АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА САМАРА
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ

Льва Толстого ул., 26, г. Самара, Россия, 443010
Тел.:(846) 332 32 50; факс: (846) 333 58 02; e-mail: dosamadm@yandex.ru

от 12 МАР 2020 г. № 12-01-02/443
на № _____

Руководителям
образовательных
учреждений городского
округа Самара

Уважаемые руководители!

В целях повышения осведомленности об угрозах, исходящих от вредоносного программного обеспечения, а также в связи с участившимися инцидентами по заражению вредоносным программным обеспечением средств вычислительной техники, компьютерных атак на информационные системы и ресурсы направляем вам для использования в работе материалы Самарского Регионального Центра Кибербезопасности.

Кроме того, ответственным за обеспечение информационной безопасности в вашем образовательном учреждении необходимо провести профилактические мероприятия с пользователями, направленные на повышение осведомленности об угрозах вредоносного программного обеспечения, актуализировать и использовать антивирусное программное обеспечение, ограничить применение макросов в пакете программ Microsoft Office.

Приложение: на 7 л. в 1 экз.

И.о. заместителя
руководителя Департамента Н.С.Некрасова

А.А.Данилина
333 32 38

ПРИЛОЖЕНИЕ 1

Профилактические меры по недопущению заражения информационных систем

Компьютерные вирусы зачастую распространяются с использованием вложений в сообщения электронной почты или мгновенных сообщений. По этой причине не следует открывать вложения в сообщениях электронной почты, полученных из неизвестных источников. Вирусы могут быть замаскированы под изображения, поздравительные открытки, звуковые или видеофайлы.

Кроме того, компьютерные вирусы распространяются через файлы, загружаемые из сети Интернет. Они могут быть скрыты в пиратском программном обеспечении или в других файлах и программах, загружаемых пользователями.

Вирусы могут иметь разный функционал, некоторые из них интегрированы с другим программным обеспечением (далее – ПО) так, что «жертва» даже не замечает, что было выполнено что-то кроме основного функционала запускаемого файла. Такие вирусы могут сохранять Ваши сохраненные пароли, файлы cookie, историю браузера, файлы с компьютера и иную информацию.

Бывают вирусы, предоставляющие удаленный доступ злоумышленнику, либо скрытно использующие вычислительные мощности Вашего компьютера для майнинга криптовалюты.

В последние время широкое распространение получили вирусы-шифровальщики. Эти файлы после запуска получают от удаленного сервера ключ шифрования и начинают шифровать все файлы жесткого диска, затем появляется баннер, в котором злоумышленники просят перевести им деньги для получения ключа дешифрования. Стоит понимать, что после перевода денег нет никаких гарантий в получении ключа дешифрования, более того, существуют вирусы, не сохраняющие на своем сервере сгенерированные ключи. Таким образом восстановление данных становится физически

невозможным. Является это задумкой злоумышленников или ошибкой – сказать сложно. Таким образом, лучше не допускать заражение компьютера ни одним из видов вирусов.

Для уменьшения вероятности заражения компьютерными вирусами рабочих станций следует придерживаться простых правил:

На всех рабочих станциях должно быть установлено антивирусное ПО;

Необходимо регулярно обновлять базы данных антивирусного ПО;

Необходимо регулярно проводить полное сканирование рабочей станции средством антивирусной защиты;

Необходимо регулярно устанавливать обновления операционных систем;

Необходимо обновлять Web-браузер, так как вирусы эксплуатируют ошибки в работе браузера для внедрения вредоносного кода на компьютер «жертвы».

Запрещено скачивать ПО с неофициальных сайтов, с пометкой «реклама» или если адрес сайта явно не является официальным;

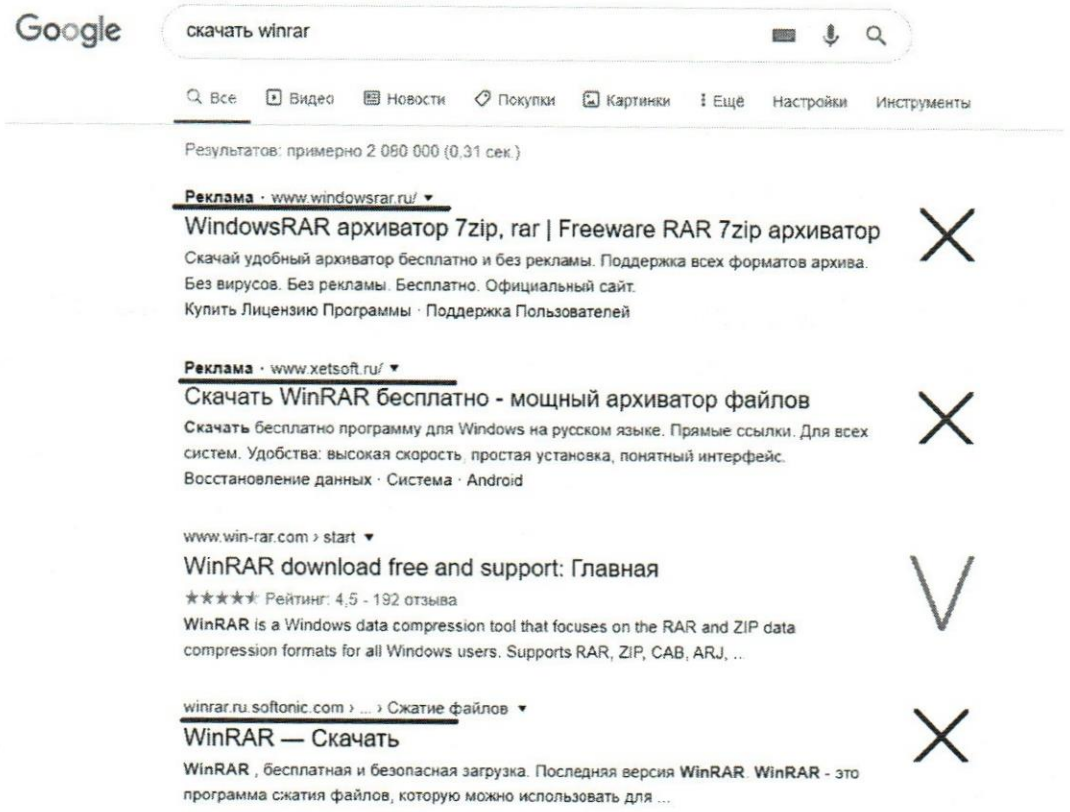

Рисунок 1. Примеры подозрительных сайтов

Запрещено на рабочих компьютерах использовать личные съемные носители (флешки, диски). Любые съемные носители должны быть просканированы средством антивирусной защиты. Для этого достаточно нажать на правку кнопку мыши, выбрав пункт «Проверить на вирусы»;

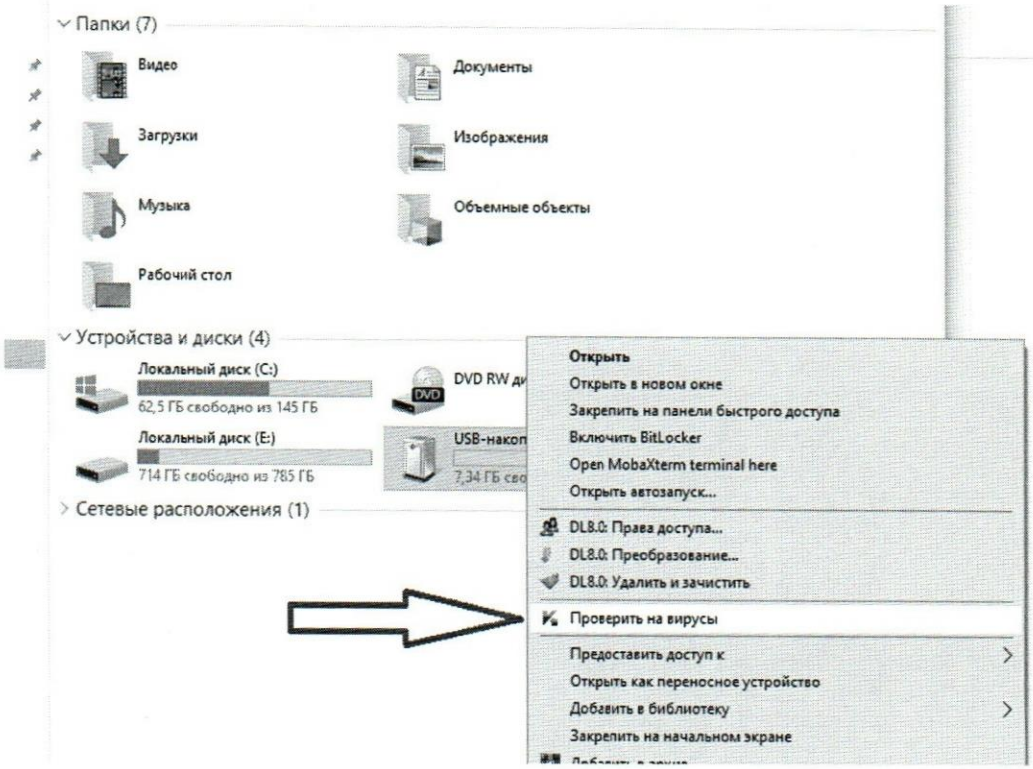

Рисунок 2. Проверка на вирусы съемных носителей

При подозрении ссылки на вредоносность рекомендуется по ней не переходить, однако, если это невозможно необходимо проверить ее с помощью онлайн-сервиса проверок, например, можно использовать https://virusdesk.kaspersky.ru/;

Необходимо внимательно смотреть на адреса сайтов и не вводить свои данные, если адрес страницы выглядит подозрителен. Примеры возможный фишинговых сайтов приведены в таблице 1.

