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

УТВЕРЖДЕНО

Директор ТОО «АстанаГорАрхитектура» города Нур-Султан

_____ Кенжебеков Н. К.

«18» октября 2020 г.

М. П.

УТВЕРЖДЕНО

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

_____ Уранхаев Н. Т.

«19» октября 2020 г.

М. П.

Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации Информационной системы «Геоинформационный портал города Нур-Султан» ГПГ.СМИБ.ПР.04.r02.20

г. Нур-Султан
2020 г.

1. Область применения

Целью настоящего документа является описание правил по обеспечению непрерывной работы активов, связанных со средствами обработки информации, и определение порядка действий ответственных сотрудников Организации, 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

В рамках работ по обеспечению ИБ проводятся мероприятия по управлению непрерывностью бизнеса с целью минимизации отрицательных последствий, вызванных бедствиями и нарушениями безопасности (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий) до приемлемого уровня с помощью комбинирования предупреждающих и восстановительных мероприятий по управлению информационной безопасностью.

Необходимо, чтобы управление непрерывностью бизнеса включало мероприятия по управлению информационной безопасностью для идентификации и уменьшения рисков, ограничения последствий разрушительных инцидентов и обеспечения своевременного возобновления работы ИС.

Настоящий документ регламентирует:

1) идентификацию событий, которые являются причиной прерывания процессов функционирования объекта аттестации (планирование должно сопровождаться оценкой рисков);
2) определение процессов обеспечения непрерывности работы активов, занесенных в реестр активов в случае их выхода из строя;
3) разработку плана обеспечения непрерывности работы активов, связанных со средствами обработки информации, и их актуализация;

4) порядок тестирования и обновления планов развития существующих процессов по непрерывности работы активов;
5) назначение ответственных лиц за процессы функционирования объекта аттестации;
6) по проведению анализа плана мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов;
7) разработку плана восстановления объекта аттестации;
8) способы размещения оборудования снижающий риск возникновения угроз, опасностей и возможностей несанкционированного доступа;
9) способы защиты оборудования от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб;
10) требования к периодичности технического обслуживания оборудования для обеспечения непрерывности функционирования, доступности и целостности.

Для оперативного реагирования и организации работ по недопущению перерывов в работе ИС разработан и утвержден План мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации.

5. Включение информационной безопасности в процесс управления непрерывностью бизнеса

План мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации, объединяет ключевые элементы управления непрерывностью бизнеса:

a) понимание рисков, с которыми сталкивается ИС, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение ценности активов;

b) идентификацию всех активов ИС;

c) понимание возможных последствий нарушения работы ИС в случае незначительных или существенных инцидентов, потенциально угрожающих жизнедеятельности ИС, а также выбора средства и способов обработки информации;

d) амортизацию реализации угроз ИС;

e) идентификацию и рассмотрение реализации дополнительных профилактических и смягчающих мероприятий;

f) организацию работ по обеспечению непрерывного функционирования ИС;

g) формулирование и документирование плана обеспечения непрерывности бизнеса;

h) регулярное тестирование и обновление компонентов СМИБ ИС;

i) обеспечение органичного включения в процессы и структуру организации планов управления непрерывностью бизнеса.

Ответственность за координацию процесса управления непрерывностью возлагается на ответственного за обеспечение ИБ.

6. Непрерывность бизнеса и оценка риска

События, которые могут стать причиной прерывания работы ИС, должны быть связаны с оценками вероятности и степени воздействия таких прерываний, а также с их последствиями для информационной безопасности.

Необходимо, чтобы планирование непрерывной работы ИС начиналось с идентификации событий, которые могут быть причиной прерывания бизнес-процессов. Планирование должно сопровождаться оценкой рисков с целью определения возможности и последствий этих прерываний (как с точки зрения масштаба повреждения, так и периода восстановления).

Оценка риска должна распространяться на все компоненты ИС и не ограничиваться только средствами обработки информации, но должна включать результаты, определенные для информационной безопасности.

В зависимости от результатов оценки рисков необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности бизнеса. Разработанный план должен быть утвержден руководством Организации по выполнению данной стратегии.

7. Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность

Для оперативного реагирования и организации работ по недопущению перерывов в работе ИС разработан и утвержден План мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации.

Необходимо, чтобы план обеспечения непрерывной работы ИС предусматривал следующие мероприятия по обеспечению безопасности:

a) определение и согласование всех обязанностей и процедур непрерывности бизнеса;

b) идентификацию приемлемых потерь информации и услуг;

c) внедрение процедур, обеспечивающих возможность восстановления бизнес- процессов и доступность информации в требуемое время. Особое внимание следует уделять оценке зависимости бизнеса от внешних факторов и существующих контрактов;

d) операционные процедуры, предназначенные для завершения процесса полного восстановления и восстановления потерянных данных;

e) документирование согласованных процедур и процессов;

f) соответствующее обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление;

g) тестирование и обновление планов обеспечения непрерывности бизнеса.

План мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации, утверждается руководством Организации и хранится в защищаемых помещениях проекта. Копии утвержденного плана передаются сотрудникам Проекта ИС.

8. Структура планов обеспечения непрерывности бизнеса

Форма структуры плана мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации отражена в Приложении 1

План мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации, определяет подход к обеспечению непрерывной работы ИС, быстрой идентификации, ликвидации и минимизации ущерба от инцидентов ИБ и внештатных (кризисных) ситуаций.

План непрерывности должен четко определять условия его реализации, а также должностных лиц, ответственных за выполнение каждого его пункта.

Ответственными лицами за процессы функционирования ИС являются:

- руководство Организации;
- ответственный за обеспечение ИБ,
- менеджер проекта ИС;
- администраторы ИС.

Зоны ответственности каждого сотрудника определяются утвержденным Планом мероприятий по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации ИС.

При выявлении новых требований необходимо вносить соответствующие корректировки в процедуры на случай чрезвычайных ситуаций, НТД по ИБ и операционные процедуры. Процедуры должны быть включены в пределах программы управления ИБ ИС, чтобы гарантировать соответствующее направление для решения вопросов непрерывной работы ИС.

За план непрерывности отвечает ответственный за обеспечение ИБ.

Необходимо, чтобы структура плана обеспечения непрерывности отвечала требованиям информационной безопасности и содержала следующее:

a) в плане должен соблюдаться порядок исполнения его пунктов;

b) процедура на случай внештатных ситуаций, которые должны быть предприняты после инцидента ИБ;

c) процедуры переключения на резервный узел ИС;

d) временные операционные процедуры, обеспечивающие завершение полного восстановления и восстановления потерянных данных;

e) процедура возобновления работы, которые описывают необходимые действия для возвращения к нормальному режиму ведения бизнеса;

f) график поддержки плана, который определяет сроки и методы тестирования, а также описание процесса поддержки плана;

g) мероприятия по обучению персонала, которые направлены на понимание процессов обеспечения непрерывности бизнеса сотрудниками, и поддержание постоянной эффективности этих процессов;

h) обязанности должностных лиц, ответственных за выполнение каждого пункта плана;

i) критические активы и ресурсы должны быть готовы к выполнению процедур, предусмотренных на случай внештатных ситуаций, систему восстановления и процедуры возобновления.

Для обеспечения непрерывности работы активов ИС в случае их выхода из строя реализован механизм отказоустойчивой работы серверного оборудования и программного обеспечения компонентов ИС.

В процесс обеспечения непрерывности работы активов входят следующие механизмы:

a) установлены и настроены два взаимозаменяемых узла ИС: основной и резервный;

b) организован защищенный шифрованием канал связи между основным узлом и резервным;

c) настроена асинхронная репликация данных информационного ресурса ИС и данных конфигурационных файлов между основным и резервным узлом ИС;

d) настроено резервное копирование данных информационного ресурса ИС и данных конфигурационных файлов между узлами в обоих направлениях;

e) настроено регулярное резервирование данных информационного ресурса ИС и данных конфигурационных файлов на съемные носители;

f) настроено автоматическое переключение на резервный узел в случае выхода из строя основного узла;

g) оборудование размещено в специализированных гермозонах с контролем электропитания, резервным электропитанием, стабилизаторами напряжениями, температуры, охраной сигнализации, круглосуточным дежурством ответственных сотрудников, видеонаблюдением и системой автоматического пожаротушения.

