Муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад № 9 г. Челябинска»
(МБДОУ «ДС № 9 г. Челябинска»)

454128, г. Челябинск, ул.250-летия Челябинска, д.14/а, тел. 796-92-36, detstvo_09@mail.ru
ИНН 7447033150, КПП 744701001, ОКПО 42480155, ОКАТО 75401364000, ОГРН 1037402322693, БИК 047501001, Р-с № 40701810400003000001, Банк ГРКЦ ГУ Банка России по Челябинской обл. г. Челябинска

ПРИКАЗ

«20» декабря 2023 г. № 70

О назначении ответственного лица за обеспечение информационной безопасности при работе с конфиденциальными сведениями в МБДОУ «ДС № 9 г. Челябинска» в 2023 /2024 учебном году

В соответствии с письмами Администрации города Челябинска от 13.12.2023 № 01-1106 и Комитета по делам образования города Челябинска от 19.12.2023 № 08/10474 в целях создания безопасной информационно-образовательной среды, повышения уровня информационной безопасности в части информирования воспитанников, их родителей (законных представителей) и педагогических работников,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за информационную безопасность в МБДОУ «ДС № 9 г. Челябинска» заместителя заведующего по УМР Панфиленко Е.Н.
2. Заместителю заведующего по УМР Панфиленко Е.Н. ознакомить всех работников МБДОУ «ДС № 9 г. Челябинска» с памяткой по информационной безопасности при работе с конфиденциальными сведениями под роспись (приложение 1).
3. Ведущему специалисту по кадрам Берсеневой М.А. хранить памятку в личном деле каждого работника.
3. Заместителю заведующего по УМР Панфиленко Е.Н. разработать памятку пользователя по информационной безопасности.
4. Заведующему Сырниковой И.М. утвердить и внести в действие памятку пользователя по информационной безопасности (приложение 2).
5. Разместить настоящий приказ и памятку пользователя по информационной безопасности на официальном сайте учреждения в течение 10 рабочих дней со дня издания настоящего приказа.
5. Контроль за исполнением приказа оставляю за собой.

Заведующий Сырникова Ирина Михайловна

Подписан цифровой подписью: Сырникова Ирина Михайловна
DN: C=RU, OU=Заведующий, O="МБДОУ ""ДС № 9 г. Челябинска""", CN=Сырникова Ирина Михайловна, E=detstvo_09@mail.ru
Основание: Я являюсь автором этого документа
Расположение:
Дата: 2023.12.26 15:47:41+05'00'
Foxit PDF Reader Версия: 12.1.0

И.М. Сырникова

С приказом ознакомлен:

Приложение № 1
к приказу № 70
от « 20» декабря 2023 г.

Памятка по информационной безопасности
при работе с конфиденциальными сведениями

1) Информация ограниченного доступа (в том числе с ограничительной пометкой «Для служебного пользования»), не содержащая сведений, составляющих государственную тайну, должна обрабатываться в электронном виде только на рабочих местах, аттестованных по требованиям безопасности информации, предъявляемым ФСТЭК России к таким автоматизированным рабочим местам.

2) Информация, содержащая сведения составляющие государственную тайну, должна обрабатываться в электронном виде только на рабочих местах, аттестованных по требованиям безопасности информации, предъявляемым ФСТЭК России и ФСБ России к таким автоматизированным рабочим местам.

3) Провести детальный анализ адресов электронной почты, созданных на сторонних почтовых сервисах (mail.ru, yandex.ru, rambler.ru, google.com и др.) в подконтрольных Вам структурных подразделениях на предмет их использования в служебных целях.

4) Запретить использование личных адресов электронной почты в рабочих целях.

5) Провести дополнительные настройки корпоративной электронной почты и почтовых серверов, при наличии, для обеспечения ее безопасности: включение двухфакторной аутентификации с использованием доверенного номера телефона, установка контрольных вопросов, включение уведомлений о новых устройствах, с которых выполнен вход в электронную почту.

6) Актуализировать необходимое количество сотрудников, которым необходим доступ к групповым адресам электронной почты Управлений, Комитетов или отделов. Определить список работников, имеющих доступ к электронной почте, и строго соблюдать конфиденциальность обрабатываемой информации, а также актуальность списка работников. Особое внимание уделить смене парольных комбинаций при проведении организационно-штатных мероприятий (увольнения, переводы и др.)

7) Обеспечить смену пароля на используемых адресах электронной почты не реже, чем раз в три месяца. Пароль должен отвечать требованиям по информационной безопасности и быть устойчивым к взлому (длина пароля не менее 8 символов, пароль должен содержать прописные и строчные буквы, цифры (не менее двух) и специальные символы !@#$%^&*() (например: 29Akf<ezPfg, Qu88nC@rd13). Не использовать одинаковые пароли к разным информационным ресурсам.

8) Запрещено сохранять пароли в браузере, а также хранить их в рукописном виде в легкодоступных местах (стикеры на рабочих столах). Рекомендуемые способы хранения паролей – менеджеры паролей, запись в личном блокноте, исключающая ознакомление других лиц.

9) На рабочих местах должно быть установлено средство антивирусной защиты. При уходе работника из кабинета, необходимо блокировать паролем рабочее место.

10) Исключить переписку по электронной почте и интернет-мессенджерам по тематикам оперативного штаба по обеспечению кибербезопасности, Антитеррористической комиссии Челябинской области и оборонными предприятиями, а также с иными владельцами чувствительной информации, утечка которой может нанести ущерб безопасности.