Оригинальные сайты	Примеры вредоносных сайтов	Описание
rzd.ru	rzd.info	Замена домена «ru» на «info»
gosuslugi.ru	Gosus1ugi.ru	Заменена «l»(«L») на «1» (единица)
Yandex.ru	Yandeex.ru	Дублирована буква «е»
Samregion.ru	Sanregion.com	Замена домена «ru» на «com» Заменена буква «m» на «n»

Таблица 1 – Примеры фишинговых сайтов.

Запрещено открывать всплывающую рекламу поверх открытой Web-страницы, переходить по ссылкам в баннерах. При появлении рекламы, если Вы видите большую кнопку «Закрыть», нажав на нее, возможен запуск установки или загрузки вредоносного ПО на Вашу рабочую станцию;

При загрузке файлов необходимо обращать внимание на их расширения. Если при загрузке текстовых файлов, видеофайлов, картинок скачанный файл имеет расширение «.exe» - скорее всего это вирус;

При работе многие сайты выдают контекстную рекламу по краю от основного текста. Запрещается переходить по таким ссылкам. Пример рекламы приведен на рисунке 3;

Рисунок 3.Примеры контекстной рекламы

Бэкапы важных файлов, конфигураций оборудования или образов виртуальных машин необходимо регулярно обновлять, а также рекомендуется хранить их на отдельных серверах.

ПРИЛОЖЕНИЕ 2

Действия в случае заражения рабочих вычислительных средств вирусом-шифровальщиком

Действия администраторов.

Рекомендованные действия для технических специалистов, ответственных за информационную безопасность, в случае, если заражение уже произошло или есть опасения, что средства вычислительной техники (далее – СВТ) заразилось вирусом-шифровальщиком:

1. Обесточить СВТ, выдернув вилку из розетки или воспользовавшись кнопкой On/Off на блоке питания. Обратите внимание, что речь идет не о кнопке включения/выключения компьютера, расположенной на лицевой стороне системного блока, а именно о тумблере блока питания (расположен сзади).

2. Обеспечить отключение зараженного устройства от сети Интернет и других сетей.

В случае, если далее предполагается обращение в правоохранительные органы по факту заражения вредоносным программным обеспечением (далее – ПО), после выполнения вышеуказанных рекомендаций должно последовать непосредственное обращение. В дальнейшем с целью снятия криминалистической копии носителей информации и проведения криминалистических экспертиз может быть принято решение об изъятии зараженных технических средств. Если обращение в правоохранительные органы не планируется или в процессе расследования оборудование не было изъято рекомендуется выполнить следующие действия:

3. Произвести загрузку операционной системы с предварительно подготовленного, защищенного от записи, носителя или использовать специальные решения антивирусных компаний (Dr.Web LiveDisk, Kaspersky Rescue Disk и др.);

4. Сделать копию зараженной системы и в дальнейшим производить все указанные действия только с копией;

5. Провести проверку копии системы с помощью антивирусного ПО;

В случае подтверждения заражения системы вирусом-шифровальщиком:

6. Если на момент обесточивания зараженной системы процесс шифрования не был закончен, скопировать нетронутые пользовательские файлы для дальнейшего использования в рабочем процессе, предварительно проверив их с помощью антивирусного ПО;

7. При наличии действующей лицензии антивирусного ПО обратиться к производителю антивируса с просьбой оказания помощи в расшифровке зашифрованной информации;

8. В случае отсутствия действующей лицензии антивирусного ПО существует вероятность расшифровки зараженной системы с помощью сообщества экспертов по информационной безопасности и открытого программного обеспечения.

Техническим специалистам, ответственным за информационною безопасность, рекомендуется провести с пользователями СВТ инструктаж на случай заражения вирусом-шифровальщиком.

Действия пользователей

Рекомендованные действия для пользователей в случае, если заражение уже произошло или есть опасения, что СВТ заразился вирусом-шифровальщиком:

1. Обесточить СВТ, выдернув вилку из розетки или воспользовавшись кнопкой On/Off на блоке питания. Обратите внимание, что речь идет не о кнопке включения/выключения компьютера, расположенной на лицевой стороне системного блока, а именно о тумблере блока питания (расположен сзади).

2. Обратиться к техническим специалистам, ответственными за информационную безопасность.

Запрещенные для пользователей действия

Ни в коем случае не стоит предпринимать следующие действия, если заражение уже произошло.

1. Осуществлять проверку и лечение компьютера с помощью антивирусного ПО;
2. Удалять или переустанавливать операционную систему;
3. Перемещать или удалять любые, в том числе незашифрованные, файлы на компьютере;
4. Изменять расширения зашифрованных файлов;
5. Использовать компьютер для выполнения любых задач;
6. Запускать утилиты дешифровки без консультации со специалистами, ответственными за информационную безопасность.