**Приложение № 6 к приказу Муниципального общеобразовательного бюджетного учреждения «Лицей № 15»**

**города Вышний Волочек Тверской области от 30 августа 2018 г. № 56-А**

**Инструкция**

**по работе администратора безопасности информации в информационной системе персональных данных Муниципального общеобразовательного бюджетного учреждения «Лицей № 15»  города Вышний Волочек**

1. **Общие положения.**
2. Администратор безопасности информации (далее – АБИ) в информационной системе персональных данных (далее – ИСПДн) назначается из числа сотрудников Муниципального общеобразовательного бюджетного учреждения «Лицей № 15»  города Вышний Волочек (далее – Учреждение) приказом директора и отвечает за обеспечение требуемого уровня защищенности персональных данных при их обработке в ИСПДн.
3. Администратор безопасности информации в своей работе руководствуется требованиями руководящих документов по обеспечению безопасности персональных данных, положениями нормативно-правовых актов РФ, приказами, а также положениями настоящей Инструкции.
4. Администратор безопасности информации является лицом, обеспечивающим безопасность персональных данных, обрабатываемых, передаваемых и хранимых в ИСПДн.
5. Методическое руководство работой АБИ осуществляется ответственным за организацию обработки персональных данных в ИСПДн.
6. **Обязанности администратора безопасности информации ИСПДн.**

**Администратор безопасности информации обязан:**

1. четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по обеспечению безопасности персональных данных при их обработке в ИСПДн и распоряжений, регламентирующих порядок действий по обеспечению безопасности персональных данных;
2. управлять средствами защиты информации (далее - СЗИ) ИСПДн и поддержание их функционирования;
3. восстанавливать функции программных и технических СЗИ от несанкционированного доступа (далее - НСД) к информации;
4. обеспечивать функционирование ИСПДн в пределах возложенных функций;
5. генерировать ключи, личные идентификаторы, а также пароли для пользователей ИСПДн;
6. формировать и управлять списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;
7. назначать права доступа, полномочия и привилегии пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода);
8. обеспечивать правильную эксплуатацию технических и программных СЗИ в ИСПДн;
9. контролировать целостность эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;
10. выявлять, анализировать и устранять уязвимости и иные недостатки в программном обеспечении;
11. в случае нарушения работоспособности (отказе) технических средств и программного обеспечения ИСПДн, в том числе СЗИ, немедленно докладывать о случившемся ответственному за обеспечение безопасности персональных данных в ИСПДн;
12. осуществлять текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации;
13. выполнять и контролировать выполнения установленного комплекса мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн;
14. проводить инструктаж и консультации пользователей ИСПДн по соблюдению установленного режима конфиденциальности при обработке персональных данных в ИСПДн;
15. контролировать соблюдение пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн по вопросам защиты информации от НСД;
16. взаимодействовать с ответственным за организацию обработки персональных данных в Учреждении и ответственным за обеспечение безопасности персональных данных в ИСПДн по вопросам обеспечения безопасности персональных данных при их обработке в ИСПДн и соблюдении прав доступа пользователей к ней;
17. выполнять и учитывать изменения, вносимые:

* в списки пользователей ИСПДн;
* в перечень защищаемых информационных ресурсов ИСПДн;

1. контролировать выполнение утвержденной технологии обработки персональных данных в ИСПДн;
2. контролировать состав технических средств, программного обеспечения и средств зашиты информации;
3. контролировать установку и обновление программного обеспечения, запрет установки неразрешённого программного обеспечения (в том числе средств обработки и отладки);
4. выявлять подозрительные действия пользователей и попытки НСД к информации, обрабатываемой в ИСПДн, путем анализа системных журналов информационной безопасности при работе в ИСПДн;
5. выполнять резервное копирование машинных документов, содержащих персональные данные;
6. обучать и консультировать пользователей ИСПДн правилам работы с СЗИ от НСД;
7. проводить антивирусную защиту информации и программных средств в ИСПДн;
8. контролировать электронный журнал сообщений и обеспечивать доступ к нему лиц, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;
9. просматривать и анализировать результаты регистрации событий, относящихся к безопасности персональных данных, и реагировать на них;
10. контролировать безотказное функционирование технических и программных средств, принимать меры по восстановлению отказавших средств;
11. обеспечивать строгое выполнение требований по обеспечению безопасности персональных данных при организации обслуживания технических средств ИСПДн и отправке их в ремонт;
12. обеспечивать соответствие состава ИСПДн техническому паспорту на ИСПДн (в т.ч. реальной конфигурации информационных связей).
13. **Права администратора безопасности информации ИСПДн.**

**Администратор безопасности информации имеет право:**

1. требовать от пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных;
2. участвовать в разработке мероприятий Учреждения по совершенствованию безопасности персональных данных;
3. останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки персональных данных, приводящих к нарушению функционирования СЗИ;
4. подавать свои предложения по совершенствованию технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн.