КГУ «Управление архитектуры, градостроительства и земельных отношений города Нур-Султан»

УТВЕРЖДЕНО

Директор ТОО «АстанаГорАрхитектура» города Нур-Султан

_____ Кенжебеков Н. К.

«19» октября 20 20 г.

М. П.

УТВЕРЖДЕНО

Руководитель Управления архитектуры, градостроительства и земельных отношений города Нур-Султан

_____ Уранхаев Н. Т.

«19» октября 20 20 г.

М.П.

Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях Информационной системы «Геоинформационный портал города Нур-Султан» ГПГ.СМИБ.ИН.16.r02.20

г. Нур-Султан
2020 г.

1. Область применения

Целью настоящего документа является описание инструкций о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта ИС.

2. Нормативные ссылки

Настоящий документ содержит указания к практическому исполнению требований, изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

3. Термины, определения и сокращения

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

4. Общие положения

Ситуация, возникающая в результате нежелательного воздействия на ИС, приведшая к угрозе ИБ называется внештатной (кризисной). Внештатная (кризисная) ситуация может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий ситуаций и стихийных бедствий.

Для обеспечения непрерывной работы компонентов ИС сотрудники проекта обязаны следовать требованиям настоящей инструкции, Правилам по обеспечению непрерывной работы активов, связанных со средствами обработки информации и Плану мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации ИС.

Для эффективной реализации мероприятий по реагированию в случае внештатных ситуаций должны проводиться регулярные тренировки по различным внештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.

Ответственным за оповещение об инцидентах ИБ, назначается СОИБ и администраторы ИС.

По степени серьезности и размерам наносимого ущерба внештатные (кризисные) ситуации разделяются на следующие категории:

1) угрожающая - приводящая к полному выходу из строя ИС и неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации.

2) серьезная - приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере

производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

К угрожающим внештатным (кризисным) ситуациям относятся:

- нарушение подачи электроэнергии в здании;
- выход из строя сервера ИС (с потерей информации или без потери);
- частичная потеря информации на сервере ИС без потери его работоспособности;
- выход из строя сети проекта (физической среды передачи данных);
- компрометация учетных данных пользователя
- отказ кондиционера воздуха в серверном помещении;
- пожарная тревога в технологическом помещении;
- затопление технологического помещения;
- стихийные бедствия и техногенные аварии;
- массовые беспорядки в непосредственной близости от зон безопасности проекта ИС.

К серьезным внештатным (кризисным) ситуациям относятся:

- выход из строя отдельных компонент ИС (с потерей информации или без потери);
- частичная потеря информации на сервере без потери его работоспособности;
- компрометация учетных данных системного администратора;
- компрометация учетных данных СОИБ.

Источники информации о возникновении внештатной (кризисной) ситуации:

- сотрудники, обнаружившие подозрительные изменения в работе или конфигурации системы, или средств ее защиты в своей зоне ответственности;
- пользователи ИС;
- средства защиты, обнаружившие внештатную (кризисную) ситуацию;
- системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения внештатной (кризисной) ситуации;
- официальные источники информации (государственные СМИ, СМС рассылки МЧС и др.).

При выявлении любой внештатной ситуации пользователь, сотрудник проекта ИС обязан проинформировать СОИБ, менеджера проекта и руководство Организации.

Важнейшими аспектами успешных действий по минимизации ущерба от возникновения внештатных ситуаций являются:

– предотвращение возникновения внештатных ситуаций, путем соблюдения установленных требований ИБ и техники безопасности при эксплуатации оборудования и ПО;

– своевременное информирование о возникновении внештатной ситуации;

– согласованность действий сотрудников проекта в ходе внештатной ситуации;

– выработка решений по действиям во внештатных ситуациях на основании полученного опыта по их недопущению и устранению.

Все пользователи, работа которых может быть нарушена в результате возникновения внештатной (кризисной) ситуации, должны немедленно оповещаться СОИБ посредством электронной почты или средствами телефонной связи. Дальнейшие действия по устранению причин нарушения работоспособности ИС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями администраторов и пользователей ИС.

Каждая внештатная (кризисная) ситуация должна анализироваться СОИБ при участии системного администратора и менеджера проекта. По результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п., при необходимости должно производиться расследование причин ее возникновения, сбор доказательств, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

Внештатные (кризисные) ситуации могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ и данных (используя резервные копии) в случае их уничтожения или порчи в угрожающих или серьезных внештатных (кризисных) ситуациях обеспечивается резервным копированием и внешним (по отношению к основным компонентам системы) хранением копий. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся на безопасном расстоянии от места наступления внештатной (кризисной) ситуации.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность и выполнение задач ИС (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

Не менее двух раз в год СОИБ должен осуществлять контроль за выполнением профилактических действий для предотвращения возникновения внештатных или кризисных ситуаций.

Все программные средства, используемые в системе, должны иметь дистрибутивные пакеты.

Необходимые действия системных администраторов ИС по созданию, хранению и использованию резервных копий программ и данных отражены в Регламент резервного копирования и восстановления информации.

5. Управление инцидентами информационной безопасности

Оповещение о событиях высокой и критичной степени важности для информационной безопасности и об обнаруженных уязвимостях

В случае обнаружения или подозрения на обнаружение инцидента информационной безопасности, внештатной ситуации или иного события, которое может стать причиной нарушения ИБ и/или нарушения работы ИС (согласно утвержденному Перечню возможных причин нарушения непрерывности процессов обеспечения ИБ и бизнес-процессов, работы активов и возникновения внештатных ситуаций), лицо обнаружившее такое событие должно оповестить СОИБ, оповестить руководство Организации (по каналам связи указанных в Памятке с телефонами экстренных служб, служб обеспечения безопасности и ответственных сотрудников), предпринять соответствующие действия согласно настоящей инструкции и утвержденному Плану мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации в границах своих должностных обязанностей, своей ответственности и компетентности.

Каждый сотрудник Организации, работник нанятый по договору, сотрудники подрядных организаций несут ответственность за свои действия или бездействие повлекшие за собой ущерб в соответствии с действующим Законодательством Республики Казахстан.

Оповещения о нарушениях и недостатках информационной безопасности.

В Настоящий документ, обеспечивает оперативность оповещения о событиях информационной безопасности и нарушениях, связанных с информационными системами, а также своевременность применения корректирующих действий.

На ответственного за обеспечение ИБ возлагается обязанность информировать, консультировать и вести разъяснительные работы с сотрудниками проекта, сотрудниками поставщиков товаров и услуг и сотрудниками партнеров о порядке действий в случае инцидентов по ИБ и во внештатных ситуациях.

Сотрудники проекта, сотрудники поставщиков товаров и услуг, сотрудники партнеров и пользователи услуг Организации должны немедленно сообщать о любых наблюдаемых или предполагаемых инцидентах ответственному за обеспечение ИБ.

Оповещение о случаях нарушения информационной безопасности

Настоящий документ, устанавливает порядок информирования об инцидентах ИБ, а также порядок реагирования на инциденты, устанавливающая действия, которые должны быть предприняты после получения сообщения об инциденте ИБ.

Об инцидентах нарушения информационной безопасности необходимо информировать ответственного за обеспечение ИБ, менеджера проекта и руководство Организации.

Контакты для оповещения ответственного за обеспечение ИБ должны быть общедоступны, сам ответственный за обеспечение ИБ всегда доступен и в состоянии обеспечить своевременное адекватное реагирование.

О случаях нарушения информационной безопасности следует сообщать по соответствующим каналам управления незамедлительно, насколько это возможно.

На ответственного за обеспечение ИБ возлагается обязанность информировать, консультировать и вести разъяснительные работы с сотрудниками проекта, сотрудниками поставщиков товаров и услуг и сотрудниками партнеров о порядке действий в случае инцидентов по ИБ и во внештатных ситуациях.

