РЕГЛАМЕНТ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

Астана

2023 г.

1. Термины и сокращения

Организация – ОЮЛ Ассоциация ВИЭ «Qazaq Green»;

Регламент – Регламент проведения резервного копирования и восстановления информации;

Специалист по информационной безопасности - сотрудник Организации, ответственный за обеспечение защиты информационных ресурсов и обеспечение информационной безопасности Организации;

Корпоративная вычислительная сеть – сеть взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов, предназначенных для решения задач обмена данными и эксплуатируемыми в Организации;

Локальная вычислительная сеть (ЛВС) – группа персональных компьютеров или периферийных устройств, объединенных между собой высокоскоростным каналом передачи данных в расположении одного или многих близлежащих зданий;

Несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

Резервное копирование – это мероприятие по обеспечению бесперебойной работы ПО и информационных систем, заключающееся в создании копий на инсталляционные аварийно-восстановительные носители данных, информации обрабатываемых и находящихся в информационных ресурсах с возможностью восстановления и дальнейшего использования;

Сеть Интернет – система сетей, обеспечивающая доступ к международным информационным ресурсам;

Эталонное копирование – это копия программного обеспечения на инсталляционные аварийно-восстановительные носители находящихся в информационных ресурсах с возможностью дальнейшей инсталляции и использовании при проведении восстановительных работ;

ПК – персональный компьютер;

ПО – программное обеспечение;

ИС – информационная система «Торговая платформа для товарных и сырьевых бирж Казахстана» 2.0.

2. Общие положения

Настоящий Регламент определяет требования к организации мероприятий по резервному копированию программных и информационных ресурсов корпоративной вычислительной сети Организации, а также

устанавливает ответственность пользователей ПК, сотрудников информационных технологий, Специалиста по информационной безопасности и других сотрудников, в компетенцию которых входит проведение этих мероприятий.

3. Копирование программных и информационных ресурсов

1. В целях обеспечения возможности оперативного восстановления информации и процессов ее обработки в случае нарушения работоспособности информационных систем, используются копирование эталонного ПО и резервное копирование информационных ресурсов.
2. Все программное обеспечение, используемые в ИС, должно иметь эталонные (дистрибутивные) копии.
3. Сотрудниками информационных технологий составляются следующие реестры:

1) реестр эталонных копий ПО, эксплуатируемого в Организации, согласно **Приложению 1** к настоящему Регламенту;

2) реестр подлежащих резервному копированию информационных ресурсов корпоративной вычислительной сети Организации, согласно **Приложению 2** к настоящему Регламенту.

3) реестры согласовываются с Специалистом по информационной безопасности.

4) Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

4. Контроль ведения реестра эталонных копий ПО и реестра информационных ресурсов, подлежащих резервному копированию, осуществляется Специалистом по информационной безопасности.
5. Контроль проведения резервного копирования, в том числе валидности резервных копий, осуществляется Системным Администратором
6. Запуск процедур резервного копирования необходимо производить в вечернее (после 21:00) либо ночное время, в некоторых случаях в нерабочие дни.
7. Резервное копирование виртуальных машин – серверов осуществляется ежедневно в автоматизированном режиме (по расписанию) в рабочие дни.
8. Хранению подлежат текущая и не менее двух предыдущих копий.
9. Для создания полных резервных копий, стандартно используется специальный сервер Backup, при нехватке места на этом сервере необходимо использовать внешний мобильный накопитель на жёстком диске.

10. В целях обеспечения безопасности, носители информации с копиями должны храниться в опечатанном железном, огнестойком сейфе у системного администратора.

11. Доступ к носителям информации с эталонными копиями ПО и резервными копиями информационных ресурсов имеют только сотрудники, в компетенцию которых входит данный вид работ.

12. Вынос носителей информации с эталонными копиями ПО и резервными копиями за пределы здания, арендуемого Организацией, необходимо согласовать с Специалистом по информационной безопасности и **фиксировать в контрольном журнале**. При этом столбцы журнала «Время начала» «Время окончания», «Простой», «Метод устранения» остаются незаполненными.

4. Порядок резервного копирования

13. Резервное копирование автоматизированных систем производится на основании следующих данных:

- состав и объем копируемых данных, периодичность проведения резервного копирования;
- максимальный срок хранения резервных копий – **1 месяц;**
- хранение 2-х следующих архивов;

14. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью. Методика проведения резервного копирования описана в **Приложении №3**.

15. При выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, выполняется внутреннее расследование системным администратором для принятия мер по закрытию уязвимых соединений.

5. Проверка резервируемых данных

16. Проверка данных представляет собой процесс подтверждения того, что значения, вводимые в объекты данных, соответствуют ограничениям в схемах наборов данных, а также правилам, установленным для приложения. Проверка данных до отправки обновлений в основную базу данных является практикой, которая уменьшает вероятность появления ошибок, а также ожидаемое количество циклов обработки между приложением и базой данных.

Оборудование, участвующее в резервном копировании

Наименование оборудования	**Функциональное назначение**
Сервера с ПО VMware ESXI	Сервер физический (хост)
Виртуальные машины	Сервера баз данных и приложений (виртуальные машины)

Программное обеспечение, участвующее в резервном копировании

Наименование программного обеспечения	Функциональное назначение
Сервера баз данных: postgressql 12 (dva, standard), 14 (clearing, capsytender) mysql 8.029(lpg) Веб серверы: Tomcat (apache tomcat version 9.0.16 (centos)) httpd (Server version: Apache/2.4.37 (centos)) nginx (nginx version: nginx/1.18.0 (Ubuntu)) Keycloak (version 4.8.3) JDK (version 12.0.1)	Система управления базами данных
Centos 8- "CentOS Linux 8 (Core)" (dva,lpg,bd) Ubuntu - "Ubuntu 20.04.5 LTS" (standard)	Операционная система

Перечень типов резервного копирования (backup) и их описание
Резервное копирование

Название резервного копирования	**Краткое описание выполнения**	**Периодичность выполнения**	**Откуда сохраняется информация**	**Куда сохраняется информация**	**Срок хранения резервной копии**
Копирование БД	Копирование через Crontab	Резервная копия раз в 24 часа	Сервер БД	Сервер резервного копирования	полные копий - 6 мес.
Копирование только конфигурационных файлов с виртуальных машин	Копирование по расписанию Crontab	Резервная копия раз день	Все виртуальные машины	Сервер Backup	7 дней Нет места для хранения большего кол-ва архивов
Копирование БД	Копирование по расписанию Crontab	Резервная копия раз день	Все виртуальные машины – хосты БД	Сервер Backup	7 дней Нет места для хранения

					большего кол-ва архивов

17. Проверка резервированных данных информации автоматизированных систем, в т.ч. баз данных, выполняется следующим образом:

Снимаются резервные копии с основного сервера на тестовый сервер, полностью поднимается систем (БД и приложение) далее тестируется.

Копия БД переносится из основного сервера на сервер Backup по защищенному VPN-каналу с шифрованием трафика, после чего также по защищенному VPN-каналу переносится на тестовый сервер.

«Журнал состояния архивов» (инцидентов).

Проверка резервированных данных проводится раз в полгода в конце июня и декабря во время не праздничных выходных дней. Результаты проверок записываются в «Журнал проверок, резервированных данных» согласно **Приложению 4.**

18. При выявлении поврежденных резервированных данных системный администратор делает запись в журнал состояния архивов (инцидентов). После чего выполняется обязательная проверка на хэш сумму трех последующих архивов, при отсутствии повреждений при этих проверках, восстанавливается стандартный порядок проверки архивов.

6. Порядок размещения серверного оборудования.

19. Репликация базы данных между основным и резервным серверами выполняется ежедневно в нерабочее время в автоматическом режиме, ПО – по мере внесения изменений.

20. Уровень физической защиты и защиты от воздействий окружающей среды в резервном пункте должен соответствовать уровню безопасности в основном здании, где расположена ИС.

21. Для поддержания средств резервирования в рабочем состоянии системный администратор регулярно, раз в квартал проводит проверку программных и технических средств резервирования, резервного оборудования.

22. По результатам проверок составляется акт выполненных работ и выполняется запись в журнал тестирования резервного оборудования и средств резервирования который описан в Приложении 4 к настоящему документу.

23. Тестирование средств резервирования и резервного оборудования

осуществляется системным администратором.

24. В случае отрицательных результатов проверки необходимо поставить в известность руководителя организации о необходимости замены средств резервирования или проведение ремонтных работ.

