«УТВЕРЖДЕНО»
Решением Правления
НАО «Университет Нархоз»
Протокол № 8 от
«15». 06 2023 г.

Регламент резервного копирования и восстановления информации информационных ресурсов Некоммерческого акционерного общества «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Регламент резервного копирования и восстановления информации информационных ресурсов Некоммерческого акционерного общества «Университет Нархоз»
Краткое описание:	Регламент резервного копирования и восстановления информации информационных ресурсов Некоммерческого акционерного общества «Университет Нархоз»
Тема:	Информационная безопасность
Статус:	Новый
Дата утверждения:	«___» _____2023г.
Дата завершения действия:	
Дата аудита:	Еженедельно
Ответственный за аудит:	Эксперт по информационной безопасности

Лист согласования

Должность	Ф.И.О.	Подпись
Директор Административного департамента	Бисенғали Л	
Советник по цифровизации	Тебаев Д.Б.	
и.о. Директора Департамента информационных технологий	Жумажанов Б.Ж.	

1 Общие положения

1.1 Настоящий Регламент резервного копирования и восстановления информации (далее – «Регламент») информационных ресурсов НАО «Университет Нархоз» (далее – «Ресурсы») Некоммерческого акционерного общества «Университет Нархоз» (далее – «Общество») определяет требования к организации мероприятий по резервному копированию и восстановлению программного обеспечения и информационных ресурсов корпоративной вычислительной сети Общества.

1.2 В настоящем Регламенте используются следующие основные понятия и термины:

• **дистрибутив** – установочный пакет программного обеспечения для начальной инициализации системы;

• **информационная безопасность в сфере информатизации (далее – ИБ)** – состояние защищенности электронных информационных ресурсов, информационных систем и информационно - коммуникационной инфраструктуры от внешних и внутренних угроз;

• **информационные ресурсы (ИР)** – организационно-техническая структура, представляющая собой совокупность следующих взаимосвязанных компонентов:

– технических средств обработки и передачи данных;

– методов и алгоритмов обработки в виде соответствующего программного обеспечения;

– баз данных на различных носителях;

– персонала и пользователей, объединенных по организационно- структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных.

• **ДИТ** – структурное подразделение Общества, ответственное за администрирование, сопровождение и обеспечение бесперебойного функционирования ИР;

• **Эксперт по информационной безопасности** (далее – «Эксперт ИБ») – работник Общества, ответственный за управление мероприятиями в области информационной безопасности;

• **эталонное программное обеспечение** – неизменное программное обеспечение.

Выполнение требований настоящего Регламента контролируется Экспертом ИБ.

2 Копирование программного обеспечения и информационных ресурсов

2.1 В целях обеспечения возможности оперативного восстановления информации и процессов ее обработки в случае нарушения работоспособности ресурсов, используются копирование эталонного программного обеспечения (далее – «ПО») и резервное копирование информационных ресурсов.

2.2 Все ПО, используемые в Обществе, должны иметь эталонные и дистрибутивные копии.

2.3 ДИТ составляются следующие реестры:

• реестр эталонных/дистрибутивных копий ПО, эксплуатируемого в Обществе, по форме согласно приложению 1 к настоящему Регламенту;

• реестр ПО и информационных ресурсов корпоративной вычислительной сети Общества, подлежащих резервному копированию, по форме согласно приложению 2 к настоящему Регламенту.

2.4 Реестр эталонных и дистрибутивных копий ПО, эксплуатируемого в Обществе, должен содержать перечень ПО, в том числе операционные системы (далее – «ОС»), системы управления базами данных, с указанием:

• порядкового номера;

• наименования эталонного/дистрибутивного ПО;

• номера лицензии и/или электронного ключа активации (при наличии);

• срока действия лицензии;

• Ф.И.О. системного администратора;

• места хранения эталонного/дистрибутивного копии ПО;

• Ф.И.О. лица, ответственного за хранение эталонной/дистрибутивной копии ПО;

• порядка использования эталонной/дистрибутивной копии ПО;

• другой информации (при необходимости).

2.5 Реестр ПО и информационных ресурсов корпоративной вычислительной сети Общества, подлежащих резервному копированию, должен содержать перечень всего ПО и информационных ресурсов, с указанием:

• места размещения ПО и информационного ресурса;

• графика копирования (для баз данных: отдельно по полному резервному копированию базы данных и резервному копированию архивных лог-файлов);

• тип копирования (полный или выборочный);

• Ф.И.О. лица, ответственного за копирование;

• места хранения резервной копии;

• необходимости дублирования копии;

• места хранения дубликата (если есть) резервной копии;

• Ф.И.О. лица, ответственного за хранение копий.

2.6 В целях обеспечения безопасности носители информации с эталонными/дистрибутивными копиями ПО по возможности должны храниться в железном сейфе в ответственного за администрирование ресурсов Общества.

2.7 Контроль ведения реестра эталонных копий ПО и реестра ПО и информационных ресурсов, подлежащих резервному копированию, осуществляется Экспертом ИБ.

