

**РЕСПУБЛИКА ДАГЕСТАН**

**АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА**

**«ТАБАСАРАНСКИЙ РАЙОН»**

**368650, Республика Дагестан, Табасаранский район, с. Хучни, ул. Османова 32, тел.: 8 (87249) 22-0-38**

**ОКПО 04047044, ОГРН 1020501623933, ИНН/КПП 0530005533/053001001**

**Методические рекомендации по обеспечению информационной безопасности в администрации МР «Табасаранский район» и в подведомственных организациях.**

**Актуальность проблемы обеспечения информационной безопасности**

В настоящее время в условиях сложившейся политической обстановки, различными хакерскими группировками проводится компьютерные атаки, направленные на вывод из строя официальных сайтов, хищение информации и нанесение ущерба информационной инфраструктуре.

**Рекомендации по обработке электронных писем**

С января 2022 года на официальные электронные адреса федеральных и региональных органов государственной власти Российской Федерации под видом официальных запросов из различных госорганов злоумышленники направляют электронные письма, содержащие запросы о предоставлении сведений, подробности которых изложены в прикрепленных архивах, содержащих вредоносное программное обеспечение (далее – ВПО), предназначенное для получения скрытого удаленного доступа к системе. В целях затруднения обнаружения антивирусными средствами ВПО упаковывается в архив, разбитый на две части, которые впоследствии также архивируются.

В целях нейтрализации выявленных угрозообразующих факторов необходимо:

1. Использовать на всех объектах информационно-телекоммуникационной сети сертифицированные ФСБ России антивирусные средства с актуальными антивирусными базами.

2. Настроить на всех автоматизированных рабочих местах (далее – АРМ) периодическую (не реже 1 раза в месяц) полную антивирусную проверку системных и пользовательских каталогов операционной системы, а также полную (не реже 1 раза в месяц) антивирусную проверку всех несъемных носителей информации.

3. Настроить на всех АРМ процедуру принудительной антивирусной проверки подключаемых внешних носителей информации.

4. Проводить осмотр вложений электронных писем, поступающих на публичный (опубликованный в сети «Интернет») почтовый адрес организации, на выделенном АРМ с установленной на нем операционной системы семейства Linux и свободно распространяемым пакетом офисных программ. Целью указанных мероприятий является проверка вложенных электронных документов на предмет наличия ВПО, признаком которых может являться появление сообщений об ошибках в работе офисных программ при открытии вложенных электронных документов. В случае появления указанных сообщений об ошибках, необходимо удалять электронные письма, содержащие вложения, предположительно зараженные ВПО, и не открывать указанные вложения на других АРМ.

5. Осуществлять антивирусную проверку входящего веб-трафика, а также его фильтрацию с использованием контент-фильтров (сайтов развлекательного характера и сайтов социальных сетей, запрет посещения потенциально опасных сайтов, запрет загрузки исполняемых файлов).

6. Своевременно устанавливать критические обновления безопасности для прикладного программного обеспечения, в том числе офисных пакетов, средств просмотра PDF документов, интернет-браузеров, средств работы с Flash и Java приложениями.

7. Отключить в настройках офисных программ возможность работы со встроенными в документы макросами.

8. Осуществить настройку системы разграничения прав доступа в операционной системе с целью предоставления пользователям минимально необходимого перечня прав доступа (ограничить возможность установки программного обеспечения, создания файлов в системных директориях, запуска исполняемых файлов из пользовательских каталогов).

**Рекомендации по защите информационной инфраструктуры от вирусов-шифровальщиков**

Внедрение вирусов-шифровальщиков осуществляется через почтовые вложения, а также через несанкционированный доступ в информационные системы посредством эксплуатации уязвимостей веб-сайтов и средств, находящихся на периметре информационных систем.

С целью предотвращения реализации угроз безопасности информации, связанных с внедрением вирусов-шифровальщиков, необходимо принять следующие дополнительные меры по повышению защищенности объектов информационной инфраструктуры (далее – объекты):

1. Обеспечить резервирование информации, обрабатываемой в объектах, и проверить наличие актуальных резервных копий.

