Приложение 16
к Положению об
информационной безопасности

Руководство администратора по сопровождению

1. Назначение документа

1. Руководство администратора по сопровождению всех Автоматизированных информационных систем (далее - АИС) принадлежащих НАО «Евразийский Национальный Университет имени Л.Н. Гумилева» (далее - Университет) предназначено для описания порядка действий администратора в различных ситуациях в рамках сопровождения системы.

2. Определения и сокращения

1) АИС – Автоматизированная информационная система;
2) Администратор системы - сотрудник, осуществляющий управление сервером АИС;
3) БД - База данных;
4) ИБ - Информационная безопасность;
5) ОС - Операционная система;
6) ПО - Программное обеспечение;
7) ППО - Прикладное программное обеспечение;
8) Пользователь - Лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования;
9) Служба техподдержки - (далее – HelpDesk) – организация или подразделение, отвечающее за электроснабжение, техническое сопровождение и обслуживание каналов связи, функционирование компьютерного оборудования и программного обеспечения, сопровождение ПО;
10) СУБД - Система управления базы данных.

3. Нормативные ссылки

2. Для разработки данного документа использовалась следующая документация:

1) Техническое задание на АИС;
2) Политика информационной безопасности АИС.
3) СТ РК ИСО/МЭК 27001-2008 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности;
4) СТ РК 1696-2007 Средства и системы контроля и управления доступом. Классификация. Общие технические требования и методы испытаний;
5) СТ РК ИСО/МЭК 27002-2015 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью».

4. Требования к действиям администратора по основным типовым работам:

3. Перечень администраторов АИС, и их роли

Наименование администратора	Роль, функции
Администратор ОС АИС	Осуществляет мониторинг производительности ОС АИС, проверка целостности файловой системы, управление безопасностью ОС АИС, создание резервных копий ОС
Администратор БД АИС	Осуществляет управление пространством БД АИС, приложениями и кодом, резервированием и восстановлением БД АИС, безопасностью СУБД АИС, обновлением версии СУБД АИС.
Администратор ПО АИС	Управляет приложением, а также выполняет работы по остановке и запуску приложений ИС в случае сбоя
Администратор-разработчик АИС	Осуществляет сопровождение прикладного программного обеспечения АИС, администрирование прав пользователей системы, обеспечивает бесперебойное функционирование АИС

4. Функциональные обязанности администраторов

5. Администратор ОС АИС имеет максимальные привилегии:

1) Конфигурирует операционную систему на сервере;
2) Выявляет ошибки пользователей серверного программного обеспечения и восстанавливает работоспособность ОС;
3) В рамках своей компетенции обеспечивает реализацию мероприятия по защите информации, согласно Политике информационной безопасности;
4) Проверка целостности файловой системы;
5) Управление безопасностью АИС;
6) Настройка производительности АИС;
7) Управление дисковым пространством;
8) Резервное копирование АИС;
9) Работы по остановке и запуску приложений в случае сбоя;
10) При необходимости проводится планирование и тестирование изменений ОС и т.д.

6. Администратор БД АИС:

11) обеспечивает своевременное копирование и резервирование данных;
12) обеспечивает взаимодействие с техническим персоналом, задействованным в проекте ИС;
13) организует доступ и устанавливает степень доступа пользователей к СУБД; регистрирует пользователей СУБД, назначает идентификаторы

и пароли; однако созданные пользователи БД для прикладного ПО не могут создавать или назначать привилегии для других пользователей БД;

14) обеспечивает безопасное функционирование БД;

15) обеспечивает соблюдение регламентов технического обслуживания, информационной безопасности, и требований прочих эксплуатационных документов обслуживающим персоналом и пользователями системы;

16) в рамках свой компетенции обеспечивает реализацию мероприятия по защите информации, согласно Политике информационной безопасности;

17) управление пространством БД;

18) управление приложениями и кодом;

19) управление резервированием и восстановлением БД;

20) управление безопасностью СУБД;

21) обновление версии СУБД.

7. *Администратор ПО АИС осуществляет:*

1) ежедневный мониторинг работоспособности портала и всех его составляющих сервисов;

2) ежедневный мониторинг доступности сторонних и внутренних ресурсов портала;

3) анализ логов и своевременное уведомление об ошибках в приложениях или сервисах;

4) создание резервных копий, проверка целостности резервных копий;

5) управление учетными записями пользователей портала;

6) при необходимости проводится планирование и тестирование изменений ПО.

8. Администратор-разработчик АИС:

1) устанавливает на серверы прикладное программное обеспечение;

2) обеспечивает интегрирование программного обеспечения на файл-серверах АИС;

3) поддерживает в рабочем состоянии прикладное программное обеспечение АИС;

4) регистрирует пользователей АИС, назначает идентификаторы и пароли, организует доступ к серверам;

5) устанавливает ограничения и права для пользователей АИС;

6) обращается к техническому персоналу при выявлении неисправностей серверного и сетевого оборудование;

7) выявляет ошибки пользователей, прикладного программного обеспечения и восстанавливает работоспособность системы при сбоях и выходе из строя серверного и сетевого оборудования;

8) выявляет ошибки пользователей, прикладного программного обеспечения и восстанавливает работоспособность системы;

9) Обеспечивает:

a) бесперебойное функционирование прикладного программного обеспечения АИС;

b) права доступа пользователей АИС;

10) Обеспечивает логический доступ к приложениям, только зарегистрированным пользователям;

11) Обеспечивает управление доступом к сервисам:

a) контролирует доступ пользователей к данным и приложениям в соответствии с политикой управления доступом;

b) обеспечивает защиту от несанкционированного доступа к системным программам, которые способны обойти средства контроля;

12) в случае обнаружения возникновения инцидента информационной безопасности или другой нештатной ситуации, в рамках своей компетенции, проводит мероприятия по предотвращению нарушения сохранности, доступности, конфиденциальности обрабатываемой информации;

13) в случае обнаружения возникновения инцидента информационной безопасности или другой нештатной ситуации ставит в известность лиц согласно «Инструкции о порядке действий пользователей во внештатных (кризисных) ситуациях в системе»;

14) принимает меры к учету, регистрации событий для целей повседневного контроля и расследований;

15) обеспечивает, в рамках своей компетенции, проверку и обеспечение сохранности критически важных данных на всех стадиях их обработки;

16) обеспечивает, в рамках своей компетенции, резервное копирование критически важных данных;

17) средствами прикладного программного обеспечения обеспечивает защиту от несанкционированных дополнений и изменений.

5. Требования к действиям администратора при возникновении инцидентов, внештатных ситуаций, стихийных природно-климатических и техногенных воздействий

9. Ситуация 1: Недоступность АИС для пользователей

Описание:	Ситуация, когда пользователи по ряду причин не могут работать с АИС, к таковым причинам могут относиться выход из строя сервера или сетевого оборудования, коммуникаций, сбой программного обеспечения.
Действия по идентификации:	Необходимо выяснить, действительно ли АИС недоступна для пользователей, не заключается ли проблема в отдельном пользователе или его компьютере. Попробовать выяснить причину совместно с причастными специалистами, администраторами, проконсультироваться с разработчиками ПО. В случае, если недоступность АИС для пользователей подтверждена, необходимо переходить к действиям по устранению.
Действия по устранению:	1. Поставить в известность непосредственное руководство о возникшей ситуации с недоступностью АИС.

	2. Поставить в известность дежурных специалистов, отвечающих за техническое сопровождение АИС по тел: 3. Самостоятельно или при участии ответственных администраторов выявить и устранить причину недоступности АИС. 4. Сделать отметку в журнале регистрации внештатных ситуаций.

10. Ситуация 2: Перебои или отсутствие энергопитания

Описание:	Отключение энергопитания, перебои или скачки в сети электропитания могут быть вызваны действиями персонала, аварийными ситуациями в здании и поставщика электроэнергии. При возникновении данной ситуации оборудование должен автоматически переводиться на систему резервного энергопитания.
Идентификация:	Система резервного питания должна оповещать администратора в случае возникновения проблем с электропитанием.
Действия:	Времени до окончательного разряда батарей системы резервного энергопитания должно быть достаточно для работы всего оборудования узла связи в течение не менее 1 часа или ее переводу на автономное питание. В случае отсутствия энергопитания более 45 минут дежурным системным администратором производиться корректное отключение серверов и оборудования по приоритетам. При обнаружении отсутствия энергопитания администратор должен известить о выявленных неполадках свое непосредственное руководство, руководство организации, а также организацию, ответственную за предоставление энергопитания. В случае угрозы полного отключения оборудования в результате разряда батарей системы резервного энергопитания, дежурный администратор должен известить свое непосредственное руководство и произвести необходимые действия по корректному завершению работы оборудования. Сделать отметку в журнале регистрации внештатных ситуаций.

