Автономная некоммерческая организация высшего образования

«Институт непрерывного образования»

(АНО ВО «ИНО»)

УТВЕРЖДАЮ:

Ректор АНО ВО «ИНО»

_____ Цветлюк Л.С.

«30» декабря 201 7 г.

Подписано цифровой подписью: АНО ВО "ИНО"
DN: ОГРН=1087746806311, STREET=Шоссе Энтузиастов д. 56 стр.32 офис 214, ИНН=007720623379, C=RU, L=г. Москва, S=77 г. Москва, E=ca@astralm.ru, O="ООО ""АСТРАЛ-М""", CN="ООО ""АСТРАЛ-М"""
Причина: Я утвердил этот документ
Местонахождение: г. Москва, Рязанский пр-т, 86/1
Дата: 30 Декабрь 2020 г. 12:43:37

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Москва, 20 17 год

1. Общие положения

1.1. Инструкция администратора информационной системы персональных данных (далее – Инструкция) разработана в целях обеспечения работоспособности элементов информационной системы персональных данных и средств защиты персональных данных.

1.2. Администратор информационной системы персональных данных (далее - Администратор) назначается и освобождается от исполнения своих обязанностей приказом ректора Автономной некоммерческой организации высшего образования «Институт непрерывного образования» (далее – Институт), в пределах полномочий подчиняется ответственному лицу за организацию обработки персональных данных.

II. Обязанности администратора

2.1. Администратор обязан:

2.1.1. Выполнять требования действующих нормативных правовых актов, а также внутренних инструкций по защите информации.

2.1.2. Производить установку, настройку и своевременное обновление элементов информационной системы персональных данных:

– программного обеспечения автоматизированного рабочего места и серверов (операционные системы, прикладное и специальное программное обеспечение);

– аппаратных средств;

– аппаратных и программных средств защиты.

2.1.3. Обеспечивать работоспособность элементов информационной системы персональных данных и локальной вычислительной сети.

2.1.4. Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.1.5. В случае отказа работоспособности технических средств или программного обеспечения элементов информационной системы персональных данных, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.1.6. Информировать администратора безопасности и лицо, ответственное за организацию обработки персональных данных, о выявленных фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам информационной системы персональных данных.

2.1.7. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ

или нарушения функционирования информационной системы персональных данных или средств защиты.

2.1.8. Обеспечивать выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующую квалификацию.

При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения конфиденциальной информации без предварительного уничтожения данных администратором информационной безопасности.

2.1.9. Присутствовать при выполнении технического обслуживания элементов информационной системы персональных данных сотрудниками сторонних организаций.

2.1.10. Принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий.

2.1.11. Все компоненты программного и аппаратного обеспечения информационной системы персональных данных должны использоваться администратором только в служебных целях. Использование их в других целях запрещается.

2.1.12. Все изменения конфигурации технических и программных средств осуществляются только после согласования планируемых изменений с администратором безопасности.

2.1.13. Любые изменения состава и конфигурации технических средств и программного обеспечения должны быть предварительно проанализированы на предмет их соответствия политике безопасности. Все добавляемые компоненты должны быть проверены на работоспособность, отсутствие вирусов и специальных вложений (вредоносных программ), а также отсутствие реализации опасных функций.

III. Антивирусный контроль

3.1. Для защиты рабочих станций необходимо использовать антивирусные программы:

– резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

– утилиты для обнаружения и анализа новых вирусов.

3.2. К использованию допускаются только сертифицированные лицензионные средства защиты от вредоносных программ.

3.3. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке применяемых средств антивирусной защиты.

3.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов.

3.5. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

3.6. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных файлов операционной системы и загружаемых файлов. В этом случае полная проверка должна осуществляться не реже одного раза в месяц в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед.

3.7. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

3.8. Применять антивирусное программное обеспечение, обеспечивающее проверку всех сообщений электронной почты. В случае, если проверка сообщения электронной почты показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться.

3.9. Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

3.10. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через

которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

– отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;

– немедленно сообщить о факте обнаружения вирусов непосредственному руководителю с указанием предположительного источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

IV. Планирование резервного копирования и восстановления информации

4.1. Для обеспечения целостности и доступности информационных систем персональных данных (баз данных информационных систем персональных данных, других необходимых данных) администратор формирует План резервного копирования информации (Приложение 1).

4.2. План резервного копирования информации включает в себя:

– периодичность резервного копирования;

– тип резервного копирования;

– параметры отчуждаемых носителей резервных копий;

– места хранения отчуждаемых носителей резервных копий;

– Ф.И.О. или должность работника, ответственного за создание и/или хранение отчуждаемых носителей резервных копий.

4.3. Периодичность резервного копирования определяется на основании важности и частоты изменения информации.

