Pandora	**«УТВЕРЖДАЮ»** **Заместитель директора по IT и IT безопасности** **ГК «Пандора»** **_____ А.Л. Миронов** **Дата вступления в силу «22» августа 2022 г.**

РУКОВОДСТВО

по Процессу управления инцидентами

Дата оригинальной редакции **22.08.2022 г**

Согласовано:

Заместитель директора по проектной деятельности ИТ _____ /В.Ю. Болотин/

Зам. ГД по безопасности _____ /Ю.Д. Петрунин/

Разработано:

Начальник отдела эксплуатации и поддержки ИТ _____ /Сидорка Ф.А./

Содержание

1. Цель

Управление инцидентами – процесс, отвечающий за управление жизненным циклом всех инцидентов, обеспечивающий минимизацию влияния на бизнес-процессы и восстановление нормального функционирования услуги наиболее быстрым способом.

Настоящее Руководство является основным документом Процесса управления инцидентами для ИТ-подразделения и внешних ИТ-подрядчиков Группы Компаний «Pandora».

Настоящее Руководство определяет основные принципы Процесса управления инцидентами, необходимые роли, общий ход процесса, порядок взаимодействия между отделами ИТ- инфраструктуры и структурными подразделениями Группы Компаний «Pandora.

2. Область действия

Процесс управления инцидентами распространяется на все компоненты ИТ, которые непосредственно относятся или могут повлиять на продуктивную среду ИТ. Сюда относятся, в частности, ИТ-инфраструктура, системы, приложения, серверы и клиенты.

Процесс управления инцидентами применяется также для процессов разработки, тестирования, обеспечения качества, интеграции и развертывания решений.

Рекомендуется применять процесс управления инцидентами для компонентов ИТ, не связанных напрямую с продуктивной средой.

Руководство включается в перечень одновременно действующих документов при проведении конкурсов среди подрядчиков.

Примечание:

Особенности обработки инцидентов информационной безопасности описаны в Руководстве по решению инцидентов информационной безопасности.

Особенности обработки значительных инцидентов описаны в Руководстве по решению значительных инцидентов.

Особенности регистрации инцидентов ИТ на производстве описаны в Руководстве по обращению в ИТ с использованием сервиса HelpDesk.

3. Сокращения

ЕТК – единая точка контакта
ИТ – информационные технологии
МЗИ – менеджер значительный инцидентов
РГЗИ – рабочая группа по устранению значительного инцидента
KPI – ключевой показатель эффективности (Key Performance Indicator)

4. Термины и определения

ИТ-услуга или ИТ-сервис	Способ предоставления ценности Заказчикам через содействие им в получении конечных результатов, которые Заказчики хотят достичь без владения специфическими затратами и рисками. Термин «услуга» может использоваться для обозначения основной услуги, ИТ-услуги или пакета услуг.
Инцидент	Незапланированное прерывание нормальной работы ИТ-услуги, связанное, обычно, с неисправностью ИТ-актива. Инцидентом является также неисправность, которая ещё не повлияла на ИТ-услугу.