Ответственным за восстановление работоспособности ИС является системный администратор. Обязанности по контролю за процессом восстановления возлагаются на ответственного за обеспечение ИБ.

План восстановления полноценной работы ИС заключается в следующих этапах:

a) идентификация программных и аппаратных компонентов ИС, вышедших из строя;

b) замена вышедшего из строя серверного оборудования или отдельных ее частей;

c) установка (при необходимости), в соответствии с требованиями Руководства системного администратора, системного и прикладного программного обеспечения;

d) восстановление из резервных (в соответствии с Регламентом резервного копирования и восстановления информации) копий файлов конфигурации системного и прикладного программного обеспечения;

e) восстановление из резервных (в соответствии с Регламентом резервного копирования и восстановления информации) данных информационного ресурса ИС;

f) тестирование результатов восстановления и конфигурации с целью выявления ошибок;

g) внесение соответствующих записей в Журнал резервного копирования, восстановления, тестирования резервных копий и тестирования средств резервирования;

h) подключение узла в качестве основного или резервного.

9. Тестирование, поддержка, анализ и пересмотр планов по обеспечению непрерывной работы ИС

План по обеспечению непрерывности тестируется для обеспечения знания своих обязанностей всеми сотрудниками проекта восстановления и другим персоналом, имеющим к этому отношение, а также для проверки полноты и согласованности действий ответственных сотрудников.

План по обеспечению непрерывности тестируется не реже одного раза в год (в соответствии с Графиком аудита информационной безопасности) и обновляется для обеспечения уверенности в его актуальности и эффективности.

План подлежит полному пересмотру в следующих случаях:

a) при изменении перечня решаемых задач, конфигурации технических и программных средств ИС, приводящих к изменению технологии обработки информации;

b) при изменении приоритетов в значимости угроз безопасности ИС.

План подлежит частичному пересмотру в следующих случаях:

a) при изменении конфигурации, добавлении или удалении программных и технических средств в ИС, не изменяющих технологию обработки информации;

b) при изменении конфигурации используемых программных и технических средств;

c) при изменении состава, обязанностей и полномочий сотрудников и пользователей системы.

В случае частичного пересмотра происходит обновление плана и могут быть добавлены, удалены или изменены компоненты плана, ответственные сотрудники, действия, контактные данные участников.

План обеспечения непрерывности тестируется путем проверки исполнения его требований с использованием требований документов по ИБ Необходимо обеспечить регулярное тестирование каждого пункта плана, при этом могут использоваться следующие методы:

a) тестирование ("имитация прогона") различных сценариев (обсуждение мер по восстановлению бизнеса на различных примерах прерываний);

b) моделирование (особенно для тренировки персонала по выполнению своих функций после инцидента и перехода к кризисному управлению);

c) тестирование технического восстановления (обеспечение уверенности в эффективном восстановлении информационных систем);

d) проверка восстановления в альтернативном месте (бизнес-процессы осуществляются параллельно с операциями по восстановлению в удаленном альтернативном месте);

e) тестирование средств и сервисов-поставщиков (обеспечение уверенности в том, что предоставленные сторонними организациями сервисы и программные продукты удовлетворяют контрактным обязательствам);

f) «генеральные репетиции» (тестирование того, что организация, персонал, оборудование, средства и процессы могут справляться с прерываниями).

Обязанности по тестированию, проведению регулярных пересмотров плана по обеспечению непрерывности возлагаются на ответственного за ИБ.

