Приложение № 7
к приказу № 78/2-ОД от 16.08.2021г

Инструкция
администратору безопасностиинформационной системы МБДОУ «Ерёминский детский сад»

1. Общие положения

Настоящая Инструкция администратору безопасности информационной системы МБДОУ «Ерёминский детский сад»(далее – Инструкция) определяет функции, права и обязанности администратора безопасности информационной системы МБДОУ «Ерёминский детский сад» (далее – ИС).

Администратор безопасности ИС назначается из числа сотрудников МБДОУ «Ерёминский детский сад» приказом заведующего МБДОУ «Ерёминский детский сад» обеспечивает правильность использования и нормальное функционирование системы защиты информации ИС (далее – СЗИ ИС).

Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. Основные функции администратора безопасности ИС

2.1. Контроль за выполнением требований действующих нормативных документов по вопросам защиты информации при её обработке в ИС.

2.2. Контроль за порядком доступа лиц в помещения, где установлены компоненты ИС, в соответствии сПеречнем лиц, имеющих право доступа впомещения ИС.

2.3. Ведение и хранение документации на ИС;

2.4. Ведение учета, хранение и выдача машинных носителей информации;

2.5. Ведение учета средств защиты информации, используемых в ИС;

2.6. Настройка и сопровождение в процессе эксплуатации подсистемы идентификации и аутентификации субъектов доступа и объектов доступа.

2.6.1. Управление идентификаторами (именами учётных записей пользователей), в том числе создание, присвоение, уничтожение идентификаторов.При этом администратор безопасности ИС:

- формирует уникальный идентификатор (логин), который однозначно идентифицирует пользователя;
- присваивает идентификатор пользователю ИС на основании Перечня лиц, допущенных к обработке информации ограниченного распространения в ИС;
- следит за исключением повторного использования идентификатора пользователя в период выполнения пользователем должностных обязанностей;
- заблаговременно блокирует идентификатор пользователя на период долговременного отсутствия пользователя;
- блокирует идентификатор пользователя через период времени неиспользования – 90 дней;
- исключает повторное использование идентификатора пользователя в течение одного года.

2.6.2. Управление средствами аутентификации (паролями), в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.Порядок управления средствами аутентификации определён в Инструкции по организации парольной защиты в ИС.

2.7. Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом субъектов доступа к объектам доступа.

2.7.1. Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей.При этом администратор безопасности ИС:

- определяет тип учётной записи (внутреннего пользователя, системная, приложения);
- осуществляет объединение учётных записей в группы (при необходимости);
- осуществляет верификацию пользователя (проверку личности пользователя, его должностных (функциональных) обязанностей) при заведении учётной записи пользователя;
- заводит учётную запись пользователя в ОС;
- присваивает учётную запись конкретному пользователю ИС;
- предоставляет пользователю права доступа к объектам доступа ИС в соответствии с Разрешительной системой доступа субъектов доступа к объектам доступа ИС;
- при необходимости производит корректировку учётных записей пользователей;
- на период длительного отсутствия пользователя блокирует его учётную запись в средстве защиты информации (далее – СЗИ)от несанкционированного доступа (далее – НСД)и в операционной системе.

2.7.2. Разработка и поддержание в актуальном состоянии Разрешительной системы доступа субъектов к объектам доступа ИС.

2.7.3. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа на основании Разрешительной системы доступа субъектов к объектам доступа ИС.

2.7.4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС на основании Разрешительной системы доступа субъектов к объектам доступа ИС.

2.7.5. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС, на основании Разрешительной системы доступа субъектов к объектам доступа ИС.

2.7.6. Ограничение неуспешных попыток входа в ИС (3 неуспешные попытки входа).

2.7.7. Настройка механизмов блокирования сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.

2.7.8. Запрет действий пользователей в ИС до идентификации и аутентификации.

2.7.9. Контроль использования в ИС мобильных технических средств.

2.7.10. Управление установкой (инсталляцией) компонентов программного обеспечения (далее – ПО), в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО.

2.7.11. Установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов в соответствии с Перечнем программного обеспечения, разрешённого к использованию ИС и Перечнем типов программного обеспечения, запрещенного для установки в ИС.

2.8. Настройка и сопровождение подсистемы защиты машинных носителей информации.

2.8.1. Контроль использования в ИС только учтённых машинных носителей информации.

2.8.2. Управление доступом к машинным носителям информации.

2.8.3. Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации.

2.8.4. Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) с использованием механизмов СЗИ от НСД.

2.9. Настройка и сопровождение подсистемы регистрации событий безопасности.

2.9.1. Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

2.9.2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

2.9.3. Установка в СЗИ необходимых параметров регистрации событий безопасности.