2.8 Лицами, ответственными за резервное копирование, согласовывается с Экспертом ИБ план-график по проведению резервного копирования.

2.9 При проведении резервного копирования ведется электронный журнал записи резервного копирования ПО и информационных ресурсов корпоративной вычислительной сети Общества, в котором фиксируется наименование ПО и/или информационного ресурса, дата и время начала и завершения резервного копирования, уровень резервирования, размер копии, согласно приложению 3 к настоящему Регламенту.

2.10 Контроль проведения резервного копирования осуществляется Директором ДИТ и Экспертом ИБ.

2.11 Запуск процедур резервного копирования необходимо производить в ночное время, либо в нерабочие дни.

2.12 Хранению подлежат текущая и не менее двух предыдущих копий.

2.13 Для создания полных резервных копий необходимо использовать магнитные диски (дисковый массив) или магнитные ленты.

2.14 Системный администратор должен самостоятельно определить объем резервного копирования (полный или выборочный) и частотность его выполнения должны отражать требования ресурсов Общества, в том числе безопасность и критичность информации для длительной работы ресурсов Общества.

2.15 Доступ к носителям информации с эталонными и резервными копиями ПО и информационных ресурсов имеют Директор ДИТ, Эксперт ИБ, специалисты ДИТ в соответствии с функциональными обязанностями.

2.16 При всех действиях резервного копирования должна обеспечиваться информационная безопасность и все ответственные работники несут полную ответственность за сохранность носителей с резервными копиями.

3 Тестирование и восстановление

3.1 Процедуры проверки резервных копий необходимо выполнять для обеспечения уверенности в их целостности, а также в том, что для выполнения этих процедур потребуется не больше времени, чем определено операционными процедурами восстановления. Резервные копии должны разворачиваться с возможностью проверки их использования для восстановления с периодичностью не реже 1 раза в квартал. В журнале проверок целостности резервных копии и журнале проверок резервных копий на восстановление информационных ресурсов корпоративной вычислительной сети Общества фиксируются время и дата, IP адрес сервера, результат, время, затраченное на восстановление, Ф.И.О. ответственного исполнителя, за какую дата выполнено восстановление согласно приложению 4 к настоящему Регламенту.

3.2 В случае сбоя в работе основного серверного оборудования, необходимо переключить на резервный сервер в ручном режиме. В случае, если основное и резервное серверные оборудования, ОС или базы данных недоступны, необходимо выполнить процедуру восстановления в соответствии с руководством администратора информационных ресурсов Общества.

4 Сроки хранения резервных копий

1) БД – ежедневно, полная копия. Хранить все копии за последние 31 день, последние 12 месячных копий, 3 последние годовые копии.

2) ПО – не реже одного раза в месяц, перед каждым обновлением, и после каждого обновления, полная копия. Хранить не менее 4 последних копий.

3) ОС – ежемесячно, перед каждым обновлением или установки исправлений, и после каждого обновления или установки исправлений, полная копия. Хранить не менее 3 последних копий.

4) Эталонная копия исходных кодов хранится в соответствии с их функциональной и практической значимостью.

График проведения резервного копирования должен корректироваться не реже чем раз в год, и в случае необходимости пересматриваться.

5 Управление съёмными носителями

5.1 Для управления съёмными носителями необходимо предусмотреть следующее:

- заводится журнал учета электронных носителей резервных копий ПО и информационных ресурсов корпоративной вычислительной сети Общества, согласно приложению 5 к настоящему Регламенту;
- если носители информации многократного использования больше не требуются и удаляются за пределы организации, их содержимое должно стать невосстанавливаемым;
- где это необходимо и целесообразно, в отношении всех уничтожаемых носителей информации должно быть принято соответствующее решение, а также сделана запись в журнале учета;
- электронных носителей резервных копий ПО и информационных ресурсов корпоративной вычислительной сети;
- все носители информации должны храниться в надежном, безопасном месте, в соответствии с требованиями изготовителей;
- информация, хранящаяся на носителях, в которой нуждаются дольше, чем срок службы носителя (в соответствии со спецификациями изготовителя) должна также храниться в другом месте во избежание потери информации вследствие изношенности носителя;
- для ограничения вероятности потери данных предусматриваться регистрацию

съёмных носителей в Журнале вноса/выноса электронных носителей резервной информации Общества, согласно приложению 6 к настоящему Регламенту.

5.2 Съёмные носители информации включают картриджи с магнитными лентами, магнитные диски, флэш-диски, переносные (внешние) жёсткие диски, CD, DVD и печатные носители.

6 Требования по размещению резервного серверного оборудования и физической защиты

6.1 Резервное оборудование и средства обработки информации должны быть расположены и защищены так, чтобы уменьшить риск от воздействий окружающей среды и возможности неавторизованного доступа. Для обеспечения доступности и отказоустойчивости ресурсов Общества должно обеспечиваться:

- наличие резервного серверного оборудования;
- наличие резервного серверного оборудования, расположенного в резервном серверном помещении Общества.