Все сотрудники, подрядчики и пользователи услуг Организации должны быть ознакомлены с процедурой информирования об инцидентах нарушения информационной безопасности, а также проинформированы о необходимости незамедлительного сообщения об инцидентах.

Настоящий документ, включает:

a) процедуры обратной связи по результатам реагирования на инциденты нарушения информационной безопасности. После чего, этот вопрос должен быть решен и закрыт;

b) формы информирования об инцидентах нарушения информационной безопасности для поддержки действий информирования, и помощи информирующему лицу, чтобы он запомнил все необходимые действия в случае инцидентов нарушения информационной безопасности;

c) правильное поведение в случае инцидентов нарушения информационной безопасности, т.е.:

1) незамедлительно принимать к сведению все важные детали (например, тип несоответствия или нарушения, возникшие при сбоях системы, сообщения на экране, странное поведение);

2) не предпринимать самостоятельных действий, а следует немедленно известить соответствующее контактное лицо или администратора безопасности;

d) установление мер дисциплинарной ответственности сотрудников, подрядчиков или пользователей сторонних организаций, нарушивших требования безопасности;

e) регистрацию инцидентов ИБ и внештатных ситуаций в журналах Журнал регистрации инцидентов ИБ, Журнал учета внештатных ситуаций.

В условиях повышенного риска и там, где это необходимо, должен быть предусмотрен механизм автоматического оповещения ответственных лиц.

Примерами событий и инцидентов нарушения информационной безопасности являются:

a) потеря сервиса, оборудования или средств;
b) системные сбои или перегрузки;
c) человеческие ошибки;
d) несоблюдения политики или рекомендаций;
e) нарушения физических мер безопасности;
f) безудержные системные изменения;
g) сбои программного обеспечения или аппаратных средств;
h) нарушения прав доступа.

Ответственный за обеспечение по ИБ должен относится с повышенным вниманием к аспектам конфиденциальности, а инциденты информационной безопасности должны быть использованы в подготовке пользователей к осведомленности, например, того, что могло бы произойти, как реагировать на такие инциденты, и как избежать их в будущем.

Чтобы иметь возможность правильно сообщить о событиях и инцидентах информационной безопасности, необходимо собрать доказательство как можно быстрее после их возникновения.

Неисправности или другие неправильные режимы системы могут стать индикатором атаки безопасности или фактическими нарушениями безопасности, и, следовательно, должны быть сразу уведомлены как инциденты информационной безопасности.

Оповещение о недостатках безопасности

Сотрудники проекта, сотрудники поставщиков товаров и услуг, сотрудники партнеров и пользователи услуг Организации, должны незамедлительно сообщать о любых замеченных или предполагаемых нарушениях безопасности в ИС или услугах в порядке, установленном в настоящем документе.

Для предотвращения нарушений информационной безопасности, сотрудники проекта, сотрудники поставщиков товаров и услуг, сотрудники партнеров и пользователи услуг Организации, должны сообщать незамедлительно о возможных причинах и недостатках ИБ для принятия решений.

Ответственный за обеспечение ИБ обязан информировать сотрудников проекта, сотрудников поставщиков товаров и услуг, сотрудников партнеров и пользователей услуг Организации о порядке оповещения о недостатках безопасности и что они не должны ни при каких

обстоятельствах не пытаться доказать предполагаемые недостатки режима ИБ или уязвимости ИС.

Попытки самостоятельного поиска доказательства недостатков могут быть истолкованы как потенциальные злоупотребления ИС и могут также привести к повреждению информации или услуг и привести к правовой ответственности за такие действия.

6. Управление инцидентами информационной безопасности и его усовершенствование

Обязанность за управление инцидентами информационной безопасности и за усовершенствование этого процесса возлагается на ответственного за обеспечение ИБ.