11. Ситуация 3: Воздействие природно-климатических условий

Описание:	Ситуации возникновения стихийных природно-климатических воздействий (землетрясение, наводнения, ураганы)
Действия по идентификации:	В случае если в непосредственной близости от помещения с серверами наблюдаются стихийные

	природно-климатические воздействия (землетрясение, наводнения, ураганы.) необходимо переходить к действиям по устранению.
Действия по устранению:	1. Вызвать службу МЧС, 112 2. Поставить в известность непосредственное руководство о возникшей ситуации 3. Поставить в известность дежурных специалистов, отвечающих за техническое сопровождение серверов по тел: 4. Сделать отметку в журнале регистрации внештатных ситуаций.

12. Ситуация 4: Пожар или возгорание

Описание:	Ситуации при возникновении пожара или возгорания
Действия по идентификации:	В случае если в непосредственной близости с серверами наблюдается пожар или возгорание необходимо переходить к действиям по устранению.
Действия по устранению:	1. Вызвать пожарную службу тел: 101, звонок с моб. тел.: 010 2. В случае если сервера находятся в здании организации, необходимо вызвать противопожарную службу и сообщить дежурному диспетчеру. 3. Выполнять действия по «Инструкции по пожарной безопасности». 4. Поставить в известность непосредственное руководство о возникшей ситуации. 5. Поставить в известность дежурных специалистов, отвечающих за техническое сопровождение серверов по тел: 6. Сделать отметку в журнале регистрации внештатных ситуаций.

13. Ситуация 5: Нарушение политики информационной безопасности

Описание:	Ситуация при нарушении требований политики информационной безопасности.
Действия по идентификации:	Ознакомьтесь с политикой информационной безопасности. В случае если вы владеете информацией или наблюдаете ситуацию о нарушениях требований политики информационной безопасности, необходимо переходить к действиям по устранению.
Действия по устранению:	Поставить в известность непосредственное руководство о возникшей ситуации. Поставить в известность дежурных специалистов Отдела информационной безопасности. тел: Сделать отметку в журнале регистрации внештатных ситуаций.

14. Порядок установки, обновления и удаления ПО на серверах и рабочих станциях

15. Все изменения конфигурации технических и программных средств серверов АИС и рабочих станций (РС) должны производиться только на основании заявок начальников структурных подразделений, руководящих документов центральных государственных органов касательно правил информационного обмена с межгосударственными информационными системами либо распоряжений руководства эксплуатирующей АИС организации (Службы техподдержки).

16. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных рабочих станций и серверов АИС предоставляется:

1) в отношении системных и прикладных программных средств, а также в отношении аппаратных средств уполномоченным сотрудникам эксплуатирующей АИС организации;

2) в отношении программно-аппаратных средств защиты уполномоченным сотрудникам Службы техподдержки;

17. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов АИС кем-либо, кроме вышеперечисленных сотрудников, ЗАПРЕЩЕНО.

18. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится уполномоченными сотрудниками Службы техподдержки. Работы производятся в присутствии ответственного за информационную безопасность подразделения и пользователя данной РС (в случае работ на РС).

19. Подготовка модификаций программного обеспечения серверов АИС и рабочих станций, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в Фонд алгоритмов и программ организации (далее – ФАП) и другие необходимые действия производится согласно утвержденным инструкциям.

20. Установка или обновление подсистем АИС должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

21. Установка и обновление общего ПО (системного, тестового и т.п.) на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, а прикладного ПО - с эталонных копий программных средств, полученных из ФАП. При необходимости (в случае установки части компонент на дисках сетевых серверов) к работам привлекаются администраторы сети (серверов) и администраторы баз данных.

22. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

23. После установки (обновления) ПО администратор должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром и проверить работоспособность ПО и правильность настройки средств защиты совместно с пользователем ПК.

24. После завершения работ по внесению изменений в состав аппаратных средств системный блок должен закрываться сотрудником на ключ (при наличии штатных механических замков) и опечатываться (пломбироваться, защищаться специальной наклейкой) сотрудником службы ИБ.

