КОМИТЕТ ПО ДЕЛАМ ОБРАЗОВАНИЯ Г. ЧЕЛЯБИНСКА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«Средняя общеобразовательная школа № 91 г. Челябинска»
ОГРН 1027402825251 ИНН 7450011478 КПП 746001001
454047 г. Челябинск, ул. Жукова, 16; тел./факс: (351)721-14-57, тел.: (351)721-14-58; e-mail: shkola--91@mail.ru

ПРИКАЗ

«04» 04 2022 г. № 150

О мерах по обеспечению
защиты информации

На основании Письма Комитета по делам образования г. Челябинска № 16-05/2349 от 01.04.2022 г., в соответствии с Решением оперативного штаба по обеспечению кибербезопасности Челябинской области от 14.03.2022 г., рекомендациями Управления ФСТЭК России и Национального координационного центра по компьютерным инцидентам, для обеспечения защиты информации в образовательной организации,

ПРИКАЗЫВАЮ

1. Зам. директора по безопасности Кравченко О.В. ознакомить работников ОО с правилами защиты информации, содержащимися в приложениях №№ 1, 2, 3 к данному приказу.
2. Зам. директора по УВР Ерёменко Л.А. разместить настоящий приказ, включая приложения, на официальном сайте ОО.
3. Контроль исполнения настоящего приказа оставляю за собой.

Приложения:

1. Памятка по защите информации.
2. Рекомендации ФСТЭК России по повышению защищённости.
3. Памятка по безопасной работе с электронной почтой.

Директор МАОУ «СОШ № 91 г. Челябинска» Л.А. Иванова

Приложение № 1 к письму
Комитета по делам образования
города Челябинска
от _____№_____

Памятка по обеспечению защиты информации

1) На автоматизированном рабочем месте (далее — АРМ) следует выполнять только те задачи, которые определены должностной инструкцией работника.

2) Не рекомендуется оставлять АРМ включенным или разблокированным при необходимости покинуть рабочее место. Для блокирования компьютера можно воспользоваться сочетанием клавиш «Win + L» или выбрать соответствующий пункт в меню выключения компьютера. После окончания рабочего дня АРМ необходимо выключать стандартным способом.

3) Не рекомендуется сообщать кому-либо личную аутентификационную информацию (пары логин-пароль и другие данные). Также не следует хранить пароли и логины в общедоступных местах под клавиатурой, на мониторе и т. п. Для хранения парольной информации можно использовать специальные менеджеры хранения паролей.

4) Необходимо внепланово сменить пароли, если с последней смены пароля прошло больше 4х месяцев.

5) Рекомендуемый пароль должен отвечать следующим требованиям:

- длина пароля не менее 8 символов;
- пароль должен содержать прописные и строчные буквы, цифры и символы. Также по рекомендации ФСТЭК, в пароле должно быть не менее двух цифр.
- пароль не должен включать в себя легко вычисляемые сочетания (qwerty, abcd, 1234 и др.). Пароль не должен содержать в себе личную информацию о работнике (телефон, ФИО, номер автомобиля и др.), так как эту информацию можно узнать, основываясь на информации о пользователе.

6) Не рекомендуется использовать один и тот же пароль для доступа к различным ресурсам.

7) Не рекомендуется использовать функцию автосохранения паролей в браузерах. Уже имеющиеся пароли должны быть удалены.

8) Не рекомендуется самостоятельно устанавливать программное обеспечение на АРМ, отключать или блокировать работу средств защиты информации.

9) Не рекомендуется использовать внешние носители на рабочих местах, не предназначенных для выполнения трудовых обязанностей. Рекомендуется на аппаратном уровне запретить использование USB-портов кроме необходимых.

10) При получении каких-либо писем по электронной почте, необходимо обращать внимание на вложения и не скачивать их, если возникают сомнения. Вложения в форматах: exe, apk, bat, cmd, com, dll, jar, lib, msc, msi, sys запрещены для скачивания самостоятельно. Также если файл не открывается для просмотра в интерфейсе почты, содержание письма вызывает вопросы или Вы не ждали подобное письмо то необходимо переслать подозрительное письмо как вложение в Управление информатизации и цифровой инфраструктуры на адрес электронной почты: it@cheladmin.ru.

Приложение № 2
к письму Комитета по делам
образования города Челябинска
от _____№_____

Рекомендации ФСТЭК России по повышению защищенности

1. В целях предотвращения реализации угроз безопасности информации, направленных на утрату доступа к информации, необходимо принять следующие дополнительные меры по защите информации:

1.1. обеспечить создание резервных копий защищаемой информации, обрабатываемой в системе управления базами данных MongoDB;

1.2. запретить возможность обработки и хранения защищаемой информации в облачных сервисах MongoDB Atlas;

1.3. отключить возможность автоматического обновления программного обеспечения компании Microsoft.

2. В целях предотвращения заражения вредоносным программным обеспечением не открывать письма с электронного адреса noreply@mvd.msk.ru, в виду того что с данного электронного адреса направляются письма с вредоносным вложением «Федеральный антивирус Аврора.exe».

3. В свободно распространяемые библиотеки программного обеспечения с использованием репозитория программных модулей npm (в частности, Vue.js) встраивается вредоносный код при загрузке/обновлении с российских ip-адресов. В качестве компенсирующих мер при организации разработки программного обеспечения с использование npm-модулей может быть создан собственный npm-сервер, содержащий доверенные версии библиотек.

4. В целях предотвращения реализации угроз, направленных на эксплуатацию уязвимостей в иностранном и открытом программном обеспечении, а также модулях, плагинах и библиотеках, необходимо принять следующие дополнительные меры по защите информации:

4.1. перед установкой программного обеспечения рекомендуется проверять его на предмет наличия вредоносного программного обеспечения;

4.2. перед установкой программного обеспечения рекомендуется проверять корректность его работы на макете или тестовом стенде (при наличии);

4.3. при проверке библиотек рекомендуется обращать внимание на последние внесенные изменения, в частности, участки кода, влияющие на выполнение программы в зависимости от установленного часового пояса, например:

```
"country" : {
   "code": "RU"
   "name": "Russia",
"ip": " ".
```

5. Доступ нарушителей к объектам информационной инфраструктуры осуществляется через систему удаленного доступа к рабочему столу средств вычислительной техники, в частности незащищенный VNC-сервер. Для поиска

систем удаленного доступа нарушители используют системы поиска Интернет-ресурсов shodan.io.

В целях предотвращения возможности использования систем удаленного доступа для реализации угроз безопасности информации необходимо ограничить доступ к системам удаленного доступа из сети Интернет. В случае невозможности ограничения удаленного доступа из сети Интернет необходимо осуществлять такой доступ с использованием VPN-сетей.

6. Выявлены факты внедрения вредоностного программного обеспечения в свободно распространяемой программное обеспечение (например, в пакетах node-ipc, WordPress, плагин Mistape, Filestash и другие пакеты). Учитывая вышеизложенное, необходимо принять следующие дополнительные меры по защите информации:

6.1. при установке обновлений открытого программного обеспечения проверить их на предмет наличия вредоносного программного обеспечения;

6.2. при проверке обновлений открытого программного обеспечения рекомендуется обращать внимание на последние внесенные изменения, в частности, участки кода, влияющие на выполнение программы в зависимости от установленного часового пояса;

6.3. рекомендуется устанавливать обновления программного обеспечения только после их тестирования на макете или тестовом стенде (при его наличии).

7. В целях недопущения функционирования веб-сайтов (порталов), а также компрометации размещаемой на них информации рекомендуется принять следующие дополнительные меры по защите информации:

7.1. обеспечить размещение информационной инфраструктуры, на которой функционируют веб-сайт (порталы), на территории Российской Федерации;

7.2. для корректной работы веб-сайтов (порталов) обеспечить использование DNS-серверов, размещенных на территории Российской Федерации. Также убедиться в отсутствии в цепочке серверов различных иностранных серверов, например DNS forwarding 8.8.8.8.

7.3. обеспечить применение отечественного регистратора, который управляет доменными именами веб-сайтов (порталов);

7.4. в случае использования для публичных ресурсов основных доменных зон .com, .org и т.п., необходимо перейти на использование доменной зоны .ru;

7.5. провести инвентаризацию информационных ресурсов на предмет использования иностранного программного обеспечения, включая облачные решения, мессенджеры, системы управления, средства коллективной работы, офисное программное обеспечение, интегрированную среду разработки. В случае наличия таких решений разрабатывать план по переходу на отечественные аналоги;

7.6. обеспечить создание локальных хранилищ дистрибутивов программного обеспечения и используемого программного обеспечения с открытым исходным кодом.

Приложение № 3 к письму
Комитета по делам образования
города Челябинска
от _____№_____

Памятка по безопасной работе с электронной почтой

1. Необходимо внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом.
2. Обращайте внимание на домен в адресе отправителя, если он не принадлежит организации, от имени которой написано письмо, а тем более если ящик зарегистрирован на бесплатных почтовых сервисах, то это верный признак мошеннического письма. Официальные рассылки всегда приходят с официальных адресов.
3. Следует с осторожностью относиться к письмам от неизвестных адресатов, ни в коем случае не открывать вложения и не переходить по ссылкам.
4. Следует проверять ссылки, даже если письмо получено от коллеги. Нужно помнить, что коллегу или знакомого могли взломать.
5. Признаки фишинговых ссылок, которые могут быть отправлены в почте:
   - посторонние домены, не относящиеся к организациям;
   - при наведении курсора мышки на ссылку всплывающий адрес не совпадает с написанным;
   - ошибки в написании;
   - автоматически сгенерированные последовательности символов в адресе ссылки;
   - символы из других языков, похожие на базовую латиницу — ç вместо c, á вместо a и так далее;
   - даже если ссылка содержит в себе «https:/», это не дает гарантии в ее безопасности.
6. Рекомендуем с подозрением относиться к письмам с вложениями, особенно если это документы с макросами, архивы с паролями, а также файлы с несвойственными расширениями, например текстовый файл с расширением .exe.
7. Рекомендуем с подозрением относиться к письмам с призывом к действиям (например «открой», «прочитай», «ознакомься»), а также к письмам, в темах которых упоминаются финансы, банки, геополитическая обстановка или содержатся угрозы.
8. Необходимо с подозрением относиться к письмам со ссылками, особенно если они длинные или, наоборот, созданы с помощью сервисов сокращения ссылок (например, bit.ly, tinyurl.com). Не переходить по ссылкам из письма, если они заменены на слова, наводить на них мышкой и просматривать полный адрес.
9. Следует с подозрением относиться к письмам на иностранном языке, особенно с орфографическими ошибками и с большим количеством получателей.
10. При получении писем, не соответствующих критериям безопасности, рекомендуем направлять их в папку «спам» и сообщать специалистам, ответственным за информационную безопасность.