?????????? ??
??????????
???????????
????????????
?????????

- ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ НЕПРЕРЫВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ «SDU UNIVERSITY»

?????????? ?? ??????????? ?????????????? ?????????????? ???????????? ??????????

«SDU UNIVERSITY»

СОДЕРЖАНИЕ

1. Общие положения

2. Анализ риска

3. Анализ влияния на бизнес (BIA)

4. Стратегии непрерывности

Приложение 1

Приложение 2

1. ????? ?????????

1.Целью данного плана является обеспечение безопасности информационных систем и данных Учреждения «SDU University» (далее -Университет), а также обеспечение его готовности к возможным угрозам.

2.Эти инструкции охватывают все информационные системы, данные, приложения и пользователей.

2. ?????? ?????

2.1.Угрозы: кибератаки, стихийные бедствия, человеческий фактор, отказ оборудования, перебои в подаче электроэнергии.

2.2.Оценка риска**:** Реализовав определенные меры (Надежная аутентификация, Защита сети и системы, Защита от DDoS-атак, Защита от программ-вымогателей, Обучение и повышение осведомленности, Контроль доступа и разграничение прав), университет может существенно повысить уровень защищенности своих информационных систем. Особое внимание следует уделять повышению осведомленности о киберугрозах, а технические меры безопасности следует сочетать с ответственным поведением пользователей.

Для защиты университетских информационных систем от природных катастроф необходимо сочетать технические меры, стратегическое планирование и эффективное управление кризисными ситуациями. Оптимальная защита включает резервное копирование данных, обеспечение физической безопасности инфраструктуры и разработку четких планов действий в экстренных случаях.

Такие меры помогут университетам сохранить непрерывность образовательных и административных процессов даже в условиях природных катастроф.

Хотя человеческий фактор представляет значительную угрозу для информационных систем университетов, этот риск можно значительно снизить за счет обучения, автоматизированных систем безопасности и строгого контроля доступа. Университет должен сочетать образовательные и технические меры, чтобы обеспечить надежную защиту своих информационных систем.

Предотвращение отказов оборудования в университетских информационных системах возможно благодаря регулярному обслуживанию, резервному копированию, управлению энергоснабжением и обеспечению сетевой безопасности. Университету следует применять проактивные решения для

продления срока службы оборудования и обеспечения бесперебойной работы учебных и исследовательских процессов.

3. ?????? ??????? ?? ?????? (BIA)

3.1. Критические бизнес-процессы: В университете два раза в год проводится процесс регистрации на курсы, во время которого студенты выбирают дисциплины и формируют свое расписание на следующий семестр. Этот процесс длится примерно 10 дней, и в этот период все студенты одновременно заходят в систему, что создает большую нагрузку на серверы. Чтобы избежать сбоев, в такие периоды необходимо увеличивать серверные мощности.

3.2. Кроме того, раз в год проводится процесс зачисления новых студентов. В этот период поступающие в университет загружают в систему свои личные данные и документы. В это время особенно важно, чтобы в университете была достаточная скорость интернета и обеспечена защита данных, поскольку большое количество пользователей одновременно используют систему для передачи информации.

3.3. Максимально допустимое время простоя (RTO):Максимальное целевое время восстановления (RTO) для информационной системы университета составляет в среднем 2 часа в периоды пиковой нагрузки. Среднее время определяется в зависимости от важности работающих в информационной системе модулей и количества пользователей.

3.4. Максимально допустимая потеря данных (RPO): Максимально допустимая потеря данных зависит от времени резервного копирования виртуальных серверов. Она обозначает максимальный временной промежуток между последней доступной точкой восстановления данных и моментом сбоя. Эта информация указана в инструкции по резервному копированию.

4. ????????? ?????????????

4.1. Резервное копирование: Эта информация указана в инструкции по резервному копированию. Для процесса резервного копирования используется служебное программное обеспечение. В этом программном обеспечении серверы должны иметь планы резервного копирования.

4.2. Процедуры восстановление: Эта информация указана в инструкции по резервному копированию.

Распределение задач

Задача	Ответственный отдел/лицо	Описание
Подготовка плана обеспечения непрерывности бизнеса	Отдел информационно-технической поддержки, Отдел автоматизации	Разработка стратегии обеспечения непрерывности бизнеса и плана восстановления после аварийных ситуаций.
Проведение анализа влияния на бизнес (BIA)	Департамент "Мониторинга качества", Отдел информационно-технической поддержки, Департамент финансов и бюджетного планирования	Определение критически важных процессов, расчет параметров RTO и RPO.
Определение стратегии резервного копирования	Отдел информационно-технической поддержки	Разработка процедур резервного копирования, определение частоты копирования и мест хранения.

Разработка плана восстановления после аварии (DRP)	Отдел информационно-технической поддержки	Создание сценариев кризисных ситуаций, планирование технических процессов восстановления.
Коммуникация и координация	Департамент HR	Разработка стратегии коммуникации с внутренними и внешними заинтересованными сторонами в экстренных ситуациях.
Определение альтернативных рабочих площадок	Департамент HR	Создание процедур удаленной работы или работы в альтернативных локациях в случае перебоев в работе.
Проведение тестов и учений	Отдел информационно-технической поддержки	Регулярное тестирование планов обеспечения непрерывности бизнеса и проведение корректировок.
Обучение и повышение осведомленности	Департамент HR, Центр цифровизации	Проведение обучающих мероприятий и повышение осведомленности сотрудников о планах обеспечения непрерывности.
Обновление планов непрерывности бизнеса	Центр цифровизации	Регулярный пересмотр и обновление планов обеспечения непрерывности бизнеса.

Контактная информация для экстренных случаев

ФИО	Ответственный отдел/лицо	Контактная информация
Акимов Нуркен Жанбырбаевич	Проректор по административным работам	
Мехдиев Ясин Айдыноглу	Заведующий Отдела информационно-технической поддержки	
Шотанбаев Шокан Жумагулович	Директор Департамента по хозяйственной части	
Гунжер Ибрахим	Директор Центра цифровизации	
Глеубердіұлы Нурлан	Специалист Департамента по хозяйственной части	
Бейсембиев Шынгыс Даулетулы	Старший специалист Отдела информационно-технической поддержки	
Нагиев Эльвин	Проектный архитектор Отдела Автоматизации	