Приложение 2
к приказу
_ от 0

ИНСТРУКЦИЯ
ответственного по защите информации ограниченного доступа

1. Общие положения.

1.1 Настоящая Инструкция определяет основные функции, права и обязанности ответственного по защите информации ограниченного доступа (далее – ответственный) при её обработке в информационных системах (далее - ИС) в МОБУ «РУССКАЯ ШУОЛА».

1.2 Ответственный по защите назначается из числа сотрудников школы и обеспечивает правильность использования и нормальное функционирование установленной системы защиты информации (далее - СЗИ) в ИС.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения защиты сведений ограниченного доступа и не исключает обязательного выполнения их требований.

1.4 В соответствии с моделями угроз безопасности, разработанными для ИС школы, актуальными являются только угрозы несанкционированного доступа (далее – НСД).

СЗИ ИС построена на базе:

- встроенных в лицензионные операционные системы:
«Windows 7» (далее - ОС) средств защиты от НСД;
«Windows 8» (далее - ОС) средств защиты от НСД;
«Windows 8.1» (далее - ОС) средств защиты от НСД;
«Windows 10» (далее - ОС) средств защиты от НСД;
- Единой Сети Передачи Данных (ПАО «Ростелеком»)
- средств антивирусной защиты;
- организационных мер.

2. Основные функции ответственного

2.1. Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения защиты сведений конфиденциального характера при проведении работ на автоматизированных рабочих местах (далее - АРМ), входящих в состав ИС.

2.2. Проведение инструктажа пользователей АРМ (доведение под роспись требований инструкции «По работе пользователей информационной системы».

2.3. Контроль за соответствием состава ИС техническому паспорту (в т.ч. реальной конфигурации информационных связей).

2.4. Контроль работы СЗИ и за выполнением комплекса организационных мероприятий по обеспечению безопасности информации.

2.5. Контроль над действиями администратора ИС по обеспечению функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам ИС, антивирусная защита, резервное копирование данных и т.д.)

2.6. Настройка и сопровождение работоспособности Единой Сети Передачи Данных (далее ЕСПД) на АРМ.

2.7. **Контроль порядка учета, хранения и обращения с машинными носителями информации.**

2.8. Определение порядка и осуществление контроля ремонта АРМ. При проведении технического обслуживания и ремонта средств вычислительной техники запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения конфиденциальной информации.

2.9. Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИС.

2.10. Принятие мер по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к АРМ ИС.

2.11. Незамедлительное информирование руководителя учреждения об имеющихся недостатках и выявленных нарушениях СЗИ, а также в случае выявления попыток НСД к охраняемым сведениям или попыток их хищения, копирования или изменения.

3. Контролируемые параметры при проверке СЗИ ИС

3.1. Наличие лицензионного программного обеспечения (операционная система, антивирусная программа и офисный пакет) на АРМ ИС.

3.2. Соблюдение следующих требований к личным паролям доступа пользователей к АРМ (выбираются администратором ИС):

- длина пароля должна быть не менее 6-ти буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АС, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, злоумышленником путем анализа информации о пользователе АРМ;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;
- не использовать ранее использованные пароли.

3.3. Наличие на компьютере у пользователя прав не выше «пользователь» во избежание несанкционированной установки программного обеспечения (далее - ПО).

3.4. Отсутствие на компьютере лишних учетных записей пользователей компьютера, кроме записей «Администратор», «Пользователь» (встроенная учетная запись «Гость» должна быть отключена).

3.5. Наличие пароля на вход в BIOS материнской платы компьютера с целью невозможности изменения настроек.

3.6. Наличие периодического обновления вирусной базы антивирусного ПО.

3.7. Наличие бесперебойного источника питания для штатного завершения процесса обработки информации на компьютере в случае отключения электропитания.

3.8. Отсутствие со стороны пользователя АРМ следующих нарушений:

- записи паролей в очевидных местах, внутренности ящика стола, на мониторе компьютера, на обратной стороне клавиатуры и т.д.;
- хранения паролей в записанном виде на отдельных листах бумаги;
- сообщения посторонним лицам своих паролей, а также сведений о применяемой системе защиты ИС от НСД.

С инструкцией ознакомлен: