УТВЕРЖДАЮ
Заведующий Муниципального
бюджетного дошкольного
образовательного учреждения
«Детский сад комбинированного вида
№30»

_____ (подпись) Л.Д. Расинская

«11» января 2021 г.

ТЕХНОЛОГИЧЕСКАЯ ИНСТРУКЦИЯ

администратора безопасности информации (ответственного за обработку персональных данных) по обработке информации в автоматизированной системе сегмент региональной информационной системы доступности дошкольного образования в Ставропольском крае Муниципального бюджетного дошкольного образовательного учреждения «Детский сад комбинированного вида №30» требованиям по безопасности информации

1. Общие положения

Настоящая инструкция определяет основные функции и порядок работы ответственного за обработку персональных данных (ответственного за эксплуатацию, внештатного сотрудника по защите информации, и т.п.) (далее – администратора безопасности) в технологическом процессе обработки персональных данных (конфиденциальной информации) в автоматизированной системе сегмент региональной информационной системы доступности дошкольного образования в Ставропольском крае (далее - АС), являющейся объектом информатизации, Муниципального бюджетного дошкольного образовательного учреждения «Детский сад комбинированного вида №30» (далее - Учреждение).

В процессе выполнения своих служебных обязанностей администратор безопасности должен выполнять требования конструкторской документации, поставляемой со средствами защиты информации, нормативных и правовых документов по защите информации и руководствоваться ими на этапе эксплуатации средств защиты информации:

- СКЗИ VipNet Client;
- СЗИ от НСД «Dallas Lock»;
- средства антивирусной защиты информации (САВЗ).

Как правило, особенности, порядок настройки и эксплуатации средств защиты информации описан в:

- Руководстве администратора.
- Руководстве пользователя.

2. Функции администратора безопасности

2.1. При эксплуатации средств защиты информации подсистемы сетевой защиты информации АС.

В составе системы защиты информации АС Учреждения средствами СКЗИ VipNet Client и средствами антивирусной защиты информации представлена подсистема сетевой защиты.

Администратор по безопасности должен ознакомиться с особенностями и требованиями к эксплуатации средств защиты информации (описаны в соответствующих руководствах) и руководствоваться ими в своей деятельности.

При этом администратор по безопасности, в ходе эксплуатации средств защиты информации подсистемы сетевой защиты обязан:

- периодически проводить проверку соответствия контрольных сумм установленных средств защиты информации на соответствие суммам, указанным в эксплуатационных документах;
- осуществлять проверку настроек программных средств защиты информации их соответствию конструкторской (эксплуатационной) документации в ходе эксплуатации;

- организовывать подключение АС к защищенной сети в строгом соответствии с «Регламентом….» разрабатываемым Оператором сети;

- организовать настройку правил фильтрации (прохождения) IP-пакетов;

- провести настройку сетевых фильтров средств межсетевого экранирования;

- убедиться в работоспособности функций МЭ по контролю за сетевой активностью Приложений АС;

- заблокировать средствами операционной системы и проверить блокировку удаленного доступа к АС средствами МЭ;

- включить механизм защиты модулей и исполняемых файлов средств антивирусной защиты, исключающий доступ к ним Пользователей АС;

- настроить автоматический режим обновления базы сигнатур САВЗ с периодичностью не реже чем 1 раз в сутки;

- настроить автоматический режим полного сканирования АС САВЗ с периодичностью не реже чем 1 раз в неделю.

2.2. При эксплуатации средств защиты от НСД

Администратор безопасности обязан:

- выполнять начальную установку и настройку комплекса СЗИ от НСД на средствах вычислительной техники (далее – СВТ) из состава АС (объекта информатизации);

- вести учет электронных идентификаторов СЗИ от НСД «Dallas Lock», выполнять действия по их регистрации в АС объекта информатизации, организовывать их выдачу пользователям и периодически контролировать их наличие;

- проводить работы по генерации и регулярной смене паролей пользователей;

- выполнять действия по настройке СЗИ от НСД «Dallas Lock», в АС (объекта информатизации) в соответствии с утвержденными правилами разграничения доступа (матрицей доступа);

- осуществлять оперативный контроль над функционированием СЗИ от НСД «Dallas Lock», в АС (на объекте информатизации), проводить его периодическое тестирование и осуществлять контроль целостности резервных копий программного обеспечения комплекса на носителях;

- проводить проверки целостности программного обеспечения;

- осуществлять постоянный контроль над соблюдением операторами (пользователями) технологии обработки персональных данных (конфиденциальной информации), анализировать содержимое регистрационных журналов, формируемых СЗИ от НСД «Dallas Lock», и принимать конкретные меры по выявленным нарушениям;

- организовывать и контролировать проведение работ по ремонту, наладке и сервисному обслуживанию АС и вспомогательных технических средств объекта информатизации;

- контролировать сохранность и целостность эталонных копий программного обеспечения;

- оказывать методическую и консультационную помощь операторам (пользователям) объекта информатизации в процессе эксплуатации СЗИ от НСД «Dallas Lock».