25. Для сведения к минимуму ошибочных действий со стороны ответственных за резервирование специалистов разработана инструкция по выполнению резервирования и восстановления информации ИС.

26. Ответственным за разработку, актуализацию, выполнение требований инструкции по резервированию/восстановлению данных системы является системный администратор.

27. В организационном плане специалисты технической поддержки должны руководствоваться настоящим Регламентом.

7. Хранение и учет электронных носителей резервной информации

28. В целях обеспечения безопасности, носители информации с копиями хранятся в железном сейфе руководителя, вне помещения, в котором расположена информационная система.

29. Резервная информация должна быть обеспечена гарантированным уровнем физической защиты и защиты от воздействий окружающей среды в соответствии с уровнем безопасности в основном здании.

30. Хранению подлежат текущий и дубликат копий.

31. Доступ к носителям информации с дистрибутивом информационной системы и резервными копиями информационных ресурсов имеют только ответственные сотрудники, специалист по информационной безопасности и системный администратор.

32. Удаление хранимой на носителе информации, должно проводиться способом, гарантирующим ее безвозвратное уничтожение.

33. В случае выхода из строя носителя, он должен быть утилизирован способом, гарантирующим безвозвратное уничтожение хранимой на нем информации в присутствии ответственного лица и руководителя ОИТ.

34. Уничтожение носителя резервных копий должно быть зафиксировано в акте списания.

35. Перемещение резервных копий должно быть предварительно согласовано с руководителем ОИТ, факт перемещения фиксируется в контрольном журнале учета электронных носителей с резервными копиями информационных ресурсов.

36. Факт перемещения носителей с резервными копиями вне помещения организации должен быть предварительно согласован с подразделением ОИТ и зарегистрирован в журнале вноса/выноса резервных копий.

37. Запрещается:

– вносить изменения вручную в созданные архивы резервных копий информации систем;

– передавать резервные копии информации посторонним лицам;

– хранить резервные копии в незащищенном месте.

8. Контроль результатов резервного копирования

38. Процедура резервного копирования программного обеспечения (не баз данных или виртуальных машин) осуществляется пользователями этих программ в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

39. В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает системному администратору до 18 часов текущего рабочего дня.

40. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием файловых серверов имеющих свободные дисковые массивы для обеспечения функций резервного копирования.

41. Тестирование изменений проводится по мере необходимости и обусловлено внесением изменений в настройки сервисов или установкой обновлений. Изменения в настройках конфигурации могут быть вызваны появлением рекомендаций разработчиков сервисов (улучшения безопасности). Установка обновлений происходит на регулярной основе по мере появления доступных обновлений (например: для ОС Windows Server 2022 не менее 1 раза в месяц).

9. Ротация носителей резервных копий

42. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

43. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются системным администратором.

44. Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна быть уничтожена с физическим повреждением носителя, не допускающим его теоретическое

использование в роли накопителя данных. (пример – высверливание корпуса HDD, физическое разрушение SSD) с приложением фотографий повреждений к акту списания.

45. Для защиты от вредоносного кода в Организации используется антивирусное программное обеспечение ESET Endpoint Security 6.3.2016.1, межсетевые экраны Windows в режиме повышенной безопасности.

10. Контроль за соблюдением Регламента

46. Контроль соблюдения настоящего Регламента осуществляет, специалист по информационной безопасности в соответствии с аудитом информационной безопасности, план проведения которого утверждается Руководителем Организации.

47. За нарушение норм, предусмотренных настоящим Регламентом, к работникам Организации по представлению специалиста по информационной безопасности, могут быть применены меры дисциплинарного взыскания.

11. Рассылка

Обязательное ознакомление всех сотрудников Организации под роспись (далее – Лист ознакомления).

Приложение 1
к Регламенту проведения резервного
копирования и восстановления информации

Реестр эталонных копий программного обеспечения, эксплуатируемого в ОЮЛ Ассоциация ВИЭ «Qazaq Green»

Наименование программного обеспечения	**Ответственный за эксплуатацию программного обеспечения (Ф.И.О., телефон)**	**Место хранения эталонной копии (адрес здания, № кабинета)**	**Ответственный за хранение эталонной копии (Ф.И.О., телефон)**	**Порядок использования эталонной копии (кто, в каких случаях)**
ИС Реестр углеродных единиц Qazaq Green Certificate Registry				

Приложение 2
к Регламенту проведения резервного
копирования и восстановления информации