Категоризация	Действие, направленное на определение спецификации существующего инцидента. Категоризация состоит из определения: - конфигурационной единицы или ИТ-актива, на котором произошел инцидент; - приоритета инцидента.
Приоритет	Категория, используемая для определения относительной важности инцидента по отношению к другим инцидентам. Приоритет основывается на влиянии и срочности и часто используется для определения требуемого времени обработки.
Влияние	Уровень воздействия инцидента, проблемы или изменения на бизнес-процесс. Влияние часто основано на том, как будут затронуты уровни услуги.
Срочность	Мера того, насколько быстро с момента своего появления инцидент существенно повлияет (или уже повлиял) на бизнес-процессы. *Например, инцидент с высоким уровнем влияния может иметь низкую срочность, если это влияние не затрагивает бизнес до конца финансового года.*
Влияние и срочность используются для определения приоритета.	
Значительный инцидент	Значительный инцидент – серьёзный сбой одной или нескольких критически важных для бизнеса ИТ-услуг, который затрагивает или делает невозможным выполнение основных бизнес-процессов, но может быть устранен в течение 24 часов. После истечения 24 часов значительный инцидент, как правило, переходит в статус аварии и передается в обработку соответствующим процессом. Значительный инцидент распознается посредством приоритета и утверждается решением Менеджера инцидентов.
Заявка	Зарегистрированное, неклассифицированное обращение, сообщение или информация, поступившая в ИТ- отдел от пользователей структурных подразделений или сотрудника ИТ- отдела, обнаружившего инцидент, в форме телефонного звонка или электронного письма.
Запись	Электронный документ, оформленный в Системе управления задачами (Redmine), описывающий классифицированную Заявку. В процессе управления услугами существуют различные типы записей, например: Инцидент, Проблема, Поддержка, Изменение и т.д.
Единая точка контакта (ЕТК)	Специально организованный инструмент и группа сотрудников, сопровождающие прием, регистрацию Записей и первичную обработку Заявок: Номер телефона 213 и адрес электронной почты helpdesk@pandora.pri
Заявка на Поддержку	Заявка пользователя на выполнение стандартных (т.е. не содержащих рисков) операций в рамках действующего каталога ИТ-услуг. *Например: заявки на изменение учётных записей, предоставление доступа, установку стандартного ПО, сброс пароля, вопросы типа «Где найти ...?» и т.д.*
Изменение	Согласованное изменение или расширение существующего ИТ- актива. *Например, ИТ-изменением считается согласованное добавление, изменение и удаление:* *- поддерживаемого ИТ-оборудования, (клиентского оборудования, серверов, сетевых компонентов);* *- программного обеспечения (модулей прикладных программ, приложений различных видов, ИТ-систем;* *- технологических и инфраструктурных компонентов и т.п., включая релизы и обновления;* *- существующих технологических процессов, технической и бизнес документации.*
Проблема	Обстоятельство или событие, которое может вызвать или уже вызвало неисправности/инциденты. Их причины неизвестны и, соответственно, не устранены.
Ключевой показатель эффективности (KPI)	Метрика, измеряемый показатель, который используется для управления качеством ИТ-услуги, процесса, проекта или другой деятельности. Ключевые показатели эффективности используются для цифрового отражения и измерения ключевых факторов успеха.

5. Цель и обзор Процесса управления инцидентами

5.1 Цель Процесса управления инцидентами

Максимально быстрое восстановление нормального функционирования ИТ-услуги, работоспособности пользователей, а также снижение отрицательного воздействия на бизнес-процессы

организации. При этом необходимо обеспечить максимальное соблюдение согласованного уровня предоставления услуги.

5.2 Роли в Процессе управления инцидентами

Владелец Процесса управления инцидентами, Координатор качества Процесса управления инцидентами и Координатор инцидентов Процесса управления инцидентами определяют совместно:

- Цели Процесса управления инцидентами;
- Планы достижения целей; мероприятий по улучшению;
- Измеряемые показатели процессов, соответствующие целям.

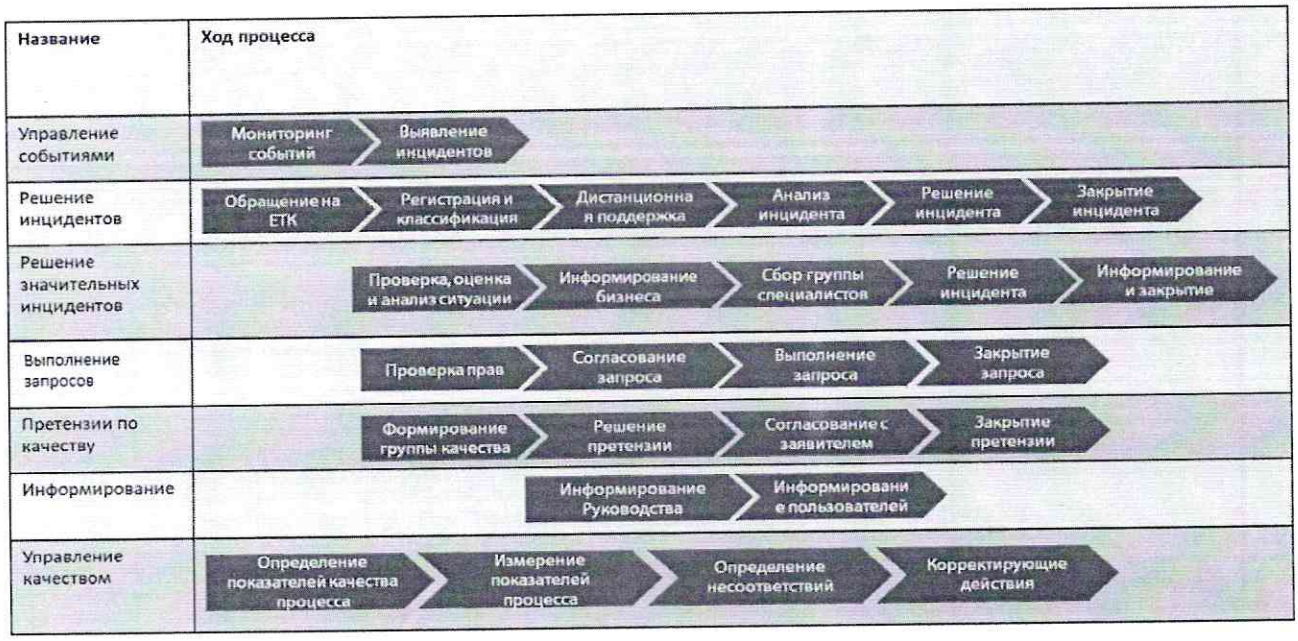
Роль	Задачи	Полномочия	Ответственность
Владелец Процесса управления инцидентами	- обеспечивает работоспособность Процесса управления инцидентами; -организует необходимое документирование Процесса управления инцидентами.	- утверждение целей, планов развития и измеряемых показателей Процесса управления инцидентами; - получение информации	- за качество и развитие Процесса управления инцидентами; - за выполнение целей Процесса управления инцидентами.
Единая точка контакта ИТ (ЕТК или Help Desk)	- регистрация, классификация инцидентов; - дистанционное устранение инцидентов в рамках первой помощи; - при невозможности дистанционного решения передача другим участникам процесса.	- принятие, оценка и классификация заявки; - регистрация инцидентов; - дистанционная поддержка пользователя; - маршрутизация инцидентов другим участникам процесса.	- за устранение неполадок и восстановление работы ИТ в рамках первой помощи; - за своевременную передачу незакрытых инцидентов другим участникам процесса; - за информирование пользователя.
Координатор качества процесса	- контроль и измерения Процесса в соответствие с согласованными показателями.	- предложение мероприятий по результатам контроля; - получение информации о Процессе и мерах по улучшению от Координатора инцидентов; - проведение анализа, определение соответствия.	- за достоверность и качество измерений Процесса.
Координатор инцидентов (Руководитель группы)	- организация и контроль работы Процесса в своей функциональной области; - сбор и консолидация необходимой отчетности; - помощь Менеджеру процесса в решении вопросов, связанных с Процессом управления инцидентами	- получение информации и отчетов от Менеджера инцидентов с целью контроля и оптимизации Процесса; - решение неопределенностей и конфликтов в своей группе, связанных с Процессом; - внедрение мероприятий по оптимизации и развитию Процесса в своей группе.	- за постановку задач Менеджеру инцидентов при поддержке Владельца Процесса управления инцидентами; - за реализацию и развитие Процесса в своем подразделении; - за определение необходимых технических условий для его реализации; - за разработку и поддержку Настоящего Руководства по Процессу управления инцидентами.
Таким образом, Координатор процесса и Менеджер процесса • *обеспечивают работоспособность процесса в своей функциональной области;* • *внедряют меры по оптимизации и развитию процесса.*			

Роль	Задачи	Полномочия	Ответственность
Менеджер значительных инцидентов (МЗИ)	- контроль за эффективной обработкой значительных инцидентов на оперативном уровне.	- формирование и координация работы группы по значительным инцидентам (ГЗИ); - обеспечение информацией Заказчика; - принятие решения для устранения значительного инцидента; - предложение/внедрение мер по оптимизации и развитию Процесса.	- за организацию работ по эффективной ликвидации значительных инцидентов; - за информирование Заказчика; - за анализ и ликвидацию причин произошедшего инцидента.
Менеджер значительных инцидентов (МЗИ) на период значительного инцидента имеет полномочия руководства.			

5.3 Обзор процесса управления инцидентами. Подпроцессы

Процесс управления инцидентами включает в себя 7 подпроцессов, представленных в таблице №1.

Таблица № 1



5.3.1 Управление событиями

Управление событиями основано на различных видах мониторинга, от визуального наблюдения до автоматического активного мониторинга ИТ-активов.

Информация о событиях поступает на ЕТК:

- в форме информационных сообщений от системы мониторинга,
- в форме заявок от сотрудников компании.

