Памятка-инструкция по информационной безопасности для пользователя муниципального учреждения дополнительного образования «Дом детского творчества» г. Благодарный

Общие положения

Настоящая памятка устанавливает обязательные правила работы с информацией и информационными системами для всех сотрудников организации. Цель — защитить персональные данные обучающихся и работников, служебную информацию, а также обеспечить бесперебойную работу ИТ-инфраструктуры.

1. Аутентификация и управление учётными данными

Требования к паролю:

- ✓ длина — не менее 12 символов;
- ✓ должны присутствовать буквы верхнего и нижнего регистра, цифры и специальные символы (например, !, @, #);
- ✓ не используйте в пароле личные данные (даты рождения, имена, названия организации), а также очевидные последовательности (123456, qwerty).

Правила обращения с учётными данными:

- ✓ не передавайте логин и пароль никому, в том числе коллегам, даже «на пять минут»;
- ✓ не фиксируйте пароли в открытом виде: не пишите на бумажках у монитора, не храните в незащищённых текстовых файлах, не отправляйте в мессенджерах и соцсетях;
- ✓ при необходимости передать доступ используйте только утверждённые в организации механизмы (например, делегирование прав администратором).

2. Защита рабочего места

Автоматическая блокировка экрана:

- ✓ экран должен блокироваться автоматически при бездействии не позднее чем через 5 минут;
- ✓ если вы отходите от рабочего места даже на короткое время — вручную заблокируйте экран (в Windows: Win + L; в macOS: Control + Command + Q или через меню пользователя).

Блокировка при ошибках входа:

- ✓ после 5 неудачных попыток ввода пароля учётная запись будет заблокирована — не пытайтесь подбирать пароль многократно. При проблемах обратитесь к ответственному за ИТ-сопровождение или директору.

3. Программное обеспечение и защита от вредоносного ПО

Установка ПО:

- ✓ не устанавливайте программы из непроверенных источников (с неизвестных сайтов, через ссылки в письмах, с чужих флешек);
- ✓ любое ПО устанавливается только с согласования ответственного лица за ИТ-сопровождение или директора.

Антивирусная защита:

- ✓ антивирус должен работать постоянно в режиме реального времени;
- ✓ запрещено отключать антивирус или его отдельные компоненты;
- ✓ обновления баз сигнатур происходят автоматически — не отменяйте и не откладывайте их.

4. Безопасное использование каналов связи и удалённого доступа

Электронная почта и мессенджеры:

- ✓ не пересылайте в мессенджерах, соцсетях и по почте конфиденциальные данные (персональные данные, сканы документов, пароли, ключи доступа);
- ✓ будьте внимательны к вложениям и ссылкам в письмах: не открывайте файлы от неизвестных отправителей, не переходите по подозрительным ссылкам.

Удалённый доступ:

- ✓ использование средств удалённого доступа допускается только в соответствии с утверждёнными правилами организации;
- ✓ не передавайте данные аутентификации (логины, пароли, одноразовые коды) через мессенджеры, почту или по телефону;
- ✓ при работе из дома соблюдайте те же правила безопасности, что и на рабочем месте.

5. Действия при инцидентах информационной безопасности

Если вы заметили что-либо из перечисленного ниже — немедленно сообщите ответственному за информационное и техническое сопровождение (контакты указаны в конце памятки):

- ✓ компьютер работает необычно медленно, появляются странные окна, всплывающие сообщения, самопроизвольно открываются программы;
- ✓ вы получили письмо с подозрительной ссылкой или вложением, особенно если оно запрашивает ввод пароля или личных данных;

- ✓ кто-то запрашивает у вас логин, пароль, коды подтверждения;
- ✓ вы случайно ввели пароль на подозрительном сайте или перешли по фишинговой ссылке;
- ✓ обнаружены признаки несанкционированного доступа или утечки данных (например, в системе видны действия, которые вы не совершали).

Что сделать сразу:

1. Прекратите любые действия, требующие ввода паролей или передачи данных.
2. Не пытайтесь «исправить» проблему самостоятельно (не удаляйте файлы, не отключайте антивирус).
3. Сообщите ответственному лицу, кратко описав: что произошло, когда, какие действия вы успели выполнить, какие файлы/ссылки открывали.

6. Работа с носителями информации и физическими устройствами

- ✓ Не используйте чужие флешки, карты памяти и другие съёмные носители без согласования с ответственным за ИТ-сопровождение или директора.
- ✓ Если необходимо перенести данные — используйте только утверждённые способы (корпоративное облачное хранилище, защищённые сетевые папки, официально одобренные носители).
- ✓ Не оставляйте ноутбуки, планшеты и телефоны без присмотра в общественных местах.
- ✓ При утере устройства немедленно сообщите ответственному лицу — это критично для предотвращения утечки данных.

7. Работа с конфиденциальной информацией и персональными данными

- ✓ Обрабатывайте персональные данные только в рамках своих должностных обязанностей и в соответствии с локальными актами организации.
- ✓ Не публикуйте в открытых источниках (соцсети, форумы, чаты) информацию об организации, сотрудниках, обучающихся, внутренних процессах.
- ✓ Файлы с персональными данными храните в утверждённых защищённых папках; не размещайте их на личных облачных дисках (Google Drive, Яндекс Диск и т.п.) без согласования.

Контакты для экстренных обращений

Ответственный за информационное и техническое сопровождение:

Малиновский В.Э., старший педагог МУ ДО «ДДТ»

Ответственность и контроль

- ✓ Соблюдение требований информационной безопасности — обязанность каждого сотрудника.
- ✓ Нарушение правил может повлечь дисциплинарные меры и создать риски для всей организации.
- ✓ Регулярно проводятся проверки соблюдения требований и внеплановые инструктажи — будьте готовы к участию в них.