Реестр информационных ресурсов корпоративной вычислительной сети ОЮЛ Ассоциация ВИЭ «Qazaq Green», подлежащих резервному копированию

Наименование информационного ресурса	Место размещения информационного ресурса	График копирования	Ф.И.О., телефон ответственного за копирование	Необходимость дублирования копии	Место хранения резервной копии (адрес здания, № кабинета)	Место хранения дубликата резервной копии (адрес здания, № кабинета)	Ф.И.О., телефон ответственного за хранение копий
ИС Реестр углеродных единиц Qazaq Green Certificate Registry	Абая 26 ЦОД АО “Казактелеком”	Ежедневно		Да	г. Астана, ул. Абая 26 ЦОД АО «Казактелеком»	г. Астана, пр. Кабанбай батыра 62 ТОО “NLS”	

Приложение 3
к Регламенту проведения резервного
копирования и восстановления информации

Методика резервного копирования

1. Для организации системы резервного копирования используется встроенное программное обеспечение (далее - ПО) архивации и созданные файлы формата .sh с применением возможностей функции «Планировщика задач». Учитывая пропускные способности каналов, объемы резервируемых данных, представляется оптимальным установить независимые серверы резервного копирования. С целью оптимизации расходов на развертывание системы резервного копирования, запись резервной копии осуществляется на жесткий диск.

2. С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования данных, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.

3. Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в ночное время. Существуют три набора резервных копий:

- месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – месяц. Хранится на сервере резервного копирования.
- недельная копия. Записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы. Хранится на сервере.
- ежедневная копия. Записывается ежесуточно, кроме выходных дней. Срок хранения – неделя. Записывается на сервер Backup, при отсутствии места на съемный жесткий диск. Жесткий диск по отдельному расписанию выносится за пределы офиса, либо в противоположную часть офиса.

4. В Организации различаются два принципиально разных источника информации, подлежащей резервированию:

1) Информация, хранимая непосредственно в файловой системе – MS Windows – FAT32, NTFS, REFS.

2) Базы данных Прикладной информационной системы – LINUX EXT2, EXT3, EXT4, XFS.

5. Для резервирования информации, хранимой непосредственно в файловых системах, используется встроенное ПО, посредством которого формируются задания на проведение резервного копирования информации, находящейся в каталогах файловых систем MS Windows. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

6. Для резервирования информации, хранимой в базах данных Прикладной информационной системы, в качестве промежуточного звена автоматизации используются средства конфигурирования Прикладной информационной системы и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных Прикладной информационной системы. Посредством встроенного ПО формируются задания на проведение резервного копирования этого каталога. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.

Резервные копии должны храниться в удаленном месте, на надежном расстоянии, достаточном, чтобы избежать любого повреждения вследствие аварийной ситуации в основном здании.

Приложение 4
к Регламенту проведения резервного
копирования и восстановления информации

Журнал резервного копирования

Краткие данные по резервному копированию БД		Срок хранения копий БД, дней	
Название проекта:	ИС Торговая платформа для товарных и сырьевых бирж Казахстана 2.0		
Срок хранения копий БД на HDD сервера	1 год		
Срок хранения копий БД на ленте	Не хранится		
Время запуска резервного копирования	01:00		

	Дата			
IP-адрес сервера	время	происшествие	причина	примечание

Журнал восстановления базы данных

Дата выполнения работы	IP-адрес сервера	Тип восстановления	Дата резервной копии БД	Причина	Примечание	Исполнитель

Журнал резервного копирования для центрального узла

Краткие данные по резервному копированию БД		Срок хранения копий БД, дней
Название проекта:	ИС Торговая платформа для	

	товарных и сырьевых бирж Казахстана 2.0	
IP-адрес боевого сервера БД:	172.16.11.30	
IP-адрес резервного сервера БД:	45.86.81.78	
IP-адрес архивного сервера копий БД:	89.218.68.69	
IP-адрес FTP-сервера:		
Срок хранения копий БД на ленте	Не хранится	
Время запуска резервного копирования	01:00	

Дата проведения резервного копирования	Наличие копий БД										Примечание
	На файловой системе сервера БД		Резервный сервер БД		Ленточный носитель		Архивный сервер		FTP-сервер		
21.06.2023			Да		Нет		Да				

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Личная подпись	Дата
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				