ЕТК классифицирует события и принимает решение о регистрации инцидента.

5.3.2 Решение инцидентов

5.3.2.1 Регистрация заявок

Началом процесса и ключевым действием является обращение на ЕТК и регистрация Заявки в системе RedMine.

Каналы обращений:

- Почтовый адрес helpdesk@pandora.pri — это предпочтительный путь передачи заявки, т.к. система автоматически регистрирует Запись на основании письма, которую специалисты ЕТК могут сразу категоризировать и принять в работу.
- Телефон 213 - заявку в системе регистрирует ЕТК и присваивает Заявке категорию и приоритет. В этом случае специалисты ЕТК регистрируют Заявку вручную и также проводят её категоризацию
- Автоматическое создание Заявки по событию из системы мониторинга. Специалисты ЕТК проверяют категоризацию и принимают Заявку в работу

Зарегистрированная Заявка получает статус «Новая»

5.3.2.2 Категоризация заявок

Приоритет инцидента определяется исходя из Срочности (класса риска актива) и Влияния. В RedMine приоритет записи обозначается таким образом: 4 – Низкий, 3 – Нормальный, 2 – Высокий, 1 – Срочный. Критерии определения приоритета инцидента представлены в таблице № 2.

Таблица № 2

Приоритет инцидентов			Срочность (класс риска ИТ актива)			
			1 Срочно	2 Высокий	3 Средний	4 Низкий
			Топ 10	Критичные	Продуктив	Прочие
Влияние	Значительный	Полный отказ ИЛИ воздействие на всех пользователей	1	1	2	3
	Высокий	Полный отказ ИЛИ воздействие на группу пользователей	1	2	3	3
	Средний	Небольшое снижение качества услуг ИЛИ воздействие на отдельных пользователей	2	3	3	4
	Низкий	Незначительное снижение качества услуг ИЛИ не затрагивает пользователей	3	3	4	4

5.3.2.3 Дальнейшая обработка заявок

Специалисты ЕТК проводит дальнейшую обработку и документирование записи инцидента в RedMine.

Специалисты ЕТК проводят первичный анализ, оказывают дистанционно первичную поддержку и закрывают инцидент, если возможно.

Если специалисты ЕТК не в состоянии устранить ошибку, инцидент передается соответствующим компетентным Менеджерам инцидентов.

После категоризации Заявки и нужный специалист начал с ней работать специалист изменяет её статус на «В работе»

Если необходимо подключение нескольких специалистов, специалист создает соответствующие связанные Записи в RedMine и назначают нужным специалистам.

Приоритет задач передается из исходной Записи. Специалисты вправе изменить установленный приоритет.

5.3.2.4 Документирование работ и закрытие Записи.

В ходе выполнения работ специалист, ответственный за Запись документирует основные шаги и существенные детали работ.

После выполнения необходимых работ специалист переводит Запись в статус «Решено». Если есть связанные Записи, то основную Запись нельзя закрыть до тех пор, пока не будут закрыты связанные.

В этом случае за выполнение Заявки в целом отвечает специалист, ведущий основную Запись.

Координатор инцидентов наблюдает за инцидентом на протяжении всего жизненного цикла инцидента, использует, при необходимости, ресурсы нужных специалистов и руководства.

5.3.3 Решение значительных инцидентов

ЕТК выполняет регистрацию и классификацию инцидента. Любой Инцидент с приоритетом 1 является кандидатом Значительного Инцидента. В этом случае приоритет должен быть согласован с Координатором инцидентов

Так как в случае Значительного Инцидента речь идёт о критической угрозе для бизнеса, помимо общих целей Процесса управления инцидентами выдвигаются также дополнительные цели:

- Определение Менеджера Значительного инцидента
- Запуск процесса обработки Значительного Инцидента;
- Назначение ответственного за информирование структурных подразделений и ИТ;
- Оптимальная коммуникация и распределение ресурсов ИТ во время обработки Инцидента;
- Понятный и единый ход процесса для всех подразделений предприятия и ИТ;
- Ясное распределение ответственностей;
- Однозначно определенные права принятия решений.

5.3.4 Выполнение запросов

Если после классификации Заявки выяснилось, что это Выполнение запросов, ЕТК действует по заранее определенным инструкциям. Производится проверка полномочий, согласование и выполнение запроса. После этого Заявка закрывается. При отсутствии полномочий Заявитель уведомляется, и Заявка закрывается, как выполненная.