2. Обеспечить хранение резервных копий в изолированных от сети «Интернет» сегментах объектов.

3. Ограничить доступ пользователей объектов к резервным копиям данных.

4. Ограничить (при возможности) сетевое взаимодействие между сегментами объектов по принципу «запрещено все, что явно неразрешено» (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. Провести анализ защищенности периметра объектов и веб-серверов в части выявления и устранения критических уязвимостей, ошибок конфигурации, а также удаления паролей, используемых по умолчанию.

7. Запретить пользователям подключать к объектам 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».

8. Ограничить (по возможности) администраторам объектов права по сетевому подключению к автоматизированным рабочим местам пользователей.

9. Ограничить использование беспроводных сетей (wi-fi).

10. Обеспечить применение средств антивирусной защиты и антиспама, а также своевременное обновление их баз данных.

11. Настроить в средствах антивирусной защиты, антиспама (при наличии) проверку всех поступающих на почту вложений.

12. Создать отдельный электронный почтовый адрес, на который пользователи объектов будут присылать письма, которые могут содержать вредоносное содержание (ссылку или вложение).

13. Проинформировать пользователей объектов 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, tinurl.com и т.д.);

не нажимать на ссылки из электронных писем, если они заменены на слова;

проверять ссылки, даже если письмо получено от другого пользователя объекта;

не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;

внимательно относиться к электронным письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;

в случае появления сомнений – направлять полученное письмо в качестве вложения администратору информационной системы.

**Рекомендации по недопущению взлома сайтов.**

Уязвимости, приводящие к инцидентам информационной безопасности в информационной сфере классифицируются на 2 вида:

1) уязвимости, связанные с устаревшими версиями модулей и плагинов, содержащих ошибки безопасности в коде, скриптах, используемых на сайте;

2) утечка информации о реквизитах доступа к административной панели, вследствие наличия вредоносного программного обеспечения на локальном компьютере и использования протоколов передачи данных без шифрования.

Необходимые меры защиты:

1) использовать на хостинге сертифицированных средств межсетевого экранирования и антивирусной защиты.

2) обновить системы управления CMS и ее плагинов до актуальных версий.

3) изменить пароли доступа к панели управления, FTP, административной части сайтов и баз данных. Рекомендации к парольной защите: длина пароля – не менее 8 символов, включающих не менее одного символа прописной буквы английского алфавита (от А до Z), не менее одного символа строчной буквы английского алфавита (от а до z), не менее одного символа десятичной цифры (от 0 до 10) и не менее одного неалфавитного символа (@, #, $, &, \*, % и т.п.). Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd и т.п.).

4) использовать безопасные протоколы передачи данных с шифрованием (SSH, SFTP, HTTPS).

5) настроить регулярное выполнение резервного копирования для оперативного восстановления сайта в случае взлома.

6) отключить на сайтах сервисы иностранных разработчиков, в том числе сервисы детальной статистики.

7) настроить правила доступа для всех категорий пользователей веб-серверов к файлам и каталогам веб-сервера в соответствии с установленными правилами разграничения доступа (например, для пользователей, от имени которых запускается веб-сервер, для пользователей ftp-серверов и пользователей других служб).

8) установить минимально необходимые для работы правила доступа к файлам и директориям веб-серверов пользователям и администраторам.

9) ограничить доступ к каталогам систем контроля версий и их содержимому (таким как .git, .svn и другим каталогам), которые осуществляют сканирование.

10) настроить запрет выдачи листинга каталогов при отсутствии в них индексируемых файлов (если иное не предусмотрено функциональными возможностями веб-сервера).

11) настроить с использованием файла с именем robots.txt разрешенные и запрещенные для индексации каталоги и файлы.

12) ограничить хранение в директориях веб-сервера резервных копий и прочих файлов, наличие которых не требуется для функционирования веб-приложения.

13) ограничить использование на веб-страницах серверов информационных ресурсов (видеофайлов, электронных документов, изображений и других файлов), размещенных на сторонних серверах.

Подготовил:

**Ахмедханов Тельман Сейфутдинович,**

заместитель начальника отдела экономики и информационных технологий.