','Высокий',
'2017-04-01 12:00','2017-04-01 12:00','2017-04-01 16:30','Хищение информации',
'Намеренная','ВредоносноеПО','Потеряцелостности','Средний','Заражение программного
обеспечения рабочих станций и серверов вредоносным кодом',30000,'ESET NOD32',NULL),
(201,002,2,0,'Закрыт',NULL,'другое','Низкий','2017-05-05 07:00','2017-05-05 13:03',NULL,
NULL,NULL,NULL,'Нетвоздействия','Несуществующий',NULL,NULL,'Сотрудник',NULL),
(202,003,3,1,'В работе',NULL,'компрометация учетных записей или паролей','Средний',
'2017-04-25 01:34','2017-04-26 08:03','2017-04-26 10:00','Нарушение доступности
ИС','Неизвестно','Другое','Нетвоздействия','Низкий','Ошибка при регистрации в
информационной системе: ввод неправильных персональных регистрационных данных (пароля,
имени пользователя и т.п.) более трех раз подряд',0,'Сотрудник',NULL)
```

Заполненная таблица представлена на рисунке 3.5.4:

incident...	staff...	incid...	inciden...	incident_st...	incident_state	incident_type	incident_pr...	incident_edate	incident_cd...	incident_d...	incident_eff...	threat_ty...	threat_name
200	1	1	True	Закрыт	Действительн...	внедрение вр...	Высокий	2017-04-01	2017-04-01	2017-04-01	Хищение ин...	Намерен...	Вредоносное ...
201	2	2	False	Закрыт	NULL	другое	Низкий	2017-05-05	2017-05-05	NULL	NULL	NULL	NULL
202	3	3	True	В работе	NULL	компромета...	Средний	2017-04-25	2017-04-26	2017-04-26	Нарушение ...	Неизвест...	Другое
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Рисунок 3.5.4 – Заполненная таблица «Инциденты»

Заполним поля таблицы «Действия» с помощью запроса:

```
useDB_Incidents
insertintoactionsValues
(300,001,'Обновить базы данных сигнатуры вирусов',200,'Выполнено',NULL),
(301,001,'Провести дополнительную проверку сервера и рабочих
станций',200,'Выполнено',NULL),
(302,005,'Провести восстановление доступа к ИС',202,'Выполнено',NULL)
```

Заполненная таблица представлена на рисунке 3.5.5

action_id	staff_id	action_name	incident_id	action_status	comission_id
300	1	Обновить базы данных сигнатуры вирусов	200	Выполнено	NULL
301	1	Провести дополнительную проверку сервера и рабочих станций	200	Выполнено	NULL
302	5	Провести восстановление доступа к ИС	202	Выполнено	NULL
NULL	NULL	NULL	NULL	NULL	NULL

Рисунок 3.5.5 – Заполненная таблица «Действия»

Для просмотра инцидентов, которые были решены и закрыты в Организациис указанием сотрудника, создавшего инцидент,создадим представление «closed_incident», используя следующий запрос:

```
CREATEVIEW closed_incident AS
SELECTincident_cdate,incident_status,incident_type,incident_desription,incident_effect,st
aff_name
FROM incidents i, staff s
WHEREi.staff_id=s.staff_idANDincident_status='Закрыт'
```

В результате получим следующую выборку (рисунок 3.5.6):

incident_cdate	incident_status	incident_type	incident_desription	incident_effect	staff_name
2017-04-01	Закрыт	внедрение вредоносного кода	Заражение программного обеспечения рабочих станц...	Хищение информации	Иванов Иван Иванович
2017-05-05	Закрыт	другое	NULL	NULL	Николаев Алексей Васильевич

Рисунок 3.5.6 – Выборка по закрытым инцидентам

3.6 Проектирование макета пользовательского интерфейса

Для прототипирования пользовательского интерфейса было использовано программное обеспечение Axure RP 8.

«Axure RP – это уникальное приложение для быстрого прототипирования интерфейса сайта, ориентированное под фреймворк прототипов сайтов. Продукт

предназначен для снижения затрат при разработке сайтов. Это решение поможет вам быстро создать рабочий прототип будущего сайта в визуальном режиме, затем загрузить его в HTML и просмотреть его через браузер. Готовый проект может быть использован для постановки задач дизайнерам и программистам, а также для того, чтобы заказчик понял конечный результат» [27].

Основные функции Axure RP:

– инструменты для создания набросков сайтов и полноценных интерфейсов;
– быстрое переключение в схематичный режим;
– высокая эффективность работы;
– использование мастеров;
– библиотека виджетов;
– интерактивный контент;
– быстрая генерация кода HTML;
– добавление Вашего логотипа;
– аннотации к виджетам и заметки к страницам.

Чтобы иметь возможность использовать разработанную подсистему, пользователь должен войти в систему «АльфаДок». Далее необходимо нажать на пиктограмму меню рабочих столов и перейти по ярлыку «Инциденты ИБ» (рисунок 3.6.1):

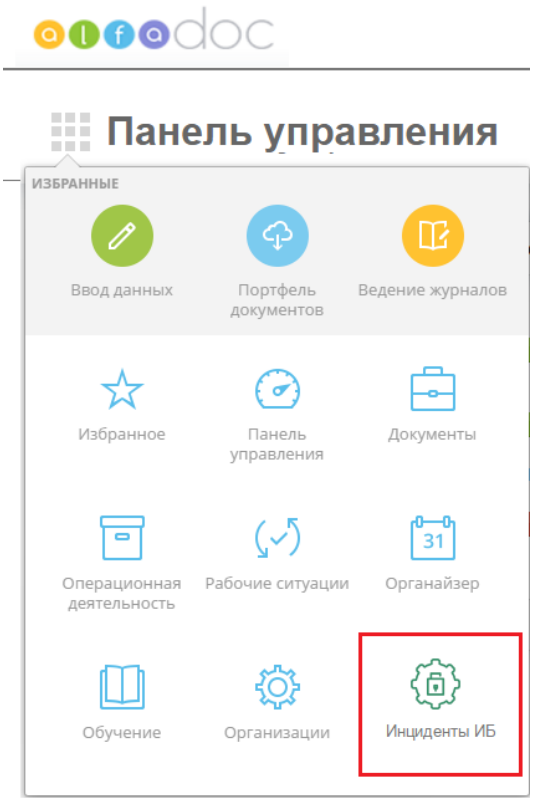

Рисунок 3.6.1 – Меню рабочих столов

После нажатия по ярлыку «Инциденты ИБ» пользователь попадает на рабочий стол «Инциденты ИБ», который изображен на рисунке 3.6.2:

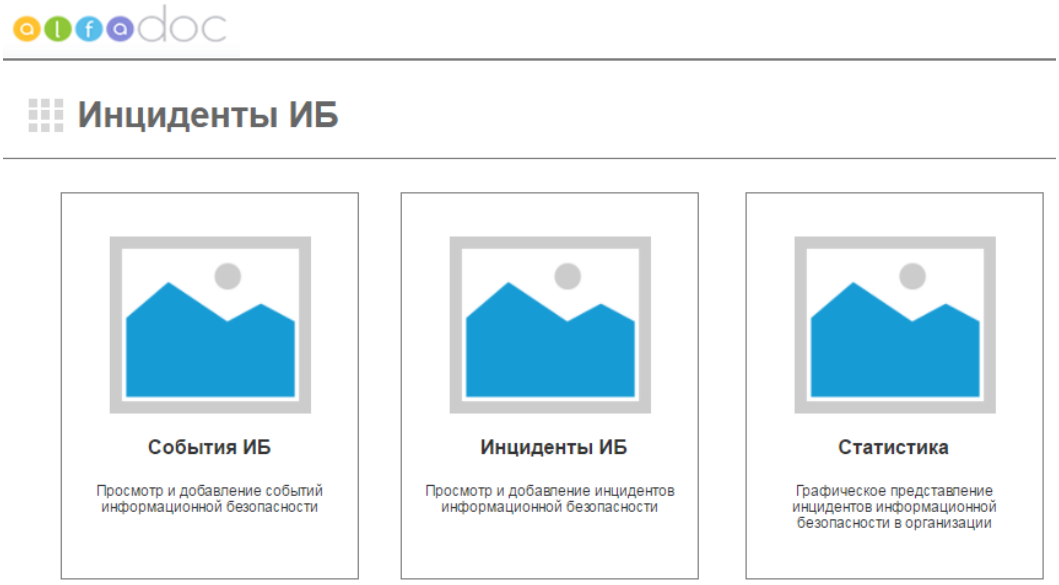

Рисунок 3.6.2 – Меню рабочего стола «Инциденты ИБ»

После осуществления перехода по ярлыку «События ИБ» появляется возможность вносить события ИБ в реестре событий ИБ, а также просматривать состояние ранее созданных событий ИБ (рисунок 3.6.3).

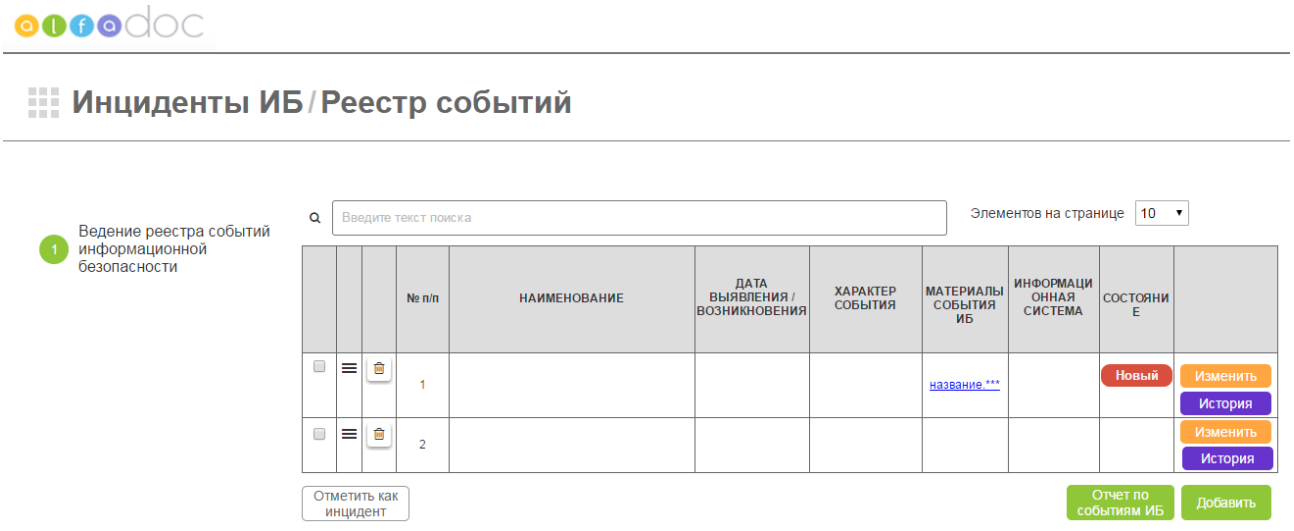

Рисунок 3.6.3 – Реестр событий информационной безопасности

Для добавления нового события ИБ, необходимо нажать кнопку «Добавить», после нажатия которой откроется модальное окно для добавления события ИБ (рисунок 3.6.4).

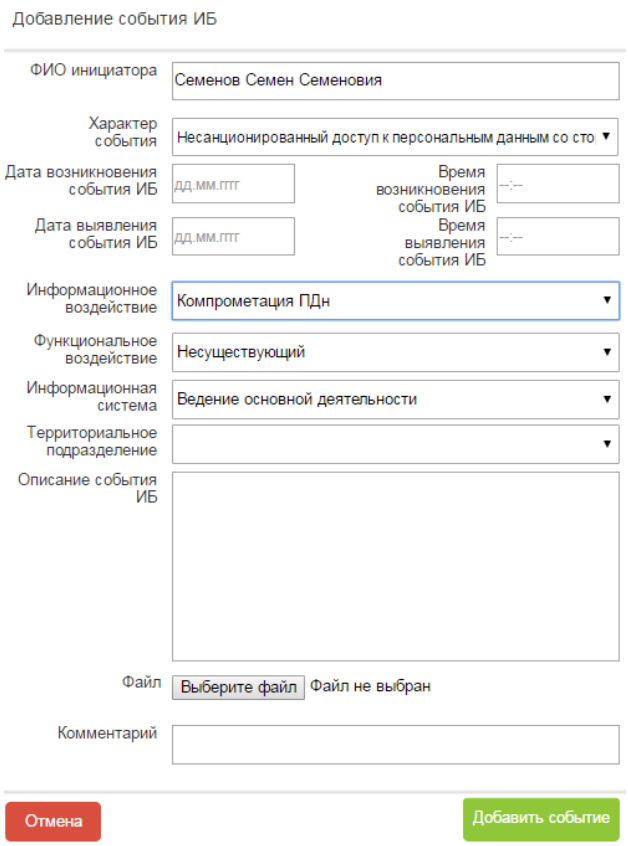

Рисунок 3.6.4 – Добавление события информационной безопасности

После открытия формы, если роль события информационной безопасности определена как сотрудник подчиненной организации, то поле «ФИО инициатора» автоматически загружается из данных, введенных в профиле сотрудника. Сотрудник Организации должен заполнить следующие данные события информационной безопасности: характер события, выбор значения; дата возникновения события информационной безопасности и дата его обнаружения; выбрать из справочника функциональное и информационное воздействие; указать, в какой информационной системе и территориальной единице произошло это событие. В поле «Описание события ИБ» введите дополнительную информацию, которая ранее не вводилась. Если у сотрудника есть какие-либо файлы, которые содержат информацию о событии ИБ в качестве доказательства, они должны быть прикреплены в поле «Файл». И в конце ввода информации нажмите «Добавить событие». После этого форма добавления события ИБ закроется, и событие перейдет в реестр событий ИБ с присвоением статуса «Новый».

Если сотруднику необходимо изменить сведения по событию ИБ, то он может это сделать до тех пор, пока событие не возьмет в работу Ответственный.

После того, как событие было создано, на почтовом ящике сотрудников появится оповещение, что такая проблема возникла.

В таблице событий ИБ пользователи с ролью сотрудники могут видеть только созданные ими события ИБ, а также отслеживать историю их изменений. Сотрудники, с ролью Ответственного, могут видеть все события ИБ, добавленные в систему.

Для того, чтобы определить событие как инцидент, Ответственному нужно выбрать требуемое событие, после чего кнопка «Отметить как инцидент» станет активной, и нажать данную кнопку (рисунок 3.6.5).