5.3.5 Претензии по качеству

Претензии по качеству выполненных работ являются источником информации для анализа и улучшения качества услуг ИТ. Претензия принимается на ЕТК стандартным способом, регистрируется в привязке к соответствующей Записи и направляется Координатору инцидентов. Координатор инцидентов проводит анализ Претензии, планирует и обеспечивает выполнение корректирующих действий.

5.3.6 Информирование

В течение всего жизненного цикла заявки пользователь может получать информацию о её состоянии на ЕТК. Особое значение имеет информирование в подпроцессе управления значительными инцидентами.

5.3.7 Управление качеством

Для достижения целей процесса Владелец Процесса управления инцидентами и Координатор качества процесса определяют критические факторы успеха процесса и измеримые показатели качества. В ходе процесса Координатор качества проводит измерения показателей, выявляет несоответствия и, совместно с Координаторами инцидентов, определяет корректирующие действия. Ответственность за выполнение корректирующих действий лежит на Координаторах инцидентов при поддержке Владельца Процесса управления инцидентами.

6. Критические факторы успеха

- Регистрация, классификация и документирование всех инцидентов;
- Своевременное устранение инцидентов;
- Повышение квалификации участников процесса;
- Наличие базы знаний по известным ошибкам и решениям.

Описание KPI

Количество зарегистрированных инцидентов	
Описание:	Общее количество инцидентов за отчетный период. Необходимо убедиться, чтобы все инциденты были зарегистрированы и описаны
Общая цель: Все инциденты должны быть зарегистрированы и решены в рамках процесса. Это позволяет проводить анализ инцидентов, накапливать знания и повышать качество процесса и ИТ в целом.	
Точки измерения и источник данных: RedMine	**Способ расчёта:** Количество инцидентов за период
Комментарий:	Количество зарегистрированных инцидентов должно отражать реальное количество происходящих неисправностей в ИТ.

Время реакции	
Описание:	Время реакции – это время, требуемое для приёма Записи в обработку.
Общая цель: Время реакции должно оставаться минимальным.	
Точки измерения и источник данных: RedMine	**Способ расчета:** Время реакции = Время приема Заявки – Время перевода Заявки в статус «В работе»
Комментарий:	Сокращение времени реакции является важным, т.к. в этом временном промежутке не происходит непосредственная обработка Заявок, увеличивается время решения инцидентов.

7. Интерфейсы процесса

7.1 Интерфейс в Процесс управления изменениями

Для решения некоторых инцидентов требуется провести изменение на одном или нескольких компонентах ИТ окружения. В этом случае к записи инцидента присоединяется запись типа Изменение с соответствующим запросом. Из процесса возвращаются стандартные документированные изменения, которые можно применять для решения инцидентов без обращения в другой процесс.

7.2 Интерфейс в Процесс управления проблемами

После решения инцидента бывает неясна его причина и/или инцидент повторяется и регистрируется вновь. В этом случае к инциденту прикрепляется запись типа Проблема, в которой документируется процесс анализа, поиска и ликвидации причин инцидента. В процесс возвращаются проверенные обходные решения инцидентов, если причину инцидента ликвидировать не удается.

7.3 Интерфейс в Процесс управления активами

Любой инцидент связан с каким-либо активом ИТ. В запись инцидента передается информация о технических характеристиках актива. Информация об инциденте передается в Процесс управления активами с целью анализа качества актива.

7.4 Интерфейс в Процесс управления знаниями

Эффективные и проверенные способы решения инцидентов, документированные процедуры хранятся в базе управления знаниями. Успешное решение инцидента может стать кандидатом в базу знаний.

7.5 Интерфейс в Процесс управления непрерывностью ИТ

Любой инцидент влияет на непрерывность предоставления ИТ услуг и может быть причиной более серьезных последствий для бизнеса. В процесс управления инцидентами поступает информация о методах классификации инцидента. Из процесса поступает статистика для выявления критичных ИТ-услуг.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ изменения	Дата изменения	Основание для внесения изменений / Содержание изменений	Подпись лица, зарегистрировавшего изменение

ЛИСТ ОЗНАКОМЛЕНИЯ

Дата	Должность	Утверждено (дата)	Ф.И.О. работника	Подпись

Дата	Должность	Утверждено (дата)	Ф.И.О. работника	Подпись