Настоящий документ определяет обязанности и порядок управления инцидентами ИБ для обеспечения быстрой и организованной реакции на нарушения информационной безопасности, а также описывает процесс непрерывного усовершенствования мониторинга, оценки, общего управления инцидентами информационной безопасности, и сбор доказательств.

Ответственность и процедуры

Настоящий документ устанавливает ответственность руководства и процедуры, позволяющие обеспечить быстрое, эффективное и последовательное реагирование на инциденты информационной безопасности.

Руководство Организации ставит следующие цели в области управления инцидентами информационной безопасности проекта ИС:

a) мониторинг и анализ событий ИТ-инфраструктуры проекта и смежных областей деятельности с целью превентивного прогнозирования нежелательных событий ИБ;

b) своевременное и оперативное реагирование на поступающие сообщения о недостатках безопасности;

c) своевременное и оперативное реагирование на инциденты ИБ;

d) полноценное и всеобъемлющее расследование инцидентов ИБ для выяснения их причин;

e) разработка, таких корректирующих действий, которые предотвратили бы повторение инцидентов ИБ;

f) применение соответствующих корректирующих решений;

g) мониторинг и анализ внедрения корректирующих решений для определения их эффективности.

В дополнение к оповещению о событиях информационной безопасности и нарушениях, для обнаружения инцидентов информационной безопасности, осуществляется мониторинг использования ИС, а также средства предупреждения и уязвимостей ПО.

В отношении инцидентов нарушения информационной безопасности Инструкция о порядке действий пользователей по реагированию на

инциденты ИБ и во внештатных (кризисных) ситуациях описывает использование следующих мер:

a) определены процедуры в отношении критических инцидентов нарушения информационной безопасности:

1) недоступность информационной системы;

2) воздействие природно-климатических условий;

3) пожар или возгорание;

4) нарушение политики информационной безопасности и других НТД в области информационной безопасности;

b) в дополнение к обычным планам обеспечения непрерывности, на случай непредвиденных ситуаций, описаны процедуры выполнения требований:

1) анализ и идентификация причины инцидента;

2) ограничение распространения;

3) планирование и внедрение средств, предотвращающих повторное проявление инцидентов, при необходимости;

4) взаимодействия с лицами, на которых инцидент оказал воздействие участвующих в устранении последствий инцидента;

5) информирования о действиях соответствующих должностных лиц;

c) журналы аудита и аналогичные свидетельства собираются в установленном порядке (13.2.3) и защищены соответствующим образом с целью:

1) внутреннего анализа проблемы;

2) использования как доказательство в отношении возможного нарушения условий контракта, нарушения требований законодательства или, в случае гражданских или уголовных судебных разбирательств, касающихся, например, защиты персональных данных или неправомочного использования компьютеров;

3) ведения переговоров относительно компенсации ущерба с поставщиками программного обеспечения и услуг;

d) действия по устранению сбоев систем и ликвидации последствий инцидентов нарушения информационной безопасности тщательно контролируются, процесс и результаты документируются. СМИБ в целом обеспечивает уверенности в том, что:

1) только полностью идентифицированному и авторизованному персоналу предоставлен доступ к системам и данным в среде промышленной эксплуатации (6.2 в отношении доступа третьей стороны);

2) все действия, предпринятые при чрезвычайных обстоятельствах, подробно документально оформлены;

3) о действиях, предпринятых при чрезвычайных обстоятельствах, сообщено руководству Организации, и они должны быть проанализированы в установленном порядке;

4) целостность бизнес-систем и система контроля подтверждены в минимальные сроки.

Руководство Организации оставляет за собой обязательства по обеспечению быстрого и результативного реагирования на инциденты ИБ, внештатные ситуации и события, которые могут стать причиной нарушения непрерывности процессов обеспечения ИБ и бизнес-процессов, работы активов и возникновения внештатных ситуаций, а именно (но не ограничиваясь перечисленным):

1) конфиденциальность любого обращения;

2) полюбовное примирение (если последствия события не повлекли административное и/или уголовное преследование);

3) смягчение или не применение административного наказания со стороны Организации (если последствия события не повлекли административное и/или уголовное преследование);

4) поощрение и/или премирование положительно отличившихся лиц.

