Содержание

Введение

В настоящее время бизнес всецело зависит от информационно-коммуникационных технологий. Информационные технологии позволяют автоматизировать работу, упростить задачи, помогают собирать статистические данные, на основе этих данных принимать решения, а также пользоваться электронной почтой, интернетом, удаленно взаимодействовать с партнерами и клиентами.

Внедрение и эксплуатация информационной системы для автоматизации бизнес-процессов компании является сложной задачей и требует специальных знаний в области информационных технологий. ИТ-отдел внутри компании позволяет решить эту задачу, но ИТ-отдел также подразделение на содержание, которого уходит существенная часть бюджета компании. Затраты становятся больше, если ИТ-отдел развернут в самой компании.

Преимуществом является то, что собственный ИТ-отдел отличается пониманием бизнес-процессов компании, а не только наличием технических решений, которые может дать компания аутсорсер. Но в последнее время, чтобы повысить свою конкурентоспособность компании аутсорсеры стремятся подстроиться под нужды бизнеса. Поэтому стал широко развиваться аутсорсинг.

Идет делегирование определенных сфер деятельности компании, которые не связаны с основными задачами, стороннему предприятию, специализирующемуся как раз на таких задачах. Аутсорсеры руководствуются рекомендациями библиотеки ITIL при построении своего бизнеса. После внедрения информационной системы, либо после развертывания услуг компании аутсорсера в качестве ИТ-подразделения в организации идет эксплуатация информационной системы и применение услуг аутсорсинга в бизнесе.

Для устранения проблем, возникающих в процессе работы в информационной системе внедряется Service Desk. Служба технической поддержки является сервисной структурой и осуществляет поддержку пользователей в ряде услуг, которые помогут устранить неполадки в работе с компьютерными аппаратными средствами, программным обеспечением. Перед службой технической поддержки ставится задача обеспечения доступности поддерживаемых информационных систем и своевременного разрешения инцидентов. Существует определенная модель решения инцидентов, но она недостаточно эффективна при поступлении большого количества заявок. В среднем, каждая 5-я заявка из числа принятых звонков не регистрируется в системе.

При управлении инцидентами большое количество заявок не обслуживаются вовремя, возникает проблема нарушения сроков разрешения

инцидента. При большом потоке заявок появляются непринятые вызовы, это критично, так как пользователь обращается за помощью тогда, когда возникшая проблема имеет высокую степень значимости для него или для его бизнеса. Наличие проблем говорит о недостаточной степени эффективности функционирования инцидент-менеджмента и отсутствии сервис-ориентированного подхода при организации инцидент-менеджмента.

Служба технической поддержки является важной функциональной составляющей ITIL (библиотеки инфраструктуры информационных технологий), позволяющая выявить проблемные участки инфраструктуры ИТ, оценить эффективность работы подразделения ИТ.

Для ИТ-компании большую значимость представляет объем информации, которая у них скапливается. Исходя из объема хранимой, поступающей и обрабатываемой информации накапливаются статистические данные. За счет наличия статистики осуществляется диагностика проблем, производится постоянный мониторинг ошибок, который выявляет проблемы, возникающие при работе. Этим обусловлена необходимость в снижении количества пропущенных звонков и незарегистрированных заявок в службе технической поддержки.

Таким образом, одной из важнейших задач совершенствования ИТ-инфраструктуры предприятия является повышение эффективности функционирования системы управления инцидентами

Целью исследования является повышение эффективности предоставления информационно-коммуникационных услуг путем нахождения минимального количества каналов обработки заявок при заданных ограничениях.

Для достижения поставленной цели в работе сформулированы и решены следующие задачи:

1. Ознакомится с теоретическими сведениями по процессу «Управление инцидентами» с учетом методики ITIL.

2. Разработать модель процесса «Управление инцидентами ИТ» (методология IDEF0).

3. Составить классификатор инцидентов по категориям и подкатегориям (техническое обеспечение, сетевое оборудование, программное обеспечение, информационное обеспечение).

4. Составить отчет с выводами.