2.9.4. Регулярное проведение анализа журналов регистрации событий СЗИ, а также системных журналов операционной системы и прикладного программного обеспечения ИС с целью выявления попыток несанкционированного доступа к защищаемым ресурсам. Мониторинг и анализ зарегистрированных событий безопасности должен проводиться не реже одного раза в неделю, а также при выявлении инцидентов безопасности.

2.9.5. Настройка и сопровождение подсистемы антивирусной защиты в соответствии с Инструкцией по организации антивирусной защиты в ИС.

2.10. Сопровождение подсистемы контроля (анализа) защищённости информации.

2.10.1. Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей.

2.10.2. Контроль установки обновлений ПО, включая обновление ПОСЗИ.

2.10.3. Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ.

2.10.4. Контроль состава технических средств, ПО и СЗИ.

2.10.5. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС.

2.11. Настройка и сопровождение подсистемы обеспечения целостности информационной системы и информации.

2.11.1. Осуществление контроля над резервным копированием информации.

2.11.2. Резервное копирование защищаемой информации на учтённый машинный носитель информации, не менее одного раза в неделю.

2.11.3. Восстановлениезащищаемой информации с резервных машинных носителей информации (резервных копий) в течение одного рабочего дня.

2.11.4. Совместно с системным администратором ИС осуществляет восстановление ИС, при возникновении нештатных ситуаций, включающее:

– восстановление ПО, включая ПО средств защиты информации, из резервных копий (дистрибутивов) ПО;

– импорт ранее выполненных настроек средств защиты информации и проверка работоспособности системы защиты информации, обеспечивающие необходимый класс защищенности информации;

– возврат ИС в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ИС, позволяющих решать задачи по обработке информации.

2.12. При необходимости выполнения технического обслуживания элементов ИС, администратор безопасности ИС руководствуется Инструкцией о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления

программного обеспечения, включая обновление программного обеспечения средств защиты информации в ИС.

2.13. Настройка и сопровождение подсистемы защиты информационной системы, ее средств, систем связи и передачи данных.

2.13.1. Контрольработы пользователей ИС в сетях общего пользования и (или) международного обмена (сети «Интернет») в соответствии с Инструкцией о порядке работы при подключении к информационно-телекоммуникационным сетям международного информационного обмена в ИС.

2.13.2. Контроль работоспособности средств межсетевого экранирования.

2.13.3. Обеспечение защиты мобильных технических средств, применяемых в ИС.

2.13.4. Изменение правил фильтрации межсетевого экранирования на основании заявок лица, ответственного за защиту информации при необходимости использования новых сервисов (систем) или на основании выявленных инцидентов. Изменение правил фильтрации межсетевого экранирования необходимо фиксировать в Разрешительной системе доступа.

2.13.5. Периодическое предоставление лицу, ответственному за защиту информации в ИС, отчета о состоянии защищенности информации, обрабатываемой в ИС, о нештатных ситуациях при работе в ИС, о допущенных пользователями ИС нарушениях установленных требований по защите информации.

3. Обязанности

Администратор безопасности ИС обязан:

– обеспечивать функционирование и поддерживать работоспособность СЗИ ИС в пределах возложенных на него функций;

– проводить инструктажи пользователей по правилам работы в ИС;

– в случае отказа СЗИ принимать меры по их восстановлению;

– докладывать ответственному за защиту информации в ИС о неправомерных действиях пользователей ИС, приводящих к нарушению требований по защите информации;

– проводить мероприятия по выявлению возможных каналов утечки защищаемой информации при эксплуатации ИС и подготовке предложений по совершенствованию СЗИ ИС;

– вести документацию на ИС в соответствии с требованиями нормативных документов.

4. Права

Администратор безопасности ИС имеет право:

– участвовать в служебных расследованиях по вопросам несоблюдения требований организационно-распорядительных документов по защите информации;

– требовать прекращения обработки защищаемой информации в ИС в случае нарушения установленного порядка работ или нарушения функционирования СЗИ ИС.

5. Ответственность

Администратор безопасности несет персональную ответственность за:

– неисполнение, несвоевременное или некачественное выполнение возложенных на него обязанностей по защите информации при её обработке в ИС;

– достоверность отчетных данных и других подготавливаемых материалов;

– качество работ по защите информации в соответствии с функциональными обязанностями;

– соблюдение режима конфиденциальности защищаемой информации при её обработке и хранении в ИС;

– соблюдение требований нормативных правовых актов, приказов, распоряжений и инструкций, определяющих порядок организации работ по защите информации.

Разработчик инструкции: заведующий
МБДОУ «Ерёминский детский сад» Лукошенко Л.В. _____

Лист ознакомления с инструкцией администратору безопасности информационной системы МБДОУ «Ерёминский детский сад»

№ п/п	Ф.И.О. работника	Дата ознакомления	Личная подпись