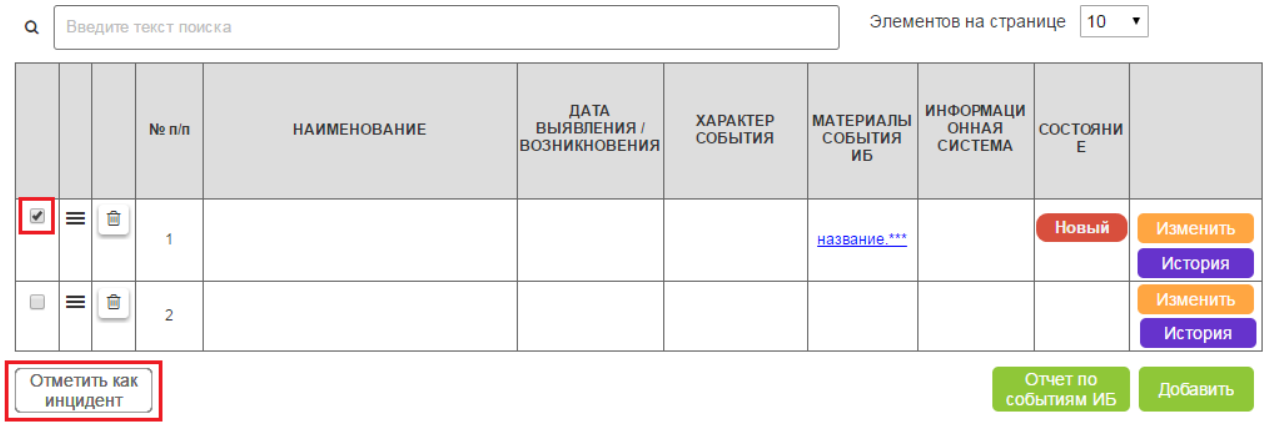

Рисунок 3.6.5 – Отметка события в качестве инцидента

После совершения предыдущего действия откроется форма добавления инцидента ИБ на основе события. На форме также появятся дополнительные поля, необходимые для добавления инцидента ИБ в систему (рисунок3.6.6).

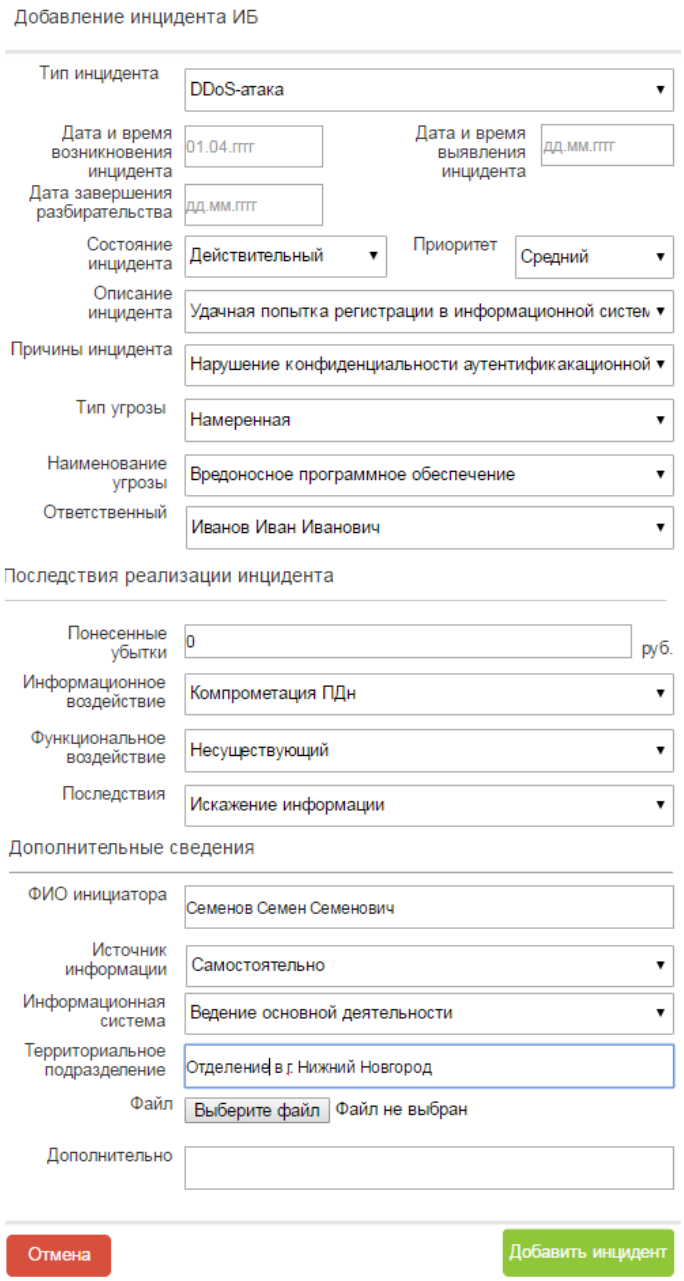

Рисунок 3.6.6 – Добавление инцидента

Для добавления инцидента ИБ, необходимо перейти на шаг «Ведение реестра инцидентов информационной безопасности» либо вернуться в меню рабочего стола «Инциденты ИБ» и выбрать ярлык «Инциденты ИБ» (рисунок 3.6.2). Для описания инцидента ИБ не на основе события требуется тот же состав полей (рисунок 3.6.6).

