РОССИЙСКАЯ ФЕДЕРАЦИЯ
СВЕРДЛОВСКАЯ ОБЛАСТЬ

ГЛАВА ОБУХОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ КАМЫШЛОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА СВЕРДЛОВСКОЙ ОБЛАСТИ

Р А С П О Р Я Ж Е Н И Е

18.03.2022 № 17
с. Обуховское

О соблюдении мер защиты информации

На основании письма Министерства цифрового развития и связи Свердловской области от 17.03.2022 № 41-01-81/974, в соответствии с поручением Губернатора Свердловской области и информированием ФСТЭК России по Уральскому Федеральному округу в целях повышения защищенности объектов информационной инфраструктуры Российской Федерации и государственных информационных систем, от реализации угроз безопасности информации, связанных с противоправными и преднамеренными действиями зарубежных хакерских группировок, а также в целях предотвращения реализации угроз безопасности информации, связанных с внедрением вирусов-шифровальщиков, и эксплуатацией уязвимостей в системном и прикладном обеспечении:

1. Обеспечить строгое соблюдение мер по повышению защищенности объектов информационной инфраструктуры Российской Федерации и государственных информационных систем от реализации угроз безопасности информации (Приложение 1).
2. Ознакомить муниципальных служащих администрации и работников подведомственных организаций МКУ ОСП «ЭХО» и МКП «Обуховское», работающих с информационными системами с данными мерами под роспись.
3. Директору МКУ «Западный ЦИКД и СД» Артюшиной О.Н. довести данное распоряжение до подчиненных и работников подведомственных домов культуры и библиотек под роспись.
4. Контроль за исполнением настоящего распоряжения возлагаю на директора МКУ ОСП «ЭХО» Анохину Н.С.

Глава
Обуховского сельского поселения В.И. Верхорубов

Приложение №1 к Распоряжению
Главы Обуховского сельского
поселения от 18.03.2022 №17

Перечень мер по повышению защищенности объектов информационной инфраструктуры Российской Федерации и государственных информационных систем от реализации угроз безопасности информации

1) обеспечить резервирование информации, обрабатываемой в информационной системе, и проверить наличие актуальных резервных копий;
2) обеспечить хранение резервных копий в изолированном от сети «Интернет» сегменте информационной системы;
3) ограничить доступ пользователей информационной системы к резервным копиям данных;
4) ограничить (при возможности) сетевое взаимодействие между сегментами информационных систем по принципу «запрещено все, что явно не разрешено» (например, с помощью технологии VLAN и списков контроля доступа сетевого оборудования);
5) активировать функции анализа и блокировки входящего сетевого трафика средств межсетевого экранирования, установленных на рабочих местах пользователей (при их наличии);
6) ограничить доступ пользователей информационной системы и доступ внешних пользователей из сети «Интернет» к системам централизованного управления инфраструктурой информационных систем (при их наличии) (например, к таким системам относятся Active Directory, SCCM, Zabbix и другие системы);
7) провести анализ защищенности периметра информационной системы и веб-серверов в части выявления и устранения критических уязвимостей, ошибок конфигурации, а также удаления паролей, используемых по умолчанию;
8) запретить пользователям подключать к информационным системам неучтенные машинные носители информации, мобильные устройства и открывать любые ссылки из почтовых сообщений, скачивать файлы из сети «Интернет, а также использовать мобильные устройства для подключения к сети «Интернет»;
9) ограничить (при возможности) администраторам информационных систем права по сетевому подключению к автоматизированным рабочим местам пользователей;
10) ограничить средствами прокси-сервера список внешних информационных ресурсов, к которым пользователи информационной системы могут получить доступ (например, путем введения белых списков информационных ресурсов, к которым разрешен доступ);

11) организовать доступ к удаленным сегментам информационных систем (при их наличии) с применением виртуальных частных сетей (VPN);

12) ограничить использование беспроводных сетей (wi-fi);

13) обеспечить применение средств антивирусной защиты и антиспама, а также своевременное обновление их баз данных;

14) настроить на средствах антивирусной защиты, антиспама (при наличии) проверку всех поступающих на почту вложений;

15) создать отдельный электронный почтовый адрес, на который пользователи информационной системы будут присылать письма, которые могут содержать вредоносное содержание (ссылку или вложение);

16) проинформировать пользователей информационной системы о необходимости безопасной работы с электронной почтой, а именно:

- внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
- не открывать письма от неизвестных адресатов;
- проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
- не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com, и т.д.);
- не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов;
- проверять ссылки, даже если письмо получено от другого пользователя информационной системы;
- не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
- внимательно относится к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;
- в случае появления сомнений — направлять полученное письмо как вложение администратору информационной системы.

1) активировать (при возможности) механизмы проверки электронной почты, проверки подлинности домена-отправителя (например, использовать технологии DKIM, DMARC, SPF), а также настроить проверку входящих писем с использованием этих технологий;

2) заблокировать (при возможности) получение пользователями информационной системы в электронным письмах вложений с расширениями ADE, ADP, .APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH;

3) заблокировать доставку писем от доменов-отправителей, страной происхождения которых являются США и страны Европейского союза.

Также просим обратить внимание на устранение следующих уязвимостей:

1. Уязвимость модуля «vote» системы управления содержимым сайтов (CMS) 1С Битрикс (BDU:2022-01141, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – критический), связанная с возможностью отправки специально сформированных сетевых пакетов, позволяющая нарушителю, действующему удаленно, записать произвольные файлы в уязвимую систему. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- отключить и удалить модуль «vote»;
- осуществить настройку средств межсетевого экранирования прикладного уровня, позволяющую блокировать специальной сформированные сетевые пакеты.

2. Уязвимость библиотеки cmark-gfm (BDU:2022-01140, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), позволяющая нарушителю, действующему удаленно, выполнить произвольный код. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- отключить расширение table extansion;
- использовать входные данные для библиотеки только из доверенных источников.

3. По имеющейся в ФСТЭК России информации, в течении суток пользователи телекоммуникационного оборудования Cisco будут отключены от Smart-аккаунтов.

В целях недопущения возникновения такой ситуации рекомендуется на выходе инфраструктуры в сеть «Интернет» организовать фильтр с запретом трафика на домены и поддомены Cisco, в частности на адрес tools.cisco.com.

Актуальные сведения об угрозах безопасности информации и уязвимостях в системном и прикладном программном обеспечении систематически обновляются в Банке данных угроз безопасности информации, ведение которого осуществляет ФСТЭК России (bdu.fstec.ru).

ЛИСТ ОЗНАКОМЛЕНИЯ

с Распоряжением Главы Администрации Обуховского сельского поселения от 18.03.2022 №17 «О соблюдении мер защиты информации»

№ п/п	ФИО	Должность исполнителя	Подпись	Дата
1	Чистяков Александр Петрович	Заместитель главы администрации ОСП		
2	Стрекалова Алена Александровна	Заместитель главы администрации ОСП		
3	Мальцева Юлия Владимировна	Ведущий специалист ОСП		
4	Сметанин Андрей Иванович	Ведущий специалист ОСП		
5	Королева Светлана Анатольевна	Специалист 1 категории ОСП		
6	Якимова Анастасия Андреевна	Специалист 1 категории ОСП		
7	Черноталова Анна Викторовна	Специалист 1 категории ОСП		
8	Большева Надежда Анатольевна	Специалист 1 категории ОСП		
9	Михайлова Наталья Александровна	Специалист 1 категории ОСП		
10	Цыбуленко Евгения Андреевна	Специалист ВУС		
11	Анохина Наталья Сергеевна	Директор МКУ ОСП «ЭХО»		
12	Калугина Наталья Сергеевна	Юрист МКУ ОСП «ЭХО»		
13	Порошина Юлия Леонидовна	Специалист МКУ ОСП «ЭХО»		
14	Шишкин Евгений Иванович	Программист МКУ ОСП «ЭХО»		
15	Артюшина Ольга Николаевна	Директор МКУ «Западный ЦИКД и СД»		
16	Макарян Олег Альбертович	Директор МКП «Обуховское»		
17	Гнатюк Владимир Юрьевич	Главный инженер МКП «Обуховское»		
18	Емельянова Ольга Александровна	Бухгалтер-расчетчик МКП «Обуховское»		