4.4. Тип резервного копирования основан на анализе состояния атрибута «архивный» у файлов, содержащих информацию. Сброшенный атрибут автоматически восстанавливается операционной системой при изменении файла.

4.5. Типы резервного копирования подразделяются на:

– полный (Normal), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация, при этом атрибут «архивный» у каждого файла сбрасывается;

– дифференциальный (Differential), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация, у которой атрибут

«архивный» у каждого файла установлен, при этом сам атрибут «архивный» в процессе копирования не изменяется;

– инкрементальный (Incremental), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация, у которой атрибут «архивный» у каждого файла установлен, при этом сам атрибут «архивный» в процессе копирования сбрасывается;

– ежедневный (Daily), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация, измененная в указанный день, независимо от состояния «архивного» атрибута копируемых файлов. Состояние атрибута «архивный» не изменяется;

– копирующий (Copy), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация. Атрибут «архивный» не анализируется и не изменяется.

4.6. Периодичность и тип резервного копирования являются определяющими параметрами при определении скорости и трудоемкости как создания резервных копий так и при восстановлении из них информации поврежденной в результате аппаратного сбоя или реализации иной угрозы.

4.7. Выбор схемы резервного копирования определяется администратором по согласованию с администратором безопасности по следующим параметрам:

– критичность к скорости восстановления работоспособности информационной системы;

– объем данных информационной системы;

– частота изменения данных информационной системы;

– периодичность создания резервных копий;

– тип носителей резервных копий.

4.8. Рекомендуются следующие варианты:

4.8.1. Занимает больше места, дольше выполняется, но быстрее восстанавливается (используются два контейнера, первый и последний):

– один раз в неделю в выходной – полная резервная копия;

– ежедневно – дифференциальная копия.

4.8.2. Занимает меньше места, быстрее выполняется, но дольше восстанавливается (используются все созданные контейнеры от первого до последнего):

– один раз в неделю в выходной – полная резервная копия;

– ежедневно – инкрементальная копия.

4.8.3. Занимает очень много места, в сравнении с предыдущими вариантами, долго выполняется, но восстанавливается быстрее всех:

– ежедневно – копирующая резервная копия.

4.9. Администратор, при составлении Плана резервного копирования, должен проанализировать требования, предъявляемые к целостности и доступности данных конкретной информационной системы и выбрать наиболее подходящие периодичность и тип резервного копирования для данной информационной системы.

4.10. На этапе исполнения Плана резервного копирования, администратор обязан неукоснительно соблюдать сроки создания копий, анализировать состояние сменных носителей (количество сбойных участков, объем свободного места) и незамедлительно докладывать ректору обо всех произошедших или ожидаемых отклонениях от плана.

4.11. Администратор обязан разработать и согласовать со всеми соответствующими ответственными работниками Регламент восстановления поврежденных или утраченных данных информационной системы (Приложение 2).

4.12. В регламенте необходимо указать:

– Ф.И.О. или должность работника ответственного за содержание данных информационной системы (владелец информационной системы персональных данных – начальник соответствующего отдела);

– способ связи с ответственным сотрудником, в том числе экстренный;

– местонахождение Плана резервного копирования с отметками об исполнении;

– место хранения носителей резервных копий;

– Ф.И.О. или должность работника ответственного за создание и/или хранение резервных копий;

– порядок действий по определению признаков повреждения информационной системы,

– принятию решения на восстановление данных, предварительному извещению и получению санкции ответственных сотрудников, и непосредственному восстановлению информации из резервных копий, включая предварительное копирование (при возможности) файлов с поврежденной информацией.

4.13. Администратор обязан не реже одного раза в месяц проверять работоспособность созданных резервных копий путем тестового восстановления данных на резервной системе.

Отметка о проведении тестового восстановления проставляется в соответствующем поле Плана резервного копирования.

4.14. Администратор обязан согласовывать любые изменения настроек резервного копирования с администратором безопасности и незамедлительно вносить изменения в План резервного копирования и Регламент восстановления поврежденных или утраченных данных информационной системы. После любых изменений настроек резервного копирования администратор обязан проверить работоспособность созданных с измененными настройками резервных копий путем восстановления данных на резервной системе.

V. Мониторинг производительности автоматизированных систем

5.1. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

VI. Права администратора

6.1. Администратор имеет право:

6.1.1. Требовать от работников Организации соблюдения правил работы со средствами защиты информации.

6.1.2. Осуществлять взаимодействие с работниками (давать необходимые рекомендации, проводить консультации, получать требуемые сведения) по вопросам эксплуатации технических и программных средств с целью улучшения качества их работы, а также своевременного предупреждения аварийных ситуаций.

VII. Ответственность администратора

7.1. Администратор несет ответственность:

7.1.1. За неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей инструкцией.