3. Установка и настройка СЗИ от НСД «DALLAS LOCK»

3.1. Установка (повторная установка) комплекса СЗИ от НСД «Dallas Lock», выполняется в следующих ситуациях:

- на этапе ввода в действие объекта информатизации;
- в случае выхода из строя накопителей с персональными данными (конфиденциальной информацией);
- в случае возникновения сбойных и аварийных ситуаций, повлекших нарушения в работе программного обеспечения (далее - ПО) АС;
- в случае ввода новых СВТ в состав объекта информатизации.

3.2. Установка СЗИ от НСД «Dallas Lock» на СВТ объекта информатизации должна выполняться администратором безопасности в строгом соответствии с инструкциями, приведенными в документе «Руководство администратора».

3.3. Установка СЗИ от НСД «Dallas Lock» должна производиться с соответствующим образом учтенных носителей (СД-дисков). Перед установкой комплекса ПО АС должно быть проверено на отсутствие вирусного заражения.

3.4. Установка СЗИ от НСД «Dallas Lock» должна осуществляется в следующем порядке:

- установка программного обеспечения;
- инициализация комплекса;
- подготовка комплекса к эксплуатации.

3.5. Установка правил разграничения доступа производится в соответствии с утвержденными правилами разграничения доступа (матрицей доступа). Регистрация дополнительных (не указанных) в матрице доступа пользователей **запрещена**.

4. Сопровождение средств защиты информации от НСД в процессе эксплуатации

4.1. Ведение служебной информации СЗИ от НСД «Dallas Lock»

Регистрация пользователей

Действия по регистрации пользователей выполняются администратором безопасности на основании оформленных установленным порядком и утвержденных руководителем Учреждения приказов и распоряжений о допуске пользователей к обработке персональных данных (конфиденциальной информации).

В соответствии с установленными уровнями полномочий операторов (пользователей) и эксплуатационной документацией на СЗИ от НСД «Dallas Lock», администратор безопасности разрабатывает правила разграничения

доступа (ПРД) и оформляет матрицу доступа, которая утверждается руководителем Учреждения.

На основании утвержденной матрицы доступа администратор безопасности, в соответствии с эксплуатационной документацией на СЗИ от НСД «Dallas Lock», выполняет действия по настройке системы защиты СЗИ от НСД.

В процессе настройки системы защиты, администратор безопасности должен соблюдать следующие правила:

- все информационные ресурсы, к которым разрешен доступ пользователя (логические диски, каталоги и файлы) должны быть явно указаны;
- каталогам, в которых планируется размещать персональные данные (конфиденциальную информацию) должны быть заранее присвоены соответствующие метки конфиденциальности. Данные каталоги должны быть включены в список контролируемых;
- журнал регистрации должен вестись для всех пользователей;
- должен быть активизирован режим ограничения времени действия пароля по количеству проходов;
- должен быть активизирован режим «Контроль целостности»;
- должен быть активизирован режим полного удаления файлов;
- доступ к портам ввода-вывода должен быть максимально ограничен.

Установка правил разграничения доступа выполняются средствами операционной системы и средствами СЗИ от НСД «Dallas Lock».

Контроль целостности файлов и секторов, журнала транзакций, элементов реестра, PCI-устройств, ACPI, SMBIOS, оперативной памяти обеспечивается средствами СЗИ от НСД «Dallas Lock».

По окончании работ по подготовке комплекса к эксплуатации, администратор безопасности выполняет проверки функционирования общесистемной программной среды каждого зарегистрированного пользователя, тестирует работоспособность СЗИ от НСД «Dallas Lock», и корректность реализации ПРД, распечатывает текущие настройки комплекса и оформляет акт по результатам выполненных работ.

Каждому пользователю выдаётся персонифицированный идентификатор и пароль.

4.2. Генерация и смена паролей

Действия по генерации и смене паролей пользователей должны организовываться администратором безопасности.

Для организации работ по смене паролей администратор безопасности устанавливает ограничения на время действия пароля.

Процедура генерации паролей должна исключать задание в качестве паролей комбинаций критичных с точки зрения их подбора.

Смена паролей выполняется, в соответствии с эксплуатационной документацией на СЗИ от НСД «Dallas Lock».

Установленные (новые) пароли администратор безопасности должен лично сообщать каждому конкретному пользователю. Администратор безопасности несет ответственность за разглашение личных паролей пользователей.

4.3. Сопровождение правил разграничения доступа

Администратор безопасности обеспечивает реализацию разрешительной системы доступа в виде наборов правил разграничения доступа к техническим, программным средствам и информационным ресурсам формируемых для каждого регистрируемого пользователя.

Распределение и изменение прав доступа пользователей к конкретным программам и информационным ресурсам должно осуществляться на основании приказов и распоряжений, утвержденных руководителем Учреждения.

Правила разграничения доступа разрабатываются в соответствии с требованиями разрешительной системы доступа на основании заявок на доступ пользователей и документально оформляются в виде матрицы доступа или в виде дополнений и изменений матрицы доступа и физически реализуются настройками операционной системы.

Заявки на доступ пользователей к техническим средствам объекта должны содержать перечень (список) программ и информационных ресурсов, доступ к которым должен быть предоставлен каждому конкретному пользователю с указанием дисков и каталогов, на которых размещены данные ресурсы.

4.4. Оперативный контроль над функционированием СЗИ от НСД «Dallas Lock»

Администратор безопасности несет ответственность за нормальное функционирование СЗИ от НСД «Dallas Lock» на АС.

Администратор безопасности должен осуществлять периодическое тестирование работоспособности СЗИ от НСД «Dallas Lock». Тестированию подлежат: память платы, датчик случайных чисел и идентификатора.

В случае, когда средства комплекса СЗИ от НСД «Dallas Lock» отказывают в доступе легальным пользователям, администратор безопасности должен анализировать причины отказа в доступе и предпринимать оперативные действия по выявлению возможных нарушений.

Администратор безопасности должен предпринимать оперативные действия в случае возникновения внештатных ситуаций при работе АС, анализировать причины их возникновения и предпринимать необходимые меры по восстановлению работоспособности комплекса СЗИ от НСД «Dallas Lock» и программного обеспечения.

Администратор безопасности должен постоянно контролировать уровень защищенности информации от несанкционированного доступа (далее – НСД) и, в случае выявления возможных каналов утечки информации за счет НСД, предпринимать оперативные меры по их устранению за счет изменения параметров настройки подсистемы разграничения доступа операционной системы.

4.5. Контроль целостности объектов АС

Контроль целостности объектов осуществляется администратором безопасности с использованием функций СЗИ от НСД «Dallas Lock». Для этого администратор создаёт исходные списки объектов, которые необходимо контролировать, и сохраняет эти списки в специальных файлах-шаблонах.

Все исполняемые модули (файлы, содержащие исполняемый или интерпретируемый программный код), входящие в состав общесистемной программной среды доступ к которым разрешен конкретному пользователю, должны быть включены в список контроля целостности.

В случае выявления фактов нарушения целостности компонентов, входящих в состав общесистемного программного обеспечения, администратором безопасности должны предприниматься действия по анализу причин таких нарушений и действия по восстановлению данных компонент с эталонных копий.

Администратор безопасности обеспечивает контроль над сохранностью эталонных копий ПО и должен периодически проводить проверку состояния учтенных носителей, на которых оно расположено.

4.6. Приемка и ввод в эксплуатацию программных средств

Администратор безопасности организует и контролирует выполнение работ по установке новых программных средств, включаемых в состав АС.

Перед установкой дистрибутивные носители с новыми программными средствами, вводимыми в состав АС, должны быть соответствующим образом проверены.

Установка новых программных средств допускается только с проверенных носителей.

Перед установкой новых программных средств, СВТ из состава АС должна быть физически отключена от АС. Если физическое отключение СВТ от АС невозможно (в силу специфики устанавливаемого ПО), выполнение работ по установке новых программных средств допускается только после полного прекращения обработки конфиденциальной информации в АС.

После выполнения работ по установке новых программных средств администратор безопасности проверяет их работоспособность, выполняет необходимые действия по настройке. По результатам выполненных работ оформляется акт приемки нового программного обеспечения и утверждаются дополнения и изменения матрицы доступа.

Допуск пользователей к работе на АС на которых проводились работы по установке нового программного обеспечения разрешается только после утверждения акта приемки и матрицы доступа.

4.7. Контроль за ходом технологического процесса обработки информации

Контроль хода технологического процесса обработки информации администратор безопасности осуществляет путем регистрации и анализа действий Пользователей по системному журналу.

Обработка и анализ системных журналов должен осуществляться регулярно, но не реже чем один раз в неделю.

В случае выявления нарушений администратор безопасности проводит мероприятия по выявлению виновников и причин нарушения. Результаты расследования доводятся до сведения руководства.

5. Оказание методической и консультационной помощи пользователям

Администратор безопасности организует и проводит инструктаж пользователей по правилам применения и эксплуатации СКЗИ, СЗИ и САВЗ, и периодически контролирует их знания.

Администратор безопасности должен оказывать методическую и консультационную помощь пользователям при применении и эксплуатации всех средств защиты информации.