11) Необходимо назначить работника, ответственного за обеспечение информационной безопасности. В его должностные обязанности должно входить информирование коллег об угрозах информационной безопасности, проведение инструктажей по вопросам обеспечения информационной безопасности, а также проводить аудит информационной сети организации на предмет реализации угроз.

Приложение № 2
к приказу № 70
от « 20» декабря 2023 г.

Памятка пользователю по информационной безопасности

Парольная защита

• Никогда не сохраняйте ваши пароли в программах. Большинство программ хранят их в открытом виде и тот, кто получит доступ к вашему компьютеру, получит доступ и к ним.

• Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам, и не храните записанный пароль в общедоступных местах.

• В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых отделом по защите информации, работ, проводимых отделом информационных технологий и требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальникам этих подразделений. По окончанию производственных, или проверочных работ работники самостоятельно производят немедленную смену значений "раскрытых" паролей.

• Не используйте пароль доступа в локальную сеть ФИЦ КНЦ в других программах и на сайтах, где требуется регистрация.

Антивирусная защита

• Никогда не отключайте установленное на АРМ антивирусное программное обеспечение.

• Обязательно проверяйте на наличие вирусов все внешние носители информации (дискеты, диски, флешки и т.п.), поступающие со стороны (из внешних организаций, других подразделений Организации и т.п.)

• Во всех случаях возможного проявления действия вирусов или подозрении на наличие вируса не пытайтесь удалить вирус самостоятельно, незамедлительно сообщите об этом сотруднику техподдержки.

Интернет и электронная почта

• Содержание Интернет-ресурсов, а также файлы, загружаемые из Интернета, обязательно проверяйте на отсутствие вредоносных программ и вирусов.

• Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя.

• Не передавать по электронной почте Ваши пароли.

• Не принимайте никаких соглашений при посещении сайтов, смысла которых Вы не понимаете.

Прочее

• Не устанавливайте самостоятельно программное обеспечение, если это не входит в Ваши обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению Ваших должностных обязанностей программное обеспечение.

• Располагайте мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ к отображаемой и печатаемой информации.

• При временном оставлении рабочего места в течение рабочего дня в обязательным порядке блокируйте компьютер нажатием комбинации клавиш «Win + L».

Приложение № 3
к приказу № 70
от « 20» декабря 2023 г.

Памятка по информационной безопасности при работе с конфиденциальными сведениями

1) Информация ограниченного доступа (в том числе с ограничительной пометкой «Для служебного пользования»), не содержащая сведений, составляющих государственную тайну, должна обрабатываться в электронном виде только на рабочих местах, аттестованных по требованиям безопасности информации, предъявляемым ФСТЭК России к таким автоматизированным рабочим местам.

2) Информация, содержащая сведения составляющие государственную тайну, должна обрабатываться в электронном виде только на рабочих местах, аттестованных по требованиям безопасности информации, предъявляемым ФСТЭК России и ФСБ России к таким автоматизированным рабочим местам.

3) Провести детальный анализ адресов электронной почты, созданных на сторонних почтовых сервисах (mail.ru, yandex.ru, rambler.ru, google.com и др.) в подконтрольных Вам структурных подразделениях на предмет их использования в служебных целях.

4) Запретить использование личных адресов электронной почты в рабочих целях.

5) Провести дополнительные настройки корпоративной электронной почты и почтовых серверов, при наличии, для обеспечения ее безопасности: включение двухфакторной аутентификации с использованием доверенного номера телефона, установка контрольных вопросов, включение уведомлений о новых устройствах, с которых выполнен вход в электронную почту.

6) Актуализировать необходимое количество сотрудников, которым необходим доступ к групповым адресам электронной почты Управлений, Комитетов или отделов. Определить список работников, имеющих доступ к электронной почте, и строго соблюдать конфиденциальность обрабатываемой информации, а также актуальность списка работников. Особое внимание уделить смене парольных комбинаций при проведении организационно-штатных мероприятий (увольнения, переводы и др.)

7) Обеспечить смену пароля на используемых адресах электронной почты не реже, чем раз в три месяца. Пароль должен отвечать требованиям по информационной безопасности и быть устойчивым к взлому (длина пароля не менее 8 символов, пароль должен содержать прописные и строчные буквы, цифры (не менее двух) и специальные символы !@#$%^&*() (например: 29Akf<ezPfg, Qu88nC@rd13). Не использовать одинаковые пароли к разным информационным ресурсам.

8) Запрещено сохранять пароли в браузере, а также хранить их в рукописном виде в легкодоступных местах (стикеры на рабочих столах). Рекомендуемые способы хранения паролей – менеджеры паролей, запись в личном блокноте, исключающая ознакомление других лиц.

9) На рабочих местах должно быть установлено средство антивирусной защиты. При уходе работника из кабинета, необходимо блокировать паролем рабочее место.

10) Исключить переписку по электронной почте и интернет-мессенджерам по тематикам оперативного штаба по обеспечению кибербезопасности, Антитеррористической комиссии Челябинской области и оборонными предприятиями, а также с иными владельцами чувствительной информации, утечка которой может нанести ущерб безопасности.

11) Необходимо назначить работника, ответственного за обеспечение информационной безопасности. В его должностные обязанности должно входить информирование коллег об угрозах информационной безопасности, проведение инструктажей по вопросам обеспечения информационной безопасности, а также проводить аудит информационной сети организации на предмет реализации угроз.