По результатам тестирования (а также применения на практике) ответственный за обеспечение ИБ проводит анализ План по обеспечению непрерывности с целью:

a) выявления мест для оптимизации процессов обеспечения непрерывности;

b) выявления конфликтующих действий ответственных сотрудников при исполнении Плана по обеспечению непрерывности;

c) проверки адекватности временных рамок на исполнение требований по непрерывности работы активов;

d) проверки правильного распределения обязанностей ответственных сотрудников при выполнении Плана по обеспечению непрерывности;

e) проверки адекватности применяемых мер по обеспечению непрерывности работы активов;

f) соответствие применяемых мер по обеспечению непрерывности работы активов требованиям Политики по ИБ.

Результаты тестирования, анализа и пересмотра оформляются в виде отчета и передаются руководству Организации на рассмотрение необходимости обновления плана.

Идентифицированные изменения в работе ИС, еще не отраженные в плане по обеспечению непрерывности, должны быть учтены путем соответствующих обновлений плана. Все сотрудники проекта должны быть ознакомлены с изменениями плана.

Примерами ситуаций, которые могли бы потребовать обновления плана, включают приобретение нового оборудования или обновление операционных систем, а также изменения, связанные с:

a) персоналом;
b) адресами или номерами телефонов;
c) стратегией бизнеса;
d) местоположением, средствами и ресурсами;
e) законодательством;
f) подрядчиками, поставщиками и основными клиентами;
g) процессами (как новыми, так и изъятыми);
h) рисками (операционными и финансовыми).

10. способы защиты оборудования от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб

Ключевые требования при обеспечении защиты оборудования от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб:

Размещение оборудования в специализированных помещениях. В специализированные помещения должны быть оснащены системами:

1. контроля и управления доступом;
2. обеспечения микроклимата;
3. охранной сигнализации;
4. видеонаблюдения;
5. пожарной сигнализации;
6. пожаротушения;
7. гарантированного электропитания;
8. заземления;

Коммуникации передачи воды (отопления и холодного водоснабжения) не должны проходить через помещения.

Распределенная структура системы бесперебойного электропитания

В распределенной системе бесперебойного электроснабжения каждый потребитель (или группа потребителей) использует отдельный локальный источник бесперебойного питания (ИБП). Основными преимуществами такой системы являются возможность ее реализации без переделки сетевой

разводки в здании, особенно при использовании «розеточных» ИБП, простота наращивания и изменения конфигурации. При отказе одного из ИБП происходит отключение только части системы, и, при наличии аналогичного ИБП в «холодном» резерве, последствия отказа могут быть устранены в течение нескольких минут.

Система бесперебойного электропитания централизованной структуры

При централизованной структуре система бесперебойного энергоснабжения включает в себя один ИБП (или их комплекс), к которому подключены все значимые потребители электроэнергии. Основой построения систем гарантированного энергоснабжения (СГЭ) являются мощные ИБП, имеющие функцию двойного преобразования напряжения (on-line) и позволяющие получать электроэнергию надлежащего качества. Эти устройства обеспечивают надежную работу подключенного к ним оборудования как в штатном режиме (при наличии электропитания на входе), так и в автономном режиме (при отключении входного напряжения) за счет энергии, накопленной в аккумуляторных батареях. На сегодняшний день время автономной работы таких систем электропитания составляет, как правило, до нескольких часов.

Основное преимущество, которым обладает система бесперебойного питания с централизованной структурой, это концентрация запаса мощности в одном месте и большая емкость батарей. Такая система менее чувствительна к локальным перегрузкам и может выдержать даже короткое замыкание, переходное сопротивление которого превышает величину, определяемую запасом выходной мощности ИБП. Кроме того, при централизованной схеме построения системы бесперебойного питания можно увеличить время автономной работы основного оборудования за счет простого отключения менее ответственных потребителей энергии.

Двухуровневая система бесперебойного электропитания

Чтобы избавиться от недостатков, присущих каждой из вышеописанных систем, на практике применяют смешанную структуру, которая представляет собой комбинацию централизованной и распределенной схем. С точки зрения оптимизации мощности и стоимости оборудования задача проектировщика в этом случае состоит в определении ключевых потребителей и минимизации числа их групп путем конфигурирования вычислительной сети. При выборе двухуровневой структуры, кроме установки одного ИБП большой мощности, отдельные потребители защищаются с помощью локальных менее мощных ИБП. Целью такого резервирования является защита ответственного оборудования, например, файловых серверов, рабочих станций управления ЛВС, коммуникационного оборудования и системы связи от обесточивания из-за аварий в электросети.