7.1.2. За совершенные в процессе осуществления своей деятельности правонарушения – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

7.1.3. За причинение материального ущерба – в пределах, определенных действующим трудовым, уголовным и гражданским законодательством Российской Федерации.

Приложение 1
к Инструкции администратора
информационной системы
персональных данных

План резервного копирования информации

_____

Наименование информационной
системы персональных данных

Резервному копированию подлежит информация, расположенная на следующих информационных ресурсах:

№ п/п	Имя компьютера/сервера	Расположение информации в компьютере/сервере	Объем информации	Частота изменения информации	Ответственный за компьютер/сервер	Месторасположение компьютера/сервера

Резервное копирование выполняется по следующей схеме:

	Полное	Дифференциальное	Инкрементальное	Ежедневное	Копирующее
Понедельник					
Вторник					
Среда					
Четверг					
Пятница					
Суббота					
Воскресенье					

1. Полное резервное копирование на неотчуждаемый носитель информации выполняется в _____.

2. Дифференциальное копирование на неотчуждаемый носитель информации выполняется в _____ каждый день с понедельника по пятницу.

3. Запись копии на отчуждаемый носитель осуществляется Администратором не позднее ____ каждого рабочего дня (понедельник пятница).

4. Отчуждаемый носитель (flash-накопитель) ежедневно получается (под роспись в журнале учета носителей) Администратором у Администратора безопасности, ответственного за хранение отчуждаемых носителей содержащих персональные данные.

5. После записи резервной копии на отчуждаемый носитель Администратор сдает носитель Администратору безопасности.

6. Один раз в месяц (с первого по третье число) Администратор дополнительно сохраняет полную копию на специально маркированный оптический диск и, с помощью этой копии, проводит тестовое восстановление информации на резервной системе. Проверенная копия сдается сотруднику ответственному за хранение отчуждаемых носителей содержащих персональных данных.

Обо всех выполненных действиях Администратор и Администратор безопасности делают отметки в Журнале работы с резервными копиями:

№ п/п	Создание копии						Хранение копии		Проверка копии		
	Дата	Ресурс	Тип	Носитель	Исполнитель	Следующая	Место	Ответственный	Дата	Причина	Результат

Процедура создания резервной копии:

Администратор производит вход на компьютер содержащий информационный ресурс, подлежащий резервному копированию, с использованием идентификатора и пароля пользователя «Администратор» и выполняет следующие действия:

- контроль целостности автоматически созданных архивных копий информации (ежедневно);
- копирование последней (по дате создания) архивной копии на отчуждаемый носитель (ежедневно);
- контроль целостности, сохраненной на отчуждаемый носитель архивной копии;
- архивирование журналов средств защиты информации на отчуждаемый носитель (ежемесячно).

2. Выдача Администратору идентификаторов пользователя «Администратор» и отчуждаемого носителя конфиденциальной информации без регистрации в журнале регистрации, учета и выдачи носителей информации не допускается.

Приложение 2
к Инструкции администратора информационной системы персональных данных

РЕГЛАМЕНТ ВОССТАНОВЛЕНИЯ ПОВРЕЖДЕННЫХ ИЛИ УТРАЧЕННЫХ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В случае возникновения сбоев в работе компонентов информационных систем персональных данных, средств защиты информации, возникновения инцидентов информационной безопасности, приведших к частичной или полной потере функциональности информационных систем персональных данных, Администратор информационной системы персональных данных обязан:

1. Незамедлительно уведомить сотрудников, выполняющих обработку персональных данных, о необходимости прекращения текущей работы; а также ректора Института.

2. Проанализировать состояние аппаратных и программных технических средств, журналы событий и действия сотрудников непосредственно перед возникновением сбоя, определить причины сбоя и методы его устранения.

3. Перед проведением операций по восстановлению провести внеплановое резервное копирование баз данных, файлов пользователей и журналов безопасности.

4. Устранить причину сбоя. При необходимости переустановки операционные системы, средств защиты информации, антивирусные средства, прикладное программное обеспечение устанавливаются только с эталонных дистрибутивов. Порядок установки и восстановления программного обеспечения подробно описан в сопроводительной документации к этому программному обеспечению.

5. Произвести настройку переустановленного программного обеспечения в соответствии с эксплуатационной документацией. При необходимости восстановить базы данных, пользовательские файлы.

6. Протестировать все компоненты информационной системы персональных данных после восстановления.

7. Уведомить ответственных сотрудников о завершении работ по восстановлению компонентов информационной системы персональных данных.

8. Документально оформить факт потери функциональности информационной системы персональных данных с указанием даты, времени, причин сбоя, мер, предпринятых для восстановления, рекомендаций по предотвращению подобных сбоев.

9. В случае необходимости передачи аппаратных средств информационных систем персональных данных сторонней организации для ремонта произвести полное стирание персональных данных с передаваемых носителей.