6.2 Серверный центр должен соответствовать международным стандартам построения серверных центров TIA-942, все жизнеобеспечивающие инженерные системы резервированы.

6.3 Меры по управлению ИБ включают в себя следующие мероприятия:

- ограничение доступа в места расположения резервного оборудования и средств обработки и хранения информации;
- уменьшение риска несанкционированного наблюдения за функционированием средств обработки и хранения важной информации;
- изоляция отдельных элементов оборудования, требующих специальной защиты;
- принятие мер по минимизации риска потенциальных угроз, в том числе воровства, пожара, взрыва, задымления, затопления, пыли, вибрации, химического воздействия, помех в электроснабжении, помех связи, электромагнитного облучения, вандализма;
- мониторинг состояния окружающей среды в целях выявления условий (температура, влажность), которые могли бы неблагоприятно повлиять на функционирование средств обработки информации;
- оснащение здания, в котором расположены средства обработки информации, громоотводами;
- защита оборудования для обработки важной информации от вследствие электромагнитного излучения.

6.4 Резервные копии ресурсов Общества должны размещаться на электронных носителях информации на Резервном серверах Общества

6.5 Эталонные копии ресурсов Общества должны храниться на электронных носителях информации в сейфе ответственного за ИБ. Системный администратор ведет реестр эталонных копий.

7 Ответственность

7.1 Эксперт по ИБ несет ответственность за:

- определение ответственных лиц;
- составление перечней согласно настоящего Регламента;
- контроль выполнение периодических резервных копий;
- исполнение настоящего Регламента.

7.2 Системный администратор несет ответственность за:

- ведение реестра эталонных копий;
- резервное копирование данных ресурсов Общества.

В случае нарушения требований настоящего Регламента администраторы привлекаются к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

8 Заключительные положения

8.1. Настоящий Регламент утверждаются решением Правления.

8.2. Изменения и дополнения в Регламент вносятся решением Правления.

Приложение 1 к Регламенту
резервного копирования и
восстановления информации

Реестр эталонных копий и дистрибутивных копий ПО, эксплуатируемого в Обществе

№	Наименование эталонного (дистрибутивного) ПО	Номер лицензии и/или электронного ключа активации (при наличии)	Срок действия лицензии	Ответственный администратор системы/АИС (Ф.И.О., телефон)	Место хранения эталонной или дистрибутивной копии (адрес здания, № кабинета)	Ответственный за хранение эталонной или дистрибутивной копии (Ф.И.О., телефон)	Порядок использования эталонной копии (кто, в каких случаях)	Прочее

Приложение 2 к Регламенту
резервного копирования и
восстановления информации

Реестр программного обеспечения и информационных ресурсов корпоративной вычислительной сети Общества, подлежащих резервному копированию

№	Наименование ПО и информационного ресурса	Место размещения ПО и информационного ресурса	График копирования	Тип копирования	Ф.И.О., телефон ответственного за копирование	Место хранения резервной копии (адрес здания, № кабинета)	Необходимость дублирования копии	Место хранения дубликата резервной копии (адрес здания, № кабинета)	Ф.И.О., телефон ответственного за хранение копий

Приложение 3 к Регламенту резервного копирования и восстановления информации

Электронный журнал записи резервного копирования программного обеспечения и информационных ресурсов корпоративной вычислительной сети Общества

Наименование ПО и информационного ресурса	Дата и время начала копирования	Дата и время завершения копирования	Место размещения ПО и информационного ресурса	Тип резервирования	Место хранения резервной копии (адрес здания, № кабинета)	Размер Гб	Ф.И.О., телефон ответственного за копирование	Примечание

Приложение 4 к Регламенту резервного копирования и восстановления информации

Журнал проверок резервных копий на восстановление программного обеспечения и информационных ресурсов корпоративной вычислительной сети Общества

№	Дата и время операции	IP адрес сервера	Результат	Время, затраченное на тестовое восстановление	ФИО ответственного работника	За какую дату выполнено восстановление

Приложение 5 к Регламенту резервного копирования и восстановления информации

Журнал учета электронных носителей резервных копий программного обеспечения и информационных ресурсов корпоративной вычислительной сети Общества

№	Идентификация носителя (инвентарный номер, серийный номер)	Тип носителя	Срок службы, установленный производителем	Дата и время Операции	Место хранения резервной копии (адрес здания, № кабинета)	Наименование ПО и информационного ресурса	ФИО ответственного работника

Приложение 6 к Регламенту резервного копирования и восстановления информации

Журнал вноса/выноса электронных носителей резервной информации Общества

№	Тип носителя, объем памяти	Уникальный идентификатор	Дата выдачи	ФИО/ подпись, выдавшего	ФИО/ подпись, получившего	Дата возврата	ФИО/ подпись получившего

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Подпись	Дата
1	2	3	4	5