Функциональное разделение систем бесперебойного питания

Области применения ИБП в системах бесперебойного питания можно разделить по следующим функциональным признакам: защита

электронной обработки данных, защита общих производственных процессов и защита критических процессов.

Защита электронной обработки данных. Информационные технологии породили массовый рынок ИБП, с которым стал ассоциироваться термин «коммерческие ИБП». Типичные области применения таких систем в сфере информационных технологий — центры обработки данных, банки, страховые компании. Нарушения в системе подачи переменного тока могут негативным образом повлиять на процесс обработки данных и работу систем связи. Однако они не создают существенных рисков для жизни людей или их собственности.

Защита общих производственных процессов. Используемые в данном сегменте ИБП относят к промежуточному классу «легких промышленных систем». Они предназначены для защиты процессов, не приводящих к необратимым тяжелым последствиям даже в случае длительного пропадания входного тока, хотя нарушения в работе электроснабжения этих объектов способны привести не только к простою производственных линий, но и к большим затратам времени для восстановления и запуска производственной линии после сбоя. Типичные примеры областей применения — фармакологическая и пищевая отрасли.

Защита критических процессов. ИБП, предназначенные для этой цели, традиционно называются «промышленными» ИБП, при этом сфера их применения не ограничивается защитой систем автоматического управления на промышленных предприятиях. Наглядный пример критических приложений — нефтедобывающие и нефтеперерабатывающие комплексы, электростанции и транспорт, где последствия нарушения в системе электроснабжения настолько велики, что к оборудованию, предназначенному для защиты многочисленных узлов, предъявляются гораздо более строгие требования, нежели к коммерческим ИБП.

11. Идентификация событий, которые являются возможной причиной нарушения непрерывности процессов обеспечения ИБ и бизнес-процессов

Для обеспечения своевременной реакции, которая должна предотвратить перерыв в работе активов, обходимо регулярно выполнять идентификацию событий, которые могут стать возможной причиной нарушения непрерывности процессов обеспечения ИБ и бизнес-процессов.

На СОИБ возлагается ответственность в процессе внутреннего аудита (но не менее одного раза в год) пересматривать перечень событий, которые могут стать возможной причиной нарушения непрерывности процессов обеспечения ИБ и бизнес-процессов (по форме Приложения 2).

12. Периодическое техническое обслуживание оборудования

Для обеспечения непрерывности функционирования, доступности и целостности ИС оборудование нуждается в периодическом техническом

обслуживании: каждый квартал года. Обязательства по проведению технического обслуживания возлагаются на ответственных сотрудников закрепленных за соответствующем оборудованием.

13. Ответственность

СОИБ несет ответственность за:

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

Сотрудники проекта ИС:

a) исполнение настоящей Инструкции.

Приложении 1

ПЛАН МЕРОПРИЯТИЙ
по обеспечению непрерывной работы и восстановления работоспособности активов, связанных со средствами обработки информации Информационной системы «Геоинформационный портал города Нур-Султан» ГПГ.СМИБ.ПР.04-01.r02.20

№	Актив (в соответствии с Перечнем активов и ответственных за них сотрудников)	Инцидент	Предупреждающие действия инцидента	Восстановительные мероприятия инцидента	Допустимое время восстановления сервиса	Приемлемый уровень потери информации	Ответственные
1	2	3	4	5	6	7	8

Приложение 2

ПЕРЕЧЕНЬ
возможных причин нарушения непрерывности процессов обеспечения ИБ и бизнес-процессов, работы активов и возникновения внештатных ситуаций
Информационной системы «Геоинформационный портал города Нур-Султан»
ГПГ.СМИБ.ПР.04-02.r02.20

№ п/п	Подверженные активы (в соответствии с Перечнем активов и ответственных за них сотрудников)	Причина
1	2	3