Руководство Организации возлагает на ответственного за обеспечение ИБ обязанности по управлении инцидентами ИБ.

Инциденты нарушения информационной безопасности могут выходить за пределы Организации. Для реагирования на такие инциденты ответственный за обеспечение ИБ и руководство Организации поддерживает контакты с соответствующими компетентными органами.

Извлечение уроков из инцидентов информационной безопасности

Настоящий документ определяет механизмы, позволяющие вести мониторинг и регистрацию инцидентов информационной безопасности.

Информацию, полученную из оценки инцидентов информационной безопасности, используют для идентификации повторяющихся или значительных инцидентов.

Оценка инцидентов информационной безопасности может указывать на необходимость в совершенствовании существующих или внедрении дополнительных мероприятий по управлению информационной безопасностью.

Оценка инцидентов информационной безопасности может стать причиной инициации процесса аудита, полученные результаты следует учитывать при пересмотре политики информационной безопасности.

Сбор доказательств

В случае необходимости должен проводиться сбор доказательств инцидентов информационной безопасности, который может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, а материалы представляться в соответствии с требованиями действующего законодательства РК, представителями компетентных органов.

Все сотрудники проекта, сотрудники поставщиков товаров и услуг, сотрудники партнеров и пользователи услуг Организации обязаны содействовать и помогать ответственным лицам в сборе доказательств.

В общем случае при сборе доказательств необходимо придерживаться следующих правил:

a) допустимость свидетельств: действительно ли свидетельства могут использоваться в суде или нет;

b) весомость свидетельств: качество и полнота свидетельств.

Чтобы достичь признания допустимости свидетельств, информационная ИТ-инфраструктура проекта должна соответствовать всем юридическим требованиям и правилам в отношении допустимых свидетельств:

a) синхронизация времени с официальным эталоном времени РК;

b) авторизация с использованием, законодательно закрепленным, эквивалентом ручной подписи и персональных данных пользователей;

c) подписание электронных документов ЭЦП;

d) шифрование (там, где это необходимо) с использованием алгоритмов высокой надежности и авторизацией до передачи данных;

e) использование цифровых сертификатов подлинности, признанных на территории РК;

f) надежная защита ИТ-инфраструктуры от вторжения из вне и от утечек информации;

g) журналирование событий ИТ-инфраструктуры, действий пользователей и обслуживающего персонала;

h) обеспечение сохранности и неизменности журналов и зарегистрированных событий на длительный срок;

i) использование актуальных средств защиты от вредоносного кода;

j) контроль действий обслуживающего персонала;

k) средства предотвращения вмешательства обслуживающего персонала в работу ИТ-инфраструктуры с целью изменения данных, сокрытия своего вмешательства или фальсификации событий;

l) мониторинг и ликвидация уязвимостей ИТ-инфраструктуры;

m) автоматическая реакция и оповещение о событиях в ИТ-инфраструктуре;

n) мониторинг доступности ИС;

o) контроль управления доступом во все помещения проекта;

p) защита физического периметра проекта.

Весомость свидетельств должна соответствовать требованиям действующего законодательства. Чтобы достичь качества и полноты свидетельств, необходимо наличие убедительных подтверждений свидетельств, что эти меры контроля (процесс сбора свидетельств) осуществлялись корректно и последовательно в течение всего периода, когда установленное свидетельство инцидента нарушения информационной безопасности было сохранено и обработано системой.

В общем случае, такие убедительные подтверждения могут быть достигнуты следующим образом:

a) для бумажных документов: оригинал хранится безопасным способом и фиксируется, кто нашел его, где он был найден, когда он был найден и кто засвидетельствовал обнаружение. Необходимо, чтобы любое исследование подтвердило, что оригиналы никто не пытался исказить;

b) для информации на компьютерных носителях: копии информации, для любых сменных носителей информации, для жестких или из основной памяти компьютера, следует выполнять таким образом, чтобы обеспечить их доступность. Журнал всех действий, выполненных в течение процесса копирования, необходимо сохранять, а сам процесс копирования необходимо документировать. Одну копию носителей информации и журнал следует хранить безопасным способом.