25. Уполномоченные исполнители работ от Службы техподдержки и службы ИБ должны произвести соответствующую запись в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств РС подразделения», делают отметку о выполнении (на обратной стороне заявки) и передают исполненную заявку ответственному за информационную безопасность в подразделении для хранения вместе с формуляром данной РС (сервера).

26. Формат записей Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств РС подразделения:

N п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного пользователя РС, подпись	Подпись ответственного за информационную безопасность подразделения	Примечание
1	2	3	4	5	6	7

27. В случае установки системного ПО АИС на новый сервер действия выполняются в соответствии с документом «Руководство пользователя – системного администратора.

6. Требования к процедурам управления изменениями и анализа ПО в случае изменения системного ПО

28. После установки (обновления) программных средств АИС администратор обязан проверить работоспособность сервера, при изменении ПО ПК – ее работоспособность и правильность настройки средств защиты, установленных на компьютере.

29. При установке нового (обновлении существующего) ПО АИС администратор обязан:

1) установить права доступа пользователей системы к файлам программного средства таким образом, как это указано в формуляре на программное средство (задачу);

2) проверить корректность функционирования системы защиты;

3) в режиме обычного пользователя необходимо проверить возможность использования всех функций АИС согласно правам доступа данного пользователя;

4) внести соответствующие изменения в формуляр сервера АИС или РС пользователя.

30. Чтобы свести к минимуму повреждения АИС в случае изменений системного ПО, следует строго контролировать внедрение изменений - строго придерживаться формализованных процедур обеспечения информационной безопасности; осуществлять контроль за возможной компрометацией самих процедур; программистам, отвечающим за поддержку, предоставлять доступ только к тем частям системы, которые необходимы для их работы.

31. Необходимо обеспечить предварительное тестирование изменений ПО, для чего используется серверное оборудование, которое отделено от среды разработки и среды промышленной эксплуатации. При этом обеспечивается возможность контроля нового программного обеспечения и дополнительная защита информации, используемой в процессе тестирования.

32. Мероприятия по обеспечению ИБ при проведении изменений в ПО АИС включают в себя:

1) обеспечение протоколирования согласованных уровней авторизации;

2) обеспечение уверенности в том, что запросы на изменения исходят от авторизованных соответствующим образом пользователей;

3) анализ мер информационной безопасности и процедур, обеспечивающих целостность используемых систем;

4) идентификацию всего программного обеспечения, информации, объектов, баз данных и аппаратных средств, требующих изменение;

5) получение формализованного одобрения детальных запросов/предложений на изменения перед началом работы;

6) разрешение внесения изменений в прикладные программы авторизованным пользователем до их непосредственной реализации;

7) обеспечение обновления комплекта системной документации после завершения каждого изменения и архивирования или утилизации старой документации;

8) поддержку контроля версий для всех обновлений программного обеспечения;

9) регистрацию в журналах аудита всех запросов на изменение;

10) корректировку эксплуатационной документации и пользовательских процедур в соответствии с внесенными изменениями;

11) осуществление процесса внедрения изменений в согласованное время без нарушения затрагиваемых бизнес-процессов и остановки АИС более чем на 15 минут в рабочее время.

33. При внесении изменений в операционные системы серверов АИС необходимо провести анализ и тестирование прикладного ПО с целью удостовериться в отсутствии негативного влияния на работу АИС и информационную безопасность организации.

34. Необходимо избегать модификаций пакетов программ, а все требуемые изменения должны подлежать строгому контролю.

35. В случае существенных изменений оригинальное программное обеспечение следует сохранять в ФАП, а изменения следует вносить в четко идентифицированную копию. Программное обеспечение для управления процессом обновления должно быть выполнено для обеспечения наиболее современных утвержденных модификаций (патчи) и обновления приложений, установленных для всего авторизованного программного обеспечения.

36. Все изменения необходимо полностью тестировать и документировать таким образом, чтобы их можно было повторно использовать, при необходимости, для будущих обновлений программного обеспечения. При необходимости изменения должны быть проверены и подтверждены независимым органом оценки.

7. Ответственность

37. Администратор АИС несет ответственность за:

1) ненадлежащее выполнение своих функциональных обязанностей;

2) не обеспечение надлежащих условий эксплуатации АИС, сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции.

38. Лица, нарушившие требования настоящего документа, привлекаются к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.