После заполнения всех полей и нажатия кнопки «Добавить инцидент» откроется вкладка «Меры» (рисунок 3.6.7), на которой можно добавить необходимые действия по устранению последствий инцидента ИБ:

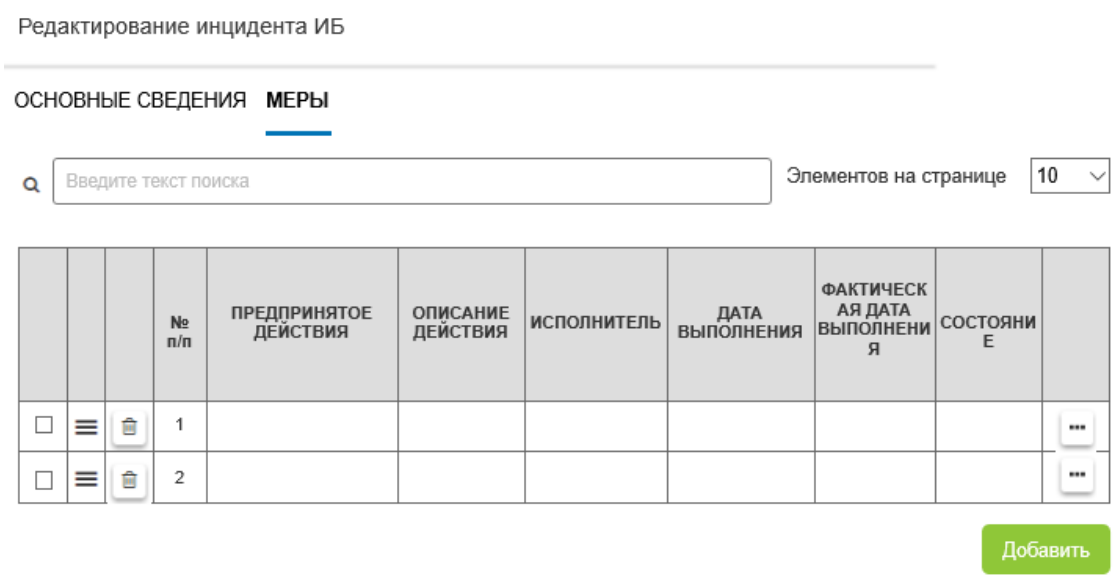

Рисунок 3.6.7 – Список мер

Для добавления действия, необходимо нажать кнопку «Добавить», после чего откроется модальное окно добавления действий по устранению инцидента ИБ (рисунок 3.6.8):

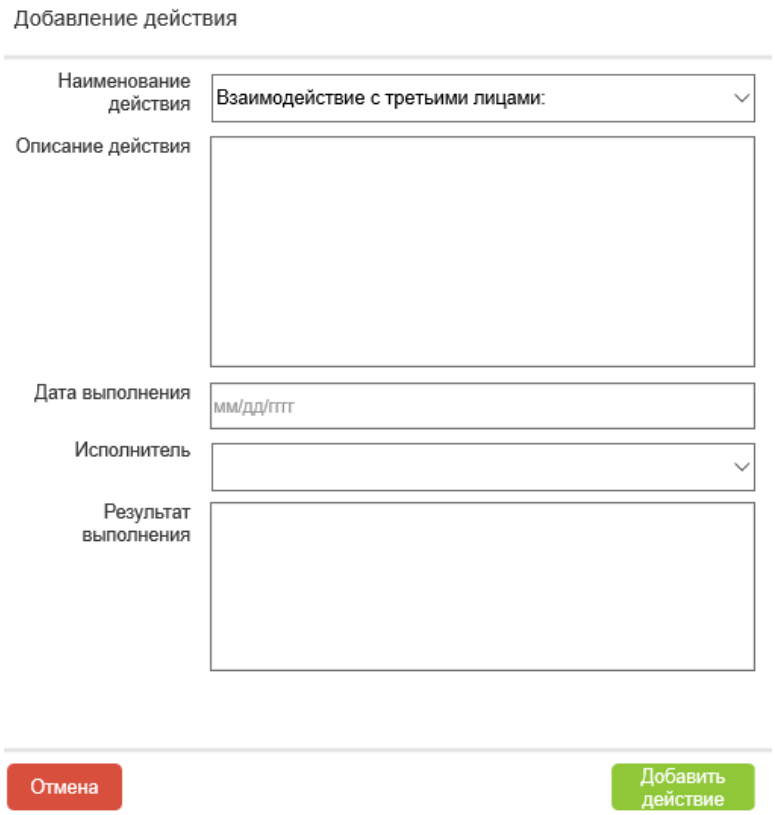

Рисунок 3.6.8 – Добавление действия

В поле «Наименование действия» необходимо выбрать действие, которое требуется выполнить, либо выбрать «Другое» и в появившемся поле написать свой произвольный вариант. Далее в поле «Описание действия» необходимо подробнее описать действие, затем в поле «Исполнитель» выбрать одного или нескольких исполнителей данного действия и установить срок выполнения в поле «Срок выполнения». Поле «Результат выполнения» можно оставить пустым, его должен заполнить исполнитель задачи. Для того, чтобы добавить действие,необходимо нажать кнопку «Добавить действие», после чего оно отобразится в списке решений повыбранному инциденту (рисунок 3.6.7).

Действие можно также отредактировать путем нажатия кнопки действий, отображенной на рисунке 3.6.9:

Рисунок 3.6.9 – Кнопка действий над мерой

И затем нажать кнопку «Изменить» (рисунок 3.6.10):

Рисунок 3.6.10 – Кнопка редактирования меры

Для выполнения действия, необходимо нажать на кнопку, изображенную на рисунке 3.6.9, а затем нажать кнопку «Начать выполнение» (рисунок 3.6.11).После чего состояние задачи примет значение «В работе».

Рисунок 3.6.11 – Кнопка начала выполнения действия

Для закрытия действия необходимо нажать кнопку «Закрыть», состояние измениться на статус «Закрыто» (рисунок 3.6.12):

Рисунок 3.6.12 – Закрытие действия

После выполнения всех операций и закрытия формы редактирования инцидента ИБ запись попадет в реестр инцидентов ИБ (рисунок 3.6.13).

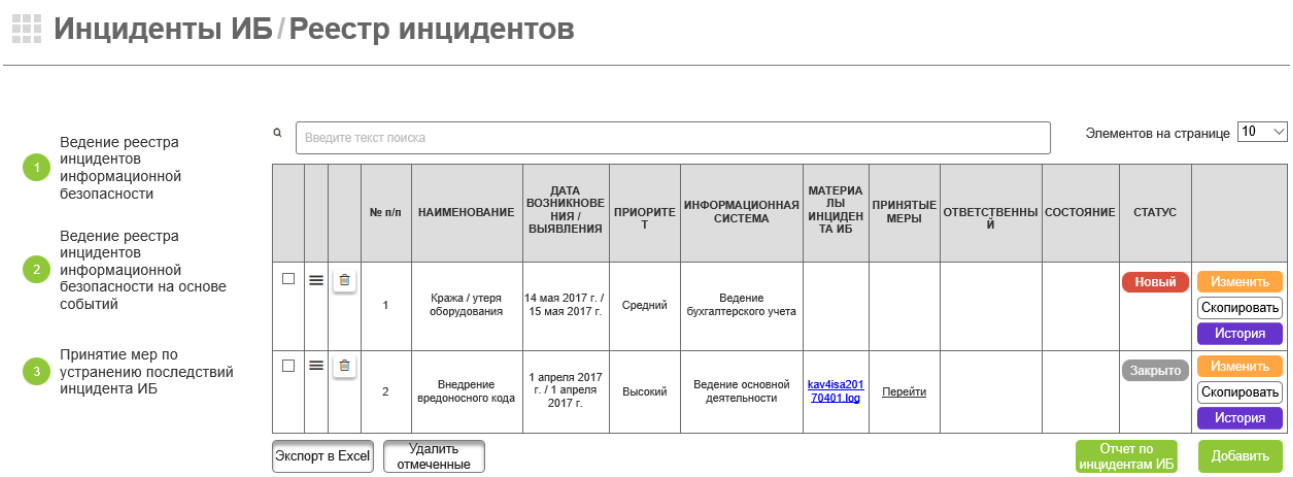

Рисунок 3.6.13 – Реестр инцидентов

В случае, если инцидент является типовым, то при помощи кнопки «Скопировать» (рисунок 3.6.14) можно создать запись о новом инциденте, основываясь на введенныхранееданные.Для выгрузки журнала ведения инцидентов ИБ в Организации достаточно выделить нужные строки и нажать кнопку «Экспорт в Excel», выгруженный файл может быть в любом из выбранных форматов:*.xlsx, *.xlsи *.csv.

Рисунок 3.6.14 – Кнопки копирования и экспорта в Excel

Все меры, которые были созданы по инцидентам, заведенным в системе, можно посмотреть на шаге «Принятие мер по устранению последствий инцидента ИБ» вкладки «Инциденты ИБ» (рисунок 3.6.15):

Рисунок 3.6.15 – Список созданных мер

В подсистеме также возможен просмотр статистики управления инцидентами в Организации в графическом представлении. Для этого нужно перейти в меню рабочих

столов «Инциденты ИБ» (рисунок 3.6.2) и нажать на ярлык «Статистика», откроется страница просмотра статистики (рисунок 3.6.16):

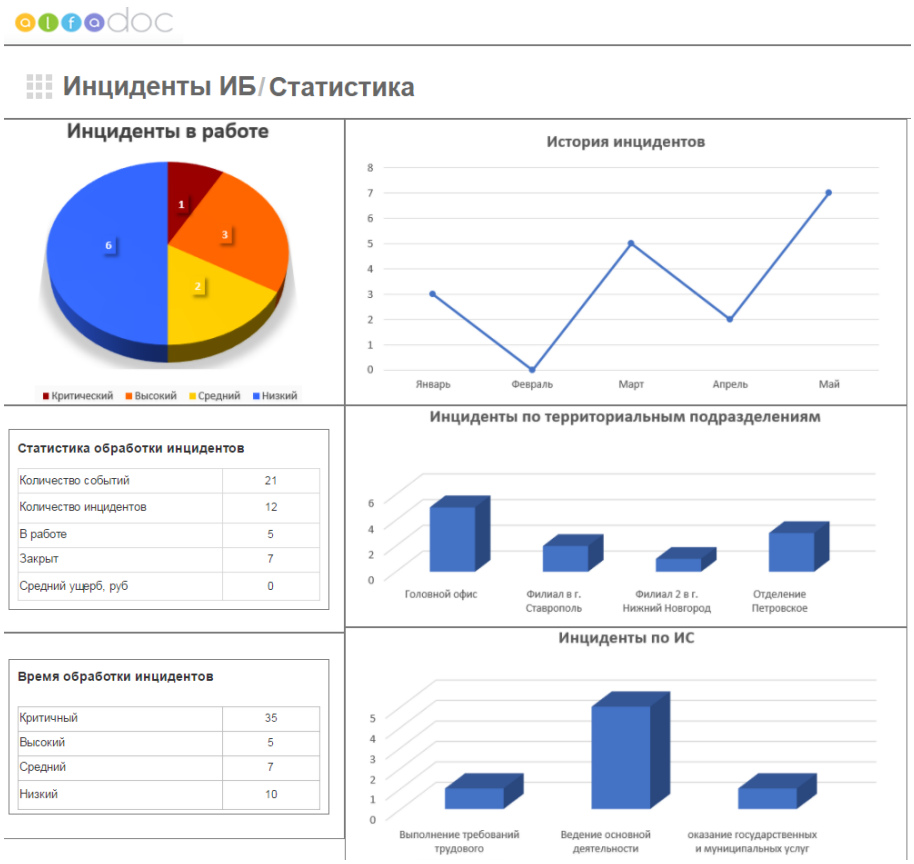

Рисунок 3.6.16 – Графическое представление инцидентов в организации

3.7 Выводы

В данной главе была спроектирована подсистема управления инцидентами информационной безопасности. Описаны основные требования к системе, компоненты системы, спроектирована работа основных компонентов, взаимодействие между ними. Подробно описана база данных подсистемы, описаны ее функции. Разработаны сводные отчеты по событиям и инцидентам ИБ.

На основе спроектированной структуры разработаны макеты пользовательского интерфейса.

Заключение

В данной работе продемонстрировано проектирование подсистемы выявления инцидентовИБ, были выполнены поставленные задачи:

– изучен теоретический материал, нормативы и стандарты, обоснована необходимость разработки подсистемы управления инцидентами информационной безопасности в онлайн-сервисе «АльфаДок»;

– проведен анализ существующих решений на рынке информационных технологий области информационной безопасности;

– разработан проект подсистемы управления инцидентами информационной безопасности в онлайн-сервисе «АльфаДок».

Список использованной литературы

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС КонсультантПлюс.
2. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС КонсультантПлюс.
3. Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 г. № 17«Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // СПС КонсультантПлюс.
4. Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС КонсультантПлюс.
5. Положение Банка России от 24.08.2016 г. № 552-П «О требованиях к защите информации в платежной системе Банка России»// СПС КонсультантПлюс».
6. Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11.02.2014 г.) // СПС КонсультантПлюс.
7. Указание Банка России от 9.06.2012 г. № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» // СПС КонсультантПлюс.
8. Указание Банка России от 21.06.2013 г. № 3024-У «О внесении изменений в Указание Банка России от 9.06.2012 года № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств») // СПС КонсультантПлюс.
9. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 г. № 375-ст). – М.:Стандартинформ, 2008.
10. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной

безопасности (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2007 г. № 513-ст) – М.: Стандартинформ, 2009.

11. ГОСТ 7.32-2001. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления. – М.: Стандартинформ, 2008. – 22 с.

12. ГОСТ 2.105-95. Единая система конструкторской документации. Общие требования к текстовым документам. – М.: Стандартинформ, 2007. – 28 с.

13. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27013-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1 (утв. приказом Федерального агентства по техническому регулированию и метрологии от 16.09.2014 г. № 1084-ст).

14. Стандарт Банка России СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014» (принят и введен в действие распоряжением Банка России от 17.05.2014 г. № Р-399).

15. Григорьева, Е. С., Максимова, Е. А., Александров, А. Х. Технические документы по критической информационной инфраструктуре / Е. С. Григорьева, Е. А. Максимова, А. Х. Александров // Состояние и перспективы развития ИТ-образования: сб. науч. тр. – Чебоксары:Изд-во Чуваш. ун-та, 2019. – С. 67-71.

