МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №12 «АЛЁНУШКА» ПОСЁЛКА ПСЕБАЙ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ МОСТОВСКИЙ РАЙОН

Безродная Инна Ивановна

Подписан: Безродная Инна Ивановна
DN: ИНН=234203191338, СНИЛС=05016378832, E=mucbo@mail.ru, C=RU, S=Краснодарский край, L=п. Псебай, O="МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №12 "" АЛЕНУШКА"" ПОСЕЛКА ПСЕБАЙ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ МОСТОВСКИЙ РАЙОН", G=Инна Ивановна, SN=Безродная, CN=Безродная Инна Ивановна
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2021-10-19 14:06:38
Foxit Reader Версия: 9.7.2

УТВЕРЖДАЮ:
Заведующий МБДОУ детского сада №12
«Аленушка» пос. Псебай
_____И.И.Безродная
МП «07» сентября 2021г.

ИНСТРУКЦИЯ
администратора безопасности информации Муниципального бюджетного дошкольного образовательного учреждения детского сада № 12 «Аленушка» поселка Псебай муниципального образования Мостовский район

1. Общее положение

1.1. Настоящая Инструкция администратора безопасности информации Муниципального бюджетного дошкольного образовательного учреждения детского сада № 12 «Аленушка» поселка Псебай муниципального образования Мостовский район (далее – Инструкция) разработана в дополнение к «Политике обработки персональных данных Муниципального бюджетного дошкольного образовательного учреждения детский сад №12 «Аленушка» поселка Псебай муниципального образования Мостовский район», является руководящим документом администратора безопасности информации Муниципального бюджетного дошкольного образовательного учреждения детского сада № 12 «Аленушка» поселка Псебай муниципального образования Мостовский район, определяет основные обязанности, права и ответственность администратора информационных систем персональных данных (далее ИСПДн), разработана на основании:

- Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации №781 от 17 ноября 2007г.;
- Приказа №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного ФСТЭК России от 05.02.2010 г.

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

1.3. Персональные данные относятся к категории информации ограниченного распространения.

1.4. Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

1.5. Работа с персональными данными (ПДн) строится на следующих принципах:

- принцип персональной ответственности - в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;
- принцип контроля и учета - все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

1.6. Требования настоящей инструкции должны выполняться во всех режимах функционирования.

1.7. Требования администратора безопасности, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками.

2. Назначение администратора безопасности

2.1. На должность администратора безопасности назначается лицо из числа наиболее квалифицированных пользователей ПЭВМ, либо имеющим образование в области защиты информации, в котором эксплуатируется информационная система.

3. Обязанности администратора безопасности

3.1. В своей повседневной деятельности администратор руководствуется данной инструкцией и другими документами, регламентирующими защиту персональных данных от утечки по техническим каналам и НСД, эксплуатационной документацией на установленные на объекте информатизации системы защиты от несанкционированного доступа к информации (СЗИ НСД) и от утечки информации по техническим каналам.

3.2. Администратор безопасности совместно со специалистами по информационным технологиям и защите информации:
- обеспечивает поддержку подсистем управления доступом, регистрации и учета информационных ресурсов;
- контролирует целостность программно-аппаратной среды, хранимой и обрабатываемой информации;
- контролирует доступность и конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации (устойчивое функционирование ЛВС и ее подсистем).

3.3. На администратора безопасности возлагаются следующие обязанности:
- следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах ПЭВМ;
- знать уровень конфиденциальности обрабатываемой информации и класс ИСПДн, следить за тем, чтобы обработка информации производилась толь о с использованием учтенных съемных и несъемных носителей информации;
- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;
- совместно со специалистами по информационным технологиям и защите информации обеспечивать доступ к защищаемой информации пользователям согласно их прав доступа;
- незамедлительно докладывать руководителю учреждения, обо всех выявленных попытках несанкционированного доступа к информации ограниченного доступа;
- контролировать правильность применения пользователями сети средств защиты информации;
- участвовать в испытаниях и проверках ИСПДн;
- не допускать к работе на рабочих станциях и серверах посторонних лиц;
- осуществлять контроль монтажа оборудования специалистами сторонних организаций;
- участвовать в приемке для нужд новых программных средств;
- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию;
- при изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт ИСПДн, обрабатывающей информацию ограниченного доступа;
- вести журнал учета работы с ИСПДн.
- Регистрации в журнале учета работ ИСПДн подлежат:
- обновление программного обеспечения ИСПДн;
- вскрытие системного блока с целью модернизации или ремонта с указанием цели вскрытия и проводимых работ;

- создание резервной копии базы данных и пр. служебной информации;
- замена системного блока с указанием факта гарантированного удаления информации с жесткого магнитного диска;
- отклонения в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции;
- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.);
- перебои в системе электроснабжения и.т.п.

3.4. При выявлении нарушения первой категории (утечка информации) администратор обязан немедленно прекратить работы в ИСПДн.

3.5. При выявлении нарушений первой, второй и третьей категорий администратор обязан подать служебную записку руководству и занести соответствующую запись в журнал регистрации работ ИСПДн с изложением факта нарушения, предпринятые и/или рекомендуемые им действия (Приложение1).

4. Ответственность

4.1. Администратор безопасности несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на его в соответствии с настоящей Инструкцией и другими нормативными документами по защите информации.

(Приложение1)

Форма журнала регистрации работ ИСПДн:

Дата	Наименование работ	Ф.И.О. исполнителя работ	ИСПДн	Роспись
1	2	3	4	5