Любая работа, связанная с судебным разбирательством, должна осуществляться только на копиях доказательного материала. Целостность всего доказательного материала должна быть защищена. Копирование материала должно контролироваться надежным персоналом, а информация о том, где и когда был проведен процесс копирования, кто осуществлял, какие инструменты и программы были при этом использованы, должны регистрироваться.

Когда инцидент обнаруживается впервые, не очевидно, что он может привести к возможным судебным разбирательствам. Поэтому, существует опасность, что необходимое показание будет случайно разрушено прежде, чем осознана серьезность инцидента. В обязанности ответственного за обеспечение ИБ входит контроль сохранности всех необходимых материалов по каждому инциденту ИБ для дальнейших разбирательств.

Сбор доказательств может выходить за пределы ИТ-инфраструктуры проекта или сотрудники Организации могут не иметь права доступа к хранимой информации. В таких случаях следует воспользоваться консультацией юридических служб и уполномоченных органов для выполнения всех необходимых действий.

Процедура сбора доказательств внутри организации

В случае необходимости представления и сбора доказательств в целях применения дисциплинарных мер, внутри Организации ответственный за обеспечение ИБ инициирует процесс создания рабочей группы, разрабатывает и утверждает план работы группы.

В состав рабочей группы должны войти руководитель Организации, ответственный за обеспечение ИБ, ответственный сотрудник отдела кадров, системный администратор. Руководителем рабочей группы назначается руководитель Организации.

Сотрудник, подозреваемый в виновности инцидента ИБ, отстраняется от работы, может присутствовать при сборе доказательств, но не имеет права пользоваться средствами обработки информации Организации.

Сбор доказательств проводится в следующем порядке:

a) фиксирование состояния и резервное копирование компонентов ИТ-инфраструктуры проекта на момент регистрации инцидента ИБ с охватом временного интервала, включающего момент самого инцидента ИБ и более ранних событий;

b) поиск точного времени свершения инцидента ИБ и свидетельств причастности к нему каких-либо лиц;

c) изъятие и фиксирование состояния средств обработки информации подозреваемых лиц;

d) опрос с протоколированием подозреваемого о его действиях на момент свершения инцидента ИБ;

e) поиск подтверждающих или опровергающих доказательств, показания подозреваемых и их причастности к инциденту ИБ;

f) хронологическая расстановка событий до и после инцидента ИБ.

Все действия рабочей группы оформляются актом, все найденные цифровые доказательства подписываются ЭЦП всеми участниками рабочей группы.

Все материалы сбора доказательств должны храниться в защищенном месте. Результаты выносятся на рассмотрение рабочей группы с целью определения вины и меры дисциплинарного воздействия.

В случае если сотрудник не согласен с результатами служебного расследования или дисциплинарными мерами, он вправе оспорить результаты в установленном законодательством РК порядке.

7. Действия работников в кризисной ситуации

Действия работников в кризисной ситуации зависят от степени ее тяжести. В случае возникновения угрожающей или серьезной критической ситуации действия работников включают следующие этапы:

уведомление о возникновении внештатной ситуации (согласно перечню контактов компетентных органов):

а) в дневное время суток:

– лицо, обнаружившее внештатную (кризисную) ситуацию должно уведомить СОИБ, руководство Организации – устно, при необходимости письменно;

– СОИБ сообщает соответствующим компетентным органа (запрашивает Ф. И. О., должность и регистрационный номер);

– СОИБ регистрирует инцидент в журнале инцидентов ИБ и учета внештатных ситуаций;

– СОИБ оповещает пользователей и сотрудников проекта;

в) в ночное время суток:

– лицо, обнаружившее внештатную (кризисную) ситуацию должно уведомить СОИБ, руководство Организации – устно;

– СОИБ сообщает соответствующим компетентным органа (запрашивает Ф. И. О., должность и регистрационный номер);

– СОИБ регистрирует инцидент в журнале инцидентов ИБ и учета внештатных ситуаций;

– СОИБ оповещает пользователей и сотрудников проекта.

Действия по устранению причин нарушения работоспособности ИС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями сотрудников.

Событие в обязательном порядке регистрируется СОИБ в журнале инцидентов ИБ и учета внештатных ситуаций (по форме согласно Приложению 1), с указанием точного времени инцидента, краткого описания событий, с указанием Ф.И.О. оповещенных лиц, описание действий направленных на устранение кризисной ситуации и их результатов.

Вынос оборудования и документов из помещений Общества, если развитие внештатной ситуации этого потребует, осуществляются сотрудниками Организации, в рамках возложенных на них задач, только по согласованию с руководством Организации.

Контроль за организацией работ в кризисных ситуациях осуществляет СОИБ.

8. Перечень возможных внештатных или кризисных ситуаций, идентификация и действия по устранению

Недоступность информационной системы.

Описание:	Ситуация, когда пользователи по неизвестным причинам не могут получить доступ к ИС.
Действия по идентификации:	СОИБ принимает сообщение об инциденте, записывает Ф. И. О., должность, название организации, точный физический адрес сообщившего, контактный телефон и уточняет физический адрес места, IP-адрес от куда ИС недоступна. Регистрирует инцидент в журнале инцидентов ИБ и учета внештатных ситуаций. Передает информацию системному администратору. Системный администратор локализует проблему.
Действия по устранению:	Системный администратор приступает к ее устранению в зависимости от ее причин: проблема на стороне пользователя, проблема каналов связи от пользователя до сервера, проблема в границах серверного помещения, проблема с сервером ИС.
Результат:	Системный администратор информирует СОИБ о ликвидации ситуации. СОИБ делает соответствующую отметку в журнале инцидентов ИБ и учета внештатных ситуаций. И доводит результат до сведения пользователей.

Воздействие природно-климатических условий.

Описание:	Ситуации возникновения стихийных природно-климатических воздействий (землетрясение, наводнения, ураганы). Такие сведения могут быть получены из официальных источников, либо при непосредственном нахождении на месте.
Действия по идентификации:	В случае если в непосредственной близости от помещения с серверами ИС наблюдаются стихийных природно-климатических воздействий (землетрясение, наводнения, ураганы.) необходимо переходить к действиям по устранению.
Действия по устранению:	1) вызвать службу МЧС; 2) поставить в известность руководство Организации; 3) сделать отметку в журнале инцидентов ИБ и учета внештатных ситуаций.
Результат:	СОИБ делает соответствующую отметку в журнале инцидентов ИБ и учета внештатных ситуаций. И доводит результат до сведения пользователей.

Пожар или возгорание.

Описание:	Сведения возникновения пожара или возгорании могут быть получены из компетентных источников.
Действия по идентификации:	В случае если в непосредственной близости от помещения с серверами ИС наблюдаются пожар или возгорание необходимо переходить к действиям по устранению.
Действия по устранению:	1) вызвать пожарную службу тел: 101, звонок с моб. тел.: 010; 2) поставить в известность руководство Организации; 3) при необходимости организовать работу по эвакуации людей и имущества, устранению возгорания. 4) сделать отметку в журнале инцидентов ИБ и учета внештатных ситуаций.
Результат:	СОИБ делает соответствующую отметку в журнале инцидентов ИБ и учета внештатных ситуаций. И доводит результат до сведения пользователей.

Нарушение политики информационной безопасности и других НТД в области информационной безопасности.