16. Бакшаева, Н. В., Павлова, Т. Н. Методические рекомендации по выполнению курсового проекта Базы данных / Н. В. Бакшаева, Т. Н. Павлова. – Чебоксары: Чуваш. гос. пед. ун-т, 2011.

17. Корнин, И. Требования для программного обеспечения: рекомендации по сбору и документированию / И. Корнин. – Москва: Нобель Пресс, 2014. – 118 с.

18. Кузин, Ф. А. Диссертация: методика написания. Правила оформления. Порядок защиты: практ. пособие для докторов, аспирантов и магистрантов / Ф.А. Кузин. – М.: Ось-89, 2000. – 320 с.

19. Максимова, Е. А., Лавина, Т. А., Александров, А. Х. Автоматизация процесса подключения бюджетных организаций к государственным информационным системам / Е. А. Максимова, Т. А. Лавина, А. Х. Александров // Информатика и вычислительная техника: сб. науч. тр. – Чебоксары: Изд-во Чуваш. ун-та, 2018. – С. 142-146.

20. Пакин, А. И. Информационная безопасность информационных систем управления предприятием [Электронный ресурс]: учебное пособие / А. И. Пакин. –

Москва:Моск. гос. акад. водного транспорта, 2012. – 41 с. – Режим доступа: http://www.iprbookshop.ru.

21. Поляков, А. В. Информационная безопасность организации: социально-управленческий анализ // Социально-гуманитарные знания. – 2010. – № 5. – С. 173-179.

22. Стасышин, В. М.Проектирование информационных систем и баз данных [Электронный ресурс]: учебное пособие / В. М. Стасышин. – Новосибирск: Новосиб. гос. техн. ун-т, 2012. – 100 с. – Режим доступа: http://www.iprbookshop.ru.

23. Торпошян, Е. А. Подсистема управления инцидентами информационной безопасности в системе управления процессами защиты информации / Е. А. Торпошян // Актуальные проблемы математических и технических наук: сб. науч. тр. – Чебоксары: Чуваш. гос. пед. ун-т, 2017. – С. 135-138.

24. Торпошян, Е. А., Александров, А. Х. Управление инцидентами информационной безопасности в системе управления процессами защиты информации / Е. А. Торпошян, А. Х. Александров // Состояние и перспективы развития IT-образования: сб. науч. тр. – Чебоксары: Изд-во Чуваш. ун-та, 2018. – С. 147-155.

25. Чистов, Д. В. Проектирование информационных систем: учеб. и практикум для академ. бакалавриата / под общ. ред. Д. В. Чистова. – Москва: Юрайт, 2016. – 258 с.

26. АльфаДок. [Электронный ресурс] – О сервисе. – URL:https://alfa-doc.ru/.

27. Axure. [Электронный ресурс] –Enterprise. – URL:https://www.axure.com/enterprise/.

28. DocShell. [Электронный ресурс] – Инциденты. – URL:https://new.docshell.ru/desktop/.

Приложение А

Сводный Отчет о событиях информационной безопасности

Сведения о событиях информационной безопасности, связанных с нарушением требований к обеспечению защиты ПДн/защищаемой информации в Организации по состоянию на «__» _____ г.

№ п/п	Характер события ИБ	Дата выявления/возникновения события ИБ	Территориальное подразделение	Описание события ИБ	Причины возникновения события ИБ	Длительность события ИБ	Источник сведений
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1.							
2.							

Приложение Б

Сводный Отчет об инцидентах информационной безопасности

Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты ПДн/защищаемой информации в Организации по состоянию на "__" _____ г.

Раздел 1. Сведения о количестве инцидентов

№ п/п	Наименование показателя	Количествоинцидентов, единиц
1	**2**	**3**
1.	Общее количество инцидентов, всего, в том числе:	
2.	– выявленных клиентами Организации	
3.	– выявленных автоматизированными системами	
4.	– выявленных сотрудниками Организации	

Раздел 2. Сведения об инцидентах отчетного периода

№ п/п	Тип инцидента	Дата выявления/возникновения инцидента	Территориальное подразделение	Описание инцидента	Причины инцидента	Последствия инцидента		Сведения об угрозе		Предпринятые действия по устранению последствий инцидента	Факт обращения в правоохранительные органы	Источник сведений	Дата завершения разбирательства по инциденту
						Суммы ущерба	Оценка убытка	Тип угрозы	Наименование угрозы				
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
1.													

Раздел 3. Сведения об инцидентах предыдущих отчетных периодов

№ п/п	Тип инцидента	Дата выявления/возникновения инцидента	Территориальное подразделение	Описание инцидента	Причины инцидента	Последствия инцидента		Сведения об угрозе		Предпринятые действия по устранению последствий инцидента	Факт обращения в правоохранительные органы	Источник сведений	Дата завершения разбирательства по инциденту
						Суммы ущерба	Оценка убытка	Тип угрозы	Наименование угрозы				
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.													

Руководитель _____ _____
(заместитель руководителя) (личная подпись) (инициалы, фамилия)
М.П.
Исполнитель _____ _____
(личная подпись) (инициалы, фамилия)