1. Теоретические основы процесса «Управление инцидентами» с учетом методики ITIL.

ITIL - это набор рекомендаций по лучшим практикам в управлении ИТ-услугами (ITSM). ITIL принадлежит британскому правительственному агентству Office of Government Commerce (OGC) и представляет собой набор публикаций, содержащих рекомендации по организации предоставления качественных ИТ-услуг, а также процессов и компонентов, необходимых для их поддержки [2].

Набор рекомендаций был разработан в конце 80-х годов и состоял из 40 томов, но на сегодняшний день доступны только несколько. В ITIL v.2 семь книг:

Поддержка услуг (Service Support);

Предоставление услуг (Service Delivery);

Планирование внедрения управления услугами (Planning to Implement Service Management);

Управление приложениями (Application Management);

Управление инфраструктурой информационно-коммуникационных технологий (ICT Infrastructure Management);

Управление безопасностью (Security Management);

Бизнес-перспектива (The Business Perspective);

Управление конфигурациями ПО (Software Asset Management).

По ITIL v.3:

Стратегия услуг (Service Strategy);

Проектирование услуг (Service Design);

Преобразование услуг (Service Transition);

Эксплуатация услуг (Service Operation);

Постоянное улучшение услуг (Continual Service Improvement).

В библиотеке ITIL рассматриваются типовые модели, описывающие цели, главные особенности, входные и выходные данные различных процессов, подлежащих внедрению в службу технической поддержки. При этом в библиотеке нет подробного описания шагов, что позволяет адаптировать передовой опыт для любого случая. Также в ITIL реализуется подход к управлению ИТ-услугами – сосредоточенность на пользователе и его потребностях, на услугах, предоставляемых ему информационными технологиями, а не на самих технологиях.

IT Service Management (ITSM) представляет собой внедрение и управление качественными ИТ-услугами, которые соответствуют требованиям бизнеса. Управление ИТ-услугами (ITSM) реализуется поставщиками ИТ-услуг путем использования наиболее оптимального сочетания людей, процессов и информационных технологий [2].

Существуют несколько базовых процессов при управлении ИТ-услугами: процесс управления инцидентами; процесс управления проблемами; процесс управления конфигурациями; процесс управления изменениями; процесс управления релизами; процесс управления уровнем услуг; процесс управления мощностями; процесс управления доступностью; процесс управления непрерывностью; процесс управления финансами.

Одним из базовых процессов, обеспечивающих поддержку и предоставление ИТ-услуг, является процесс управления инцидентами.

Под инцидентом понимается (от лат. incidens – случай, происшествие (обычно неприятное) столкновение с неприятным случаем) любое событие, не являющееся частью стандартных операций по предоставлению услуги, которое привело или может привести к нарушению или снижению качества этой услуги.

В свою очередь, управление инцидентами - есть деятельность по восстановлению нормального обслуживания с минимальными задержками и влиянием на бизнес-операции [2].

На данный момент работа ИТ-службы устроена таким образом, что процесс управления инцидентами включает в себя такие этапы как:

Выявление и регистрация инцидентов (Acceptance and Recording).

На этом этапе в Service Desk принимается сообщение о возникшей проблеме и создается запись о ней в системе управления инцидентами.

Классификация и начальная поддержка (Classification and Initial Support).

Заявке присваиваются тип, статус, степень воздействия, срочность, приоритет инцидента, срок по SLA и т.п. Пользователю может быть предложено возможное решение – консультация. В системе управления инцидентами создается запрос на Обслуживание (Service Request), осуществляется поиск ответа в Базе знаний, проверяется, не является ли инцидент уже известной ошибкой, нет ли для него решения.

Исследование и диагностика (Investigation and Diagnosis).

При отсутствии известного решения, производится исследование инцидента с целью оперативного восстановления сервиса.

Решение и восстановление (Resolution and Recovery).

Если решение найдено, то работа может быть восстановлена.

Закрытие инцидента (Closure).

С пользователем связываются, чтобы он подтвердил согласие с предложенным решением, после чего инцидент считается отработанным и разрешенным.

Мониторинг хода работ и отслеживание (Progress monitoring and Tracking).

Весь цикл обработки инцидента контролируется – идет мониторинг ошибок. Если инцидент не может быть разрешен вовремя, то производится эскалация. В завершении производится оценка полученного ущерба [3].

Применение рекомендаций ITIL начинается с внедрения процесса управления инцидентами. Проводится обследование, затем построение модели процесса управления инцидентами, с учетом методологических рекомендаций ITIL. После построения модели начинается этап технической разработки, позволяющий автоматизировать процесс управления инцидентами и этап промышленной эксплуатации, где происходит сопровождение и развитие процесса управления инцидентами.

Современные системы Service Desk способны управлять, контролировать и отслеживать запросы на обслуживание, соблюдение условий контракта, людские ресурсы и последовательности работ. Эти системы интегрируются с остальными важными компонентами совокупной системы управления ИТ-ресурсами (в том числе с рекомендуемыми ITIL — Управлением изменениями, Конфигурированием и Учетом активов, Управлением ценой, Непрерывностью бизнеса, Планированием возможностей, Управлением сетями и т.д.).

К наиболее развитым системам, предназначенным для реализации Service Desk в организациях среднего и крупного размера, относят такие системы управления инцидентами как:

– CA Service Desk Manager;

– HP Open View Service Desk;

– Tivoli Service Request Manager.

Все эти системы в высокой степени обладают необходимой функциональностью, предоставляют возможности масштабирования, удобство управления и приемлемость для разнообразных ИТ-архитектур. В этих условиях решающими факторами в выборе оказываются:

– возможность интеграции с остальными решениями по управлению различными элементами ИТ-инфраструктуры (сетями, серверами, рабочими станциями приложениями и т.д.);

– условия предоставляемой поддержки (ее полнота и доступность, а также возможность привлечения консультантов из компаний, специализирующихся на внедрении этих систем).

Внедрение службы Service Desk обычно осуществляется в виде проекта, подразумевающего предварительный консалтинг. Качественная реализация такого проекта возможна только при достаточной квалификации специалистов, участвующих во внедрении.

Анализ применения систем управления инцидентами показал, что среди малого и среднего бизнеса распространенными являются такие системы как: TerraSoft Service Desk, Naumen Service Desk, «Итилиум», HPService Management.

TerraSoft Service Desk помогает сократить время на обработку обращений и заявок. Система автоматически определяет время, необходимое на

выполнение каждого запроса на изменение, анализирует загрузку специалистов и создает задачи.

Naumen Service Desk доступен как SaaS сервис. Это популярное отечественное ИТ-решение переходит на схему SaaS. Naumen Service Desk - ведущая ITSM система на российском рынке. Она позволяет отслеживать ИТ-инфраструктуру, принимать заявки от пользователей, контролировать их решение, а также управлять обновлениями, конфигурациями, уровнем сервиса и всеми теми процессами, которые описаны в библиотеке ITIL. Для пользователей доступен клиентский портал с личным кабинетом, где можно оставлять заявки, контролировать их статус, общаться с сотрудниками технической поддержки и читать базу знаний.

«Итилиум» система управления инцидентами предназначенная для автоматизации процессов библиотеки ITIL. Система «Итилиум» разработана компанией «Деснол Софт» на базе платформы «1С: Предприятие 8». Главная особенность системы – способность в краткие сроки оптимизировать ИТ-процессы компании.

HP Service Management. Постоянно расширяется портфель решений для управления услугами, которые позволят ИТ-организациям воспользоваться дополнительными возможностями обновленной библиотеки ITIL версии 3.

В настоящее время компании-разработчики выпускают обновления и системы продолжают оставаться востребованными на рынке услуг.

Основная цель процесса управления инцидентами: максимально быстро восстановить нормальное функционирование услуг и как можно скорее минимизировать неблагоприятное воздействие на пользователей. Так как цель у процесса одна, то и модели управления инцидентами обладают схожими параметрами.

Большинство компаний применяет эталонную модель управления инцидентами, так как процесс управления инцидентами является единым для всех ИТ-подразделений.

Процесс управления инцидентами обеспечивает тотальную регистрацию обращений пользователей: все обращения, а также связанные с ними действия фиксируются в единой базе данных системы управления инцидентами. Контакт Центр (центр обработки заявок) выступает в роли единой точка контакта между пользователями и ИТ-подразделениями.

Пользователи имеют следующие способы обращения в службу поддержки:

телефон;

электронная почта;

система электронного документооборота;

web-форма;

внешняя система;

служебная записка.

Помимо существования разделения заявок на Обращения и Инциденты в рамках процесса управления инцидентами обрабатываются следующие категории обращений:

Инцидент;

Запрос на обслуживание;

Запрос на изменение;

Запрос информации;

Отзыв по качеству;

Не по адресу.

Все ИТ-специалисты кроме Диспетчеров Контакт Центра (операторы) и Инженеров Центра компетенции (специалисты) входят в рабочие группы. Один ИТ-специалист может входить в состав нескольких рабочих групп. В состав Контакт Центра входят: Руководитель; Диспетчеры. В состав Центра

компетенции входят: Координатор; Инженеры. В состав рабочей группы входят: Координатор группы; Исполнители.

Существуют основные правила обработки Обращений и Инцидентов:

Диспетчер (оператор) принимает, регистрирует Обращения, выполняет первичную классификацию и получает подтверждение пользователя о выполнении Обращения.

Специалист 1й линии технической поддержки является ответственным за классификацию или выполнение Обращений и направление Инцидентов в работу в рабочую группу к специалистам 2-й линии;

Инженер Центра компетенции отвечает за контроль сроков исполнения и контроль корректности оформления и сроков выполнения Обращений из своей зоны ответственности;

Исполнитель (специалист 2-й линии технической поддержки) является ответственным за исполнение назначенного на него Инцидента и корректность его оформления;

Координатор группы является ответственным за контроль исполнения и оформления Инцидентов, назначенных на его рабочую группу.

После выполнения работ по обращению или инциденту заявка переходит для работы к оператору (Диспетчеру КЦ), который связывается с пользователем и уточняет факт выполнения заявки, согласовав, таким образом, закрытие заявки в системе управления инцидентами.

Но, для того, чтобы выявить недостатки существующей модели управления инцидентами невозможно ограничиться только описанием процесса, необходимо более глубокое изучение процесса управления инцидентами. С этой целью проводился мониторинг заявок в существующей организации из системы управления инцидентами. Статистические данные собирались в течении месяца мониторинга за системой управления инцидентами. Отслеживались переходы статусов заявок, их сроки выполнения. Так как основным недостатком при анализе теоретических данных выступало большое количество пропущенных звонков и незарегистрированных заявок, а также

увеличенные сроки выполнения заявок, то были собраны статистические данные отражающие эти показатели.

2. Модель процесса «Управление инцидентами ИТ» (методология IDEF0).

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.

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.

Для описания бизнес-процессов управления инцидентами ИБ, используя Business Studio, было осуществлено моделирование функциональных диаграмм, основанных на технологии моделирования IDEF0 (рисунок 1).

Рисунок 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.

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
	Регламент реагирования на инциденты ИБ	«…документ, в котором указаны действия сотрудников организации при возникновении инцидента ИБ»

УПРАВЛЕНИЕ	Устав организации	Содержит правила, определяющие порядок функционирования организации
	Закон Республики Беларусь от 7 мая 2021 г. № 99-З ”О защите персональных данных“	Содержит основные требования по защитеперсональных данных
	Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 ”О мерах по совершенствованию защиты персональных данных“	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.

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.

- 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.

- 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.