Описание:	Сведения о нарушении политики информационной безопасности и других НТД в области информационной безопасности могут быть получены от пользователей, сотрудников проекта ИС, компетентных органов, систем автоматического оповещения и выявлены в процессе аудита.
Действия по идентификации:	Для выбора необходимы действий по ликвидации внештатной ситуации необходимо идентифицировать место нарушения, нарушителя и требования НТД по ИБ, которые были нарушены.
Действия по устранению:	1) лицо, ставшее свидетелем или обнаружившее нарушение режима ИБ должно оповестить СОИБ; 2) СОИБ должен оповестить руководство Организации; 3) СОИБ совместно с системным администратором и менеджером проекта должен выбрать срочные меры по ликвидации ситуации; 4) СОИБ должен сделать отметку в журнале инцидентов ИБ и учета внештатных ситуаций;
Результат:	СОИБ делает соответствующую отметку в журнале инцидентов ИБ и учета внештатных ситуаций. И доводит результат до сведения пользователей.

Выход из строя информационных и аппаратных активов ИС.

Описание:	Выход из строя программного обеспечения, серверного оборудования или информационного ресурса ИС.
Действия по идентификации:	Для выбора необходимы действий по ликвидации внештатной ситуации необходимо идентифицировать вышедшее из строя ПО, серверное оборудование или информационный ресурс ИС. Определить причину выхода из строя: ошибка в настройках, физическая неработоспособность.
Действия по устранению:	1) лицо, ставшее свидетелем или обнаружившее нарушение режима ИБ должно оповестить СОИБ; 2) СОИБ должен оповестить руководство Организации, и системного администратора ИС; 3) СОИБ совместно с системным администратором и менеджером проекта должен выбрать срочные меры по ликвидации ситуации; 4) СОИБ должен сделать отметку в журнале инцидентов ИБ и учета внештатных ситуаций; 5) в случае выхода из строя центрального узла ИС, с целью непрерывности работы, производится автоматическое переключение на резервный узел.

Результат:	СОИБ делает соответствующую отметку в журнале инцидентов ИБ и учета внештатных ситуаций. И доводит результат до сведения пользователей.

9. Действия при возникновении ситуаций, не подпадающих под перечисленный список

В случае возникновения внештатных ситуаций с ИС, не подпадающих под вышеперечисленный список необходимо:

1) поставить в известность СОИБ о возникшей ситуации;
2) поставить в известность руководство Организации о возникшей ситуации и другие компетентные органы;
3) СОИБ совместно с системным администратором и менеджером проекта должен выбрать срочные меры по ликвидации ситуации;
4) СОИБ должен сделать отметку в журнале инцидентов ИБ и учета внештатных ситуаций;
5) по окончании ликвидации внештатной ситуации СОИБ должен сделать отметку в журнале инцидентов ИБ и учета внештатных ситуаций.

10. Информирования об инцидентах нарушения ИБ подрядчиков и пользователей

Все сотрудники, подрядчики и пользователи, имеющие доступ к ИС, должны быть ознакомлены с настоящим документом, а также проинформированы о необходимости незамедлительного сообщения об инцидентах.

Сведения о имевшем место или происходящем в текущем времени инциденте должны быть доведены до сведения всех затрагивающих сторон.

11. Ответственность

СОИБ несет ответственность за:

a) контроль исполнения требований настоящего документа,
b) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

a) исполнение настоящей Инструкции.

Пользователи ИС:

b) исполнение настоящей Инструкции.

Приложение 1

Журнал инцидентов информационной безопасности и учета внештатных ситуаций Информационной системы «Геоинформационный портал города Нур-Султан» ГПГ.СМИБ.ИН.16-01.r02.20

№ п\п	Дата	Время	Источник сообщения (ФИО, организация, контакты)	Оповещенные сотрудники (ФИО, организация, контакты, рег №)	Описание инцидента	Локализация инцидента	Оповеститель (ФИО, организация, контакты)	Фактическая причина сбоя	Фактическая дата и время исправления	Предпринятые меры для устранения инцидента	Время простоя
1	2	3	4	5	6	7	8	9	10	11	12