Администрация

Верхнебуреинского муниципального района

ПОСТАНОВЛЕНИЕ

11.10.2024 № 618

п. Чегдомын

Об утверждении методических рекомендации по работе в единой информационно-телекоммуникационной сети администрации Верхнебуреинского муниципального района Хабаровского края

В целях совершенствования защиты информации и повышения осведомленности в области защиты информации для муниципальных служащих, работников структурных подразделений администрации Верхнебуреинского муниципального района Хабаровского края, в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации», Указом Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», администрация Верхнебуреинского муниципального района Хабаровского края

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые методические рекомендации по работе в единой информационно-телекоммуникационной сети администрации Верхнебуреинского муниципального района Хабаровского края (далее – методические рекомендации).

2. Руководителям структурных подразделений администрации Верхнебуреинского муниципального района Хабаровского края:

2.1. Довести утвержденные методические рекомендации до сотрудников своих подразделений.

2.2. Проконтролировать выполнение методических рекомендаций сотрудниками подразделений администрации Верхнебуреинского муниципального района Хабаровского края

3. Методическое руководство и контроль исполнения пунктов методических рекомендаций возложить на отдел информационных технологий администрации Верхнебуреинского муниципального района Хабаровского края.

4. Контроль за исполнением настоящего постановления возложить на управляющего делами администрации Верхнебуреинского муниципального района Хабаровского края Феофанову И.В.

5. Настоящее постановление вступает в силу со дня его подписания.

Глава района А.М. Маслов

Приложение 1

УТВЕРЖДЕНО

постановлением

администрации

Верхнебуреинского

муниципального района

Хабаровского края

от 11.10.2024 № 618

Методические рекомендации по работе в единой информационно-телекоммуникационной сети администрации Верхнебуреинского муниципального района Хабаровского края

1. Общие положения

* 1. Методические рекомендации по работе в единой информационно-телекоммуникационной сети администрации Верхнебуреинского муниципального района Хабаровского края (далее – рекомендации, администрация) разработаны в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации», Указом Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» и иными нормативно-правовыми документами по вопросам использования и защиты информационных ресурсов.
  2. Настоящие рекомендации разработаны в целях совершенствования защиты информации и повышения осведомленности в области защиты информации для муниципальных служащих, работников структурных подразделений (далее - пользователи) администрации, использующих в своей работе средства вычислительной техники (далее – СВТ).
  3. В рекомендациях рассматриваются методы и приемы безопасной работы на СВТ при выполнении служебных обязанностей.
  4. При возникновении проблем, описанных в настоящих рекомендациях и им подобных, следует обращаться только к уполномоченным лицам. Самостоятельное решение возникших проблем может повлечь за собой возможное ухудшение работоспособности и защищенности СВТ.

2. Общие принципы работы пользователя СВТ

2.1. Пользователю следует:

- обеспечивать сохранность выданных ему СВТ, служебных машинных носителей информации (далее – МНИ), персональных идентификаторов;

- обеспечивать конфиденциальность информации, хранимой на выданных МНИ;

- использовать выданные ему СВТ и МНИ исключительно в целях выполнения своих должностных обязанностей. Вся информация, находящаяся на МНИ должна быть служебного характера, запрещено использовать служебные МНИ для передачи файлов в личных целях;

- при использовании ключей электронной подписи в нерабочее время обеспечить хранение ключей в надежно запираемых ящиках, шкафах, сейфах;

- при оставлении рабочего места блокировать компьютер путем штатной блокировки рабочего места;

- контролировать действия лиц в рабочих кабинетах, не имеющих право самостоятельного доступа в эти кабинеты;

- размещать экран монитора таким образом, чтобы исключить несанкционированный просмотр информации с него посторонними лицами;

- своевременно сообщать к главному инженеру по защите информации отдела информационных технологий администрации о выявленных фактах нарушений.

2.2. Пользователю не допускается:

- подключать к компьютеру личные съемные устройства хранения информации (МНИ, сотовые телефоны, смартфоны, планшеты, карты памяти, USB-модемы (3G, 4G/LTE), USB Wi-Fi/Bluetooth адаптеры и т.п.);

- выбрасывать вышедшие из строя служебные съемные МНИ. При выходе из строя служебных съемных МНИ необходимо их передать комиссии по вопросам защиты информации в администрации;

- передавать свои учетные данные (имена учетных записей и пароли к ним) третьим лицам;

- совершать любые попытки повышения пользовательских привилегий;

- выбрасывать бумажные носители со служебной информацией (например, парольные карточки с разовыми паролями, телефонный справочник администрации с контактными данными и т.п.), в том числе и документы с пометкой «для служебного пользования». Такие документы подлежат уничтожению в специализированных бумагорезательных машинах;

- подключать в розетки локальной сети любые посторонние (в том числе личные) сетевые устройства.