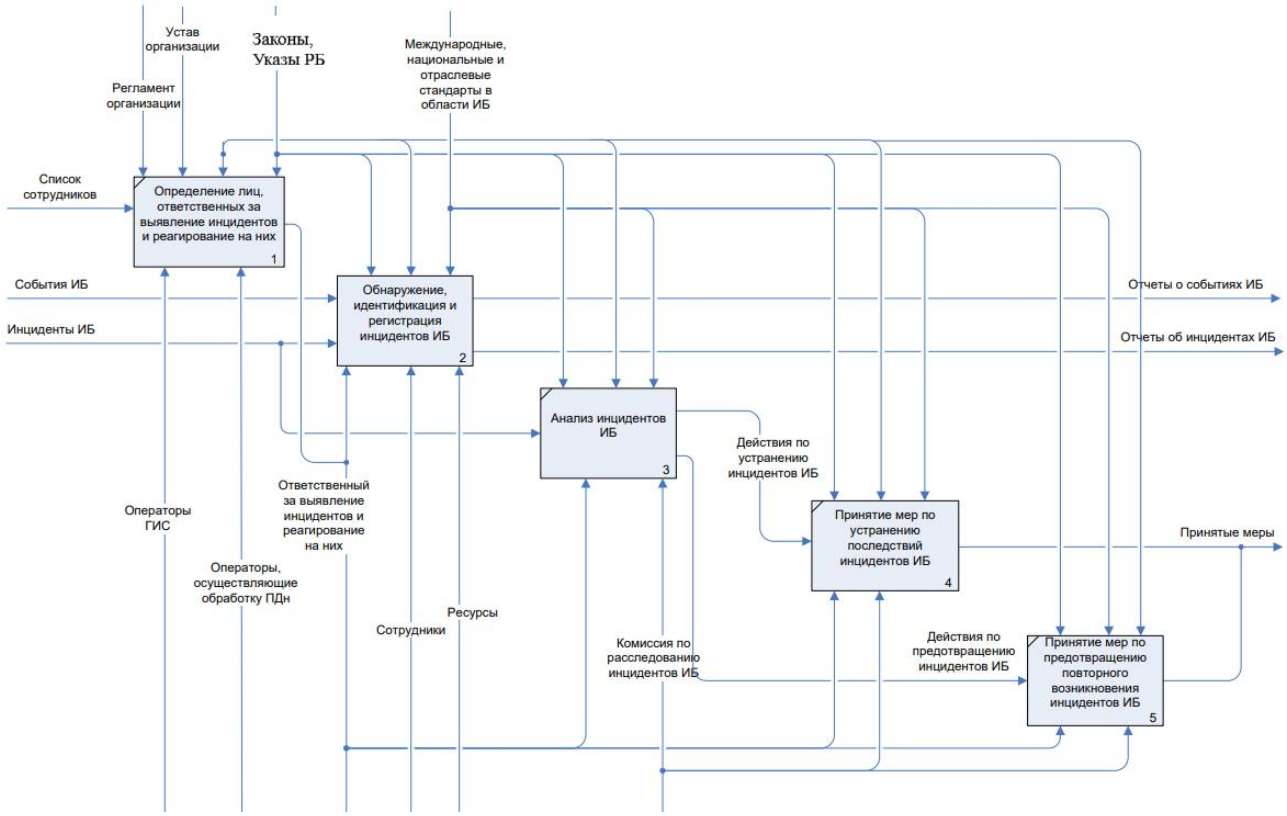

Рисунок 3.2.2 – Декомпозиция процесса управления инцидентами ИБ

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:

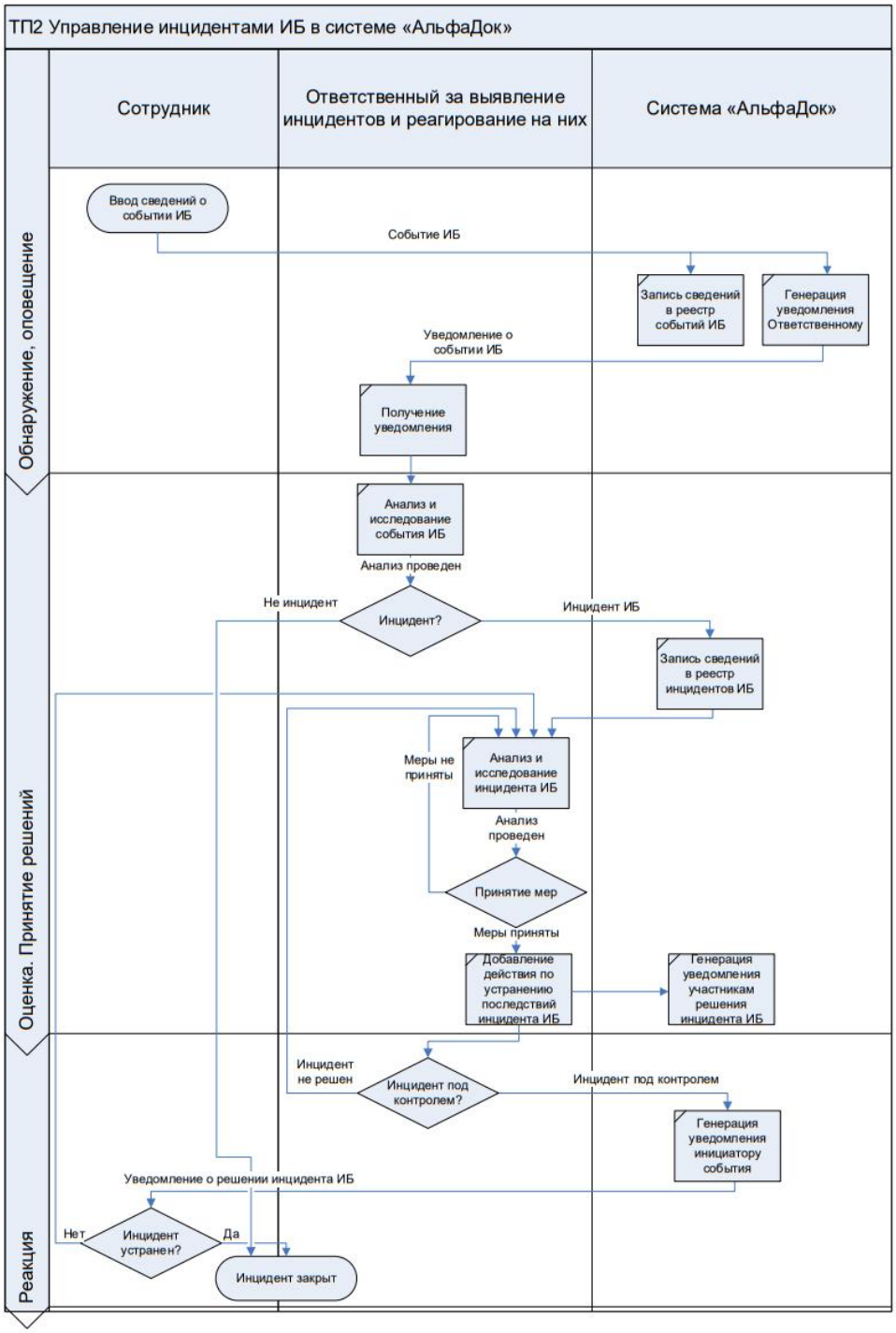

Рисунок 3.2.3 – Диаграмма последовательности действий в нотации «Процедура»

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. Классификатор инцидентов по категориям и подкатегориям (техническое обеспечение, сетевое оборудование, программное обеспечение, информационное обеспечение)

Инциденты информационной безопасности (ИБ) представлены десятками событий, объединенных в классификацию и делящихся по нескольким признакам:

- По уровню тяжести для профессиональной деятельности компании.
- По вероятному возникновению рецидива – повторное «заражение».
- По типам угроз.
- По нарушенным свойствам ИБ.
- По преднамеренности возникновения.
- По уровню информационной инфраструктуры.
- По сложности выявления.
- По сложности устранения и т.д.

По категории критичности:

- 1 категория. Инцидент может привести к значительным негативным последствиям (ущербу) для информационных активов или репутации организации.
- 2 категория. Инцидент может привести к негативным последствиям (ущербу) для информационных активов или репутации организации.
- 3 категория. Инцидент может привести к незначительным негативным последствиям (ущербу) для информационных активов или репутации Банка.
- 4 категория. Инцидент не может привести к негативным последствиям (ущербу) для информационных активов или репутации.

Приоритеты реагирования на инциденты:

- очень высокий. Соответствует 1-й категории критичности. Время реагирование не более 1 часа;
- высокий. Соответствует 2-й категории критичности. Время реагирование не более 4 часов;
- средний. Соответствует 3-й категории критичности. Время реагирование не более 8 часов;
- низкий. Соответствует 4-й категории критичности. Время реагирование не определено.

По причине возникновения:

- Случайные.
- Намеренные.

По степени нанесенного ущерба:

- Непоправимый ущерб.
- Поправимый ущерб.

- Отсутствие ущерба.

Основные примеры:

- Отказ в обслуживании. Большая категория, включающая события, которые приводят системы, сети или серверы к неспособности функционировать с прежними показателями и параметрами. Чаще всего проявляются, если пользователи в процессе авторизации получают отказ доступа. В данной группе инцидентов информационной безопасности (ИБ) выделяют несколько типов, создаваемых компьютерными и иными ресурсами: истощение и полное уничтожение ресурсов. Наиболее распространенные примеры: единовременный запуск сразу нескольких сеансов в рамках одной системы, передача данных в запрещенном формате в попытках вызвать различные нарушения или свести на «нет» их нормальную работу и т.д.

- Сбор информации. Предусматриваются действия, связанные с установлением возможных, наиболее явных целей атаки и получением сведений о соответствующих сервисах [8]. Инциденты в этой категории предполагают выполнение разведывательных мероприятий, чтобы выявить: наличие цели и ее потенциальные уязвимости. Распространенные примеры атак с использованием технических устройств – сброс записей DNS, отправление сообщений-тестов по «левым» координатам для поиска функционирующей системы, исследование объекта для идентификации, анализ открытых поротов на протокол передачи файлов и т.д.

- Несанкционированный доступ. Это остальные инциденты, которые не подходят под параметры вышеперечисленных категорий. Сюда входят несанкционированные попытки получения доступа к системе или ее неправильное использование. Типичные примеры – извлечение внутренних файлов с паролями, атаки переполнения буфера с целью получения привилегированного доступа к сети, использование уязвимостей протокола для перехвата важной информации, разрушение устройств физической защиты с последующим завладением данных и т.д.

Заключение

В настоящее время, когда информационные технологии проникают во все сферы нашей жизни, вопросы информационной безопасности становятся все более важными. Эффективное управление инцидентами ИБ не только помогает минимизировать потенциальные убытки, но и способствует восстановлению нормального функционирования системы. Осведомленность об основах и принципах управления инцидентами информационной безопасности создает основу для разработки эффективных стратегий и процедур. Эти стратегии и процедуры необходимы для предотвращения, обнаружения и адекватного реагирования на инциденты ИБ и восстановления систем после возможных нарушений безопасности организации.

Управление инцидентами информационной безопасности является неотъемлемой составляющей для современных организаций. Процесс управления инцидентами ИБ должен иметь четко спланированный и структурированный подход, что позволяет эффективно выявлять, анализировать и реагировать на инциденты. Успешное управление инцидентами информационной безопасности требует не только технических средств и документации, но и активного участия персонала, что подчеркивает важность комплексного подхода. Только через постоянное улучшение, обучение и адаптацию можно обеспечить надежную защиту данных и поддержание операционной устойчивости.

В наше время организации сталкиваются с растущими угрозами нарушения конфиденциальности, целостности и доступности их информационных ресурсов. В этом контексте эффективное управление инцидентами становится необходимостью для обеспечения безопасности и непрерывности деятельности организаций. Оно обеспечивает оперативное реагирование на угрозы, минимизирует риски для бизнеса и сохраняет репутацию организации.

Список использованной литературы

1. 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.

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

3. 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.

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

5. 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.

6. 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.

7. 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.

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