МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОЮЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА- ДЕТСКИЙ САД №37»
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОДСКОЙ ОКРУГ СИМФЕРОПОЛЬ
РЕСПУБЛИКА КРЫМ

СОГЛАСОВАНО
на заседании профсоюзного комитета
Председатель ПК
В.С. Штылова

УТВЕРЖДАЮ
Директор школы №37

ИНСТРУКЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

г.Симферополь
2021г.

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая инструкция определяет основные обязанности и ответственность пользователя, допущенного к обработке конфиденциальной информации.

1.2. Пользователь при выполнении работ в пределах своих функциональных обязанностей , обеспечивает безопасность конфиденциальной информации и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. ТРЕБОВАНИЯ К СОТРУДНИКАМ С ДОСТУПОМ К КОНФИДЕНЦИАЛЬНЫМ ДАННЫМ

Сотрудники, имеющие доступ к сведениям, представляющим коммерческую, государственную, иную тайну, должны соблюдать правила информационной безопасности.

- соблюдать правила, исключающие утечку сведений при работе с руководящими документами;
- устанавливать пароль для доступа к данным на персональном компьтере, электронных носителях;
- принимать необходимые меры защиты от вредоносных программ;
- соблюдать алгоритм действий при возникновении внештатных ситуаций;

3.ТРЕБОВАНИЯ К АДМИНИСТРАТОРУ, ОТВЕЧАЮЩЕМУ ЗА ЗАЩИТУ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Должностные лица, ответственные за проведение работ по технической защите информации локальных сетевых ресурсов, в процессе эксплуатации и модернизации, руководствуются:

- положениями федеральных законов;
- нормативными актами Российской Федерации;
- распорядительными документами Гостехкомиссии России (ФСТЭК), ФАПСИ, (ФСО, ФСБ), Гостандарта России;
- локальными правовыми актами внутреннего пользования;

Администратора под роспись знакомят с установленными правилами и обязанностями, Он может отключать доступ к сети пользователей, нарушающих требования по безопасной информации, запрещать установку нештатного программного обеспечения.

Основные обязанности администратора фиксируют документально. Они включают:

- участие в испытаниях и контроле уровня защищенности локальной сети;
- анализ данных, вносимых в журнал учета работы ЛВС для своевременного выявления нарушений требований защиты и оценки возможных последствий;- обеспечение доступа к информационной системе пользователям при наличии разрешения;

- блокировку попыток внесения изменений в программно-аппаратное обеспечение без согласования;
- немедленное оповещение службы безопасности о попытках несакционированного доступа, нарушения защиты.

Администратору строго запрещено передавать третьим лицам пароли, данные пользователей, идентификаторы, ключи на твердых носителях.

4. ЗАЩИТА ИНФОРМАЦИИ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ.

Рекомендации о методах выявления и борьбы с вирусами носят общий характер для пользователей персональными компьютерами и администраторов, ответственных за защиту информационных ресурсов.

Выделяют характерные проявления вирусных программ, нарушающих работу компьютера, способных разрушить хранящиеся в электронной форме сведения, передаваться по локальной сетевой связи. Создание перечня профилактических работ позволяет снизить риски, исключить появление и распространение вредоносных программ.

В документ включают:

- ежедневную автоматическую проверку персональных компьютеров перед началом работы и регулярную комплексную проверку со стороны администратора;
- резервирование программного обеспечения;
- защиту данных путем настройки прав доступа, допускающих лишь чтение, что предотвратит внесение посторонних записей, проникновение вирусов.

Анализируя результаты проверок на наличие вирусов, администратор делает выводы о необходимости служебного расследования. Вирусы уничтожают стиранием поврежденных файлов и с помощью специальных программ.

5.ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ ПАРОЛЬНОЙ ЗАЩИТНОЙ ИНФОРМАЦИИ.

Пользователи должны быть под роспись проинструктированы:
- о порядке генерации, смены и прекращения действия паролей, учетных записей;
- о правилах ввода пароля для получения доступа в локальную информационную систему.

Сотрудники отдела информационных технологий контролируют действия исполнителей и обслуживающего персонала.

Особые требования устанавливают для хранения паролей на бумажных носителях- в сейфе у ответственных за безопасность лиц в опечатанном конверте.

Также регламентируется порядок получения доступа к средствам вычислительной техники в случае производственной необходимости во время отсутствия штатного сотрудника, являющегося владельцем персонального компьютера.
Выбираемые парольные фразы должны соответствовать требованиям, указанным в документе.
Поскольку эта информация носит конфиденциальный характер, ответственность за разглашение, передачу сведений, лежит на владельце пароля.

6. ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ.

В целях обеспечения защиты секретных данных, снижения рисков утечки, уничтожения или заражения сетевых ресурсов вирусами, устанавливают перечень оснований, позволяющих блокировать исходящую и входящую в электронную почту.
Отдельно акцентируется внимание на запрете:
- использование корпоративного адреса электронной почты в личных целях;
- пользование бесплатными почтовыми сервисами для корпоративной переписки;
- публикации корпоративного адреса электронной почты на общедоступных интернет- ресурсах.

7. ПРАВИЛА БЕЗОПАСНОЙ РАБОТТЫ В ИНФОРМАЦИОННОЙ СЕТИ.

Документально фиксируют регламент, режимы работы компьютерного оборудования, к которому относят не только персональные компьютеры, но и принтеры, серверы, сетевые коммутаторы.
К мерам обеспечения безопасности относят:
- использование сертифицированного оборудования, соответствующего требования санитарно-эпидемиологических нормативов, ГОСТов (допустимый уровень шума, электромагнитная совместимость, устойчивость к электромагнитным помехам);
- правильную подготовку оборудования к включению и эксплуатации;
- соблюдение запретов, касающихся переключения разъемов кабелей, самостоятельного ремонта устройств, удаления с корпуса заводских и линейных номеров;
- использование при печати на лазерном принтере специальной бумаги рекомендованной плотности;
- недопустимость применения физических усилий для вытягивания бумаги во время печати из выходного отверстия принтера, что может привести к повреждению механизма печати;
- корректное выключение компьютера после закрытия работающих программ, используя в меню «Пуск» команду «Завершение работы»;
- порядок подачи доступа к информационной сети организации

Работники, ознакомленные с основными требованиями информационной безопасности, в том числе, касающимися выполнения профессиональных (должностных) обязанностей, несут ответственность за нарушения установленных правил в рамках трудового, в отдельных ситуациях уголовного законодательства.

Инструкцию разработал
специалист по охране труда Каценко Н.Г.