3. Работа в сети Интернет

3.1. Основные правила работы в сети Интернет:

- не обсуждать служебные вопросы в социальных сетях, форумах и иных веб-ресурсах;

- не открывать веб-страницу, при попытке открытия которой выходит сообщение о том, что страница заражена вирусной программой;

- при использовании сайтов, поддерживающих протокол защиты трафика (далее – SSL), следует отслеживать наличие у сайта включенной защиты.

3.2. Метод распознавания – подлинные веб-узлы используют SSL или другие технологии безопасности для защиты личных сведений, вводимых пользователем при создании учетной записи и последующем входе на веб-узел. Если на странице используются технологии безопасности, в строке состояния обозревателя отображается значок в виде замка. Кроме того, веб-адрес содержит префикс «https://» (обращаем внимание на букву «S» после «http», которая обозначает «безопасный») вместо обычного префикса «http://». Префикс «https://» означает, что на веб-ресурсе используется защищенный SSL-сертификат, подтверждающий подлинность данного ресурса.

- не нажимать активные элементы всплывающих окон веб-страниц (сообщения о том, что СВТ заражено или требует оптимизации, рекламные сообщения и т.п.);

- следить за доменными именами интернет-сервисов;

- не использовать общедоступные и личные сервисы для хранения и обмена служебной информацией;

- избегать самостоятельной установки плагинов (расширений, дополнений) к браузерам.

4. Правила использования паролей

4.1. Аутентификацию пользователя (ввод пароля) следует использовать во всех информационных системах.

4.2. Следует отказаться от использования функции «запоминания пароля», так как при получении физического доступа к СВТ, любой пользователь может зайти под запомненными учетными данными.

4.3. Рекомендуется для входа в разные информационные системы (например, почтовый сервис и система электронного документооборота) использовать уникальные пароли (отличающиеся друг от друга).

4.4. Рекомендуемые правила создания паролей:

- пароль содержит символы верхнего и нижнего регистров;

- пароль содержит комбинации букв и цифр;

- пароль содержит специальные символы;

- длина пароля составляет не менее 8 символов;

- пароль не несет смысловую нагрузку (например: пароль – «Lj,hj1» в русской раскладке «Добро1»), или не является общераспространенной комбинацией клавиш (например: «Qwerty1234»; «Asdasd123» и т.п.).

4.5. Пароль пользователя составляет его личную тайну.

4.6. Ограничения при использовании паролей:

- использовать служебные пароли в личных целях (например, использовать служебный пароль при регистрации в социальных сетях или общедоступных почтовых сервисах);

- записывать служебные пароли на любых носителях (на бумажных стикерах, в блокнотах, в файлах текстового формата и т.п.), и хранить их в доступном месте (приклеивать на монитор, хранить под клавиатурой, в ежедневнике и т.п.).

5. Правила использования электронной почты

5.1. Метод рассылки письма с рекламой (спам) может быть использован злоумышленниками для кражи служебной информации из информационных систем государственных органов. Основная опасность спам-писем заключается во внедрении вредоносного кода (компьютерного вируса) на персональный компьютер пользователя. Вредоносный код может находиться в теле письма в виде вложения, либо в письме находится гиперссылка на вредоносный код.

При получении письма следует проверять:

- авторство письма (от кого получено письмо);

- тему письма;

- наличие в письме вложений;

- содержимое письма (информационный текст) на наличие гиперссылок и других активных элементов (картинки, кнопки «нажми сюда», и т.п.).

5.2. Проверка авторства письма.

Автор вредоносных писем может указать любое имя в адресной строке отправителя (от кого получено письмо). Поэтому следует учитывать, что письмо может быть получено как от незнакомых адресов, так и с адресов, чьи имена максимально похожи с известными.

Необходимо тщательно проверять адрес отправителя и, в случае сомнения, игнорировать данное письмо.

5.3. Проверка темы письма.

Как правило, в ходе деловой переписки собеседники указывают в поле «тема письма» информацию, наиболее близкую по содержанию тела письма.

Самое распространенное содержание тем вредоносных писем, рассылаемых злоумышленниками:

- дешевые финансовые предложения (кредиты, ипотеки);

- риторические вопросы;

- вопрос, требующий срочного решения;

- денежные суммы, наименование валют в заголовке;

- фрагменты текста, выделенные яркими цветами;

- тема или отдельные слова заглавными буквами;

- в теме слова или словосочетания, связанные с деньгами: «Бесплатно», «Купи», «Заработай», «Скидка», «Деньги», «Распродажа» и т.п.

5.4. Проверка вложений к письму.

5.4.1. Вредоносный код чаще всего внедряется через прилагаемые к письму гиперссылки, вложенные файлы, активные элементы (кнопки, картинки в теле письма и т.п.).

5.4.2. Гиперссылка (обычный вид «http://адрес\_сайта.имя\_домена») переводит пользователя на заведомо зараженный Интернет-ресурс.

5.4.3. Вложенный файл может иметь как стандартное расширение (например, «\*.doc», «\*.xls», «\*.rar», «\*.zip» и пр.), так и нестандартное (например, «\*.zip1»).

5.4.4. Имя файла может иметь произвольный вид, начиная от набора символов (например, «asdasd.doc»), заканчивая именами, завуалированными под документы, создаваемые в органах государственной власти (например: «договор на оказание услуг.doc», «решение МВК.zip»).

5.4.5. Расширение файла также может быть «замаскировано» под общепринятые форматы. Например, в исполняемом файле с именем «договор\_на\_оказание\_услуг.doc.scr» расширением является «\*.scr». При выключенной опции отображения расширений имен файлов в операционной системе зараженное вложение будет иметь привычное имя для файлов Microsoft Word, что увеличивает вероятность запуска файла и дальнейшего заражения.

5.4.6. Зараженные файлы могут быть получены в социальных сетях или в интернет-мессенджерах, в том числе от учетной записи из списка контактов.

5.4.7. Проверка содержимого письма.

5.4.8. В теле письма могут быть гиперссылки и другие активные элементы (картинки, кнопки «нажми сюда» и т.п.). Настройки по умолчанию почтового сервиса Правительства края (АРМ ГС), работающего через веб-интерфейс («https://e.armgs.team») блокируют изображения в письмах. При этом в служебных целях доступна возможность включения пользователем активного содержания письма.

5.4.9. При подозрении на вредоносное письмо необходимо обратиться к главному инженеру по защите информации отдела информационных технологий администрации.

5.4.10. Нажатие любых активных элементов в полученном письме может повлечь заражение СВТ вирусным программным обеспечением.

5.5. Типовые рекомендации при получении подозрительного письма:

- при получении письма от знакомого адресата с подозрительным содержанием необходимо уточнить у адресата факт отправки письма;

- использование правил фильтрации почтовых сообщений в качестве дополнительного метода защиты от спама.

5.6. Спам-письма могут быть направлены с целью получения доступа к критическим данным (именам пользователей и паролям). Такой вид мошенничества называется «фишинг». Злоумышленник создает ссылку на заранее подготовленный ресурс, который визуально выглядит аналогично ресурсу, куда пользователь намеревается перейти. После первичного ввода имени учетной записи и пароля, введенные данные записываются на серверах злоумышленника, пользователю выдается сообщение об ошибке ввода и далее следует переадресация на легитимный ресурс.

5.7. Для уменьшения количества спам-писем не следует использовать свой служебный почтовый адрес на общедоступных интернет-сайтах (при регистрации в социальных сетях, интернет-магазинах, в качестве контактной информации и т.п.).

6. Использование средств антивирусной защиты

6.1. При выполнении служебных обязанностей возможно возникновение ситуаций, при которых реакция СВТ на действие пользователей не является ожидаемой.

6.2. Признаки вирусного заражения (без уведомления антивирусного средства):

- невозможность загрузки операционной системы;

- самовольная перезагрузка операционной системы;

- внезапная остановка работы программного обеспечения;

- вывод на экран непредусмотренных сообщений, изображений и звуковых сигналов;

- постоянное обращение к жесткому диску при простое компьютера (на системном блоке постоянно горит или мигает его светодиод) вне зависимости от действия или бездействия пользователя;

- вывод на экран предупреждений антивирусного программного обеспечения о попытке несанкционированного выхода в сеть Интернет;

- компьютер работает заметно медленнее обычного;

- самопроизвольный запуск программного обеспечения;

- продолжительная загрузка программных средств или необычное поведение интернет-браузера (например, подмена одного сайта другим, самопроизвольная подмена «домашней» страницы и/или поискового сайта, невозможность закрыть окно браузера);

- неуправляемая работа подключенных к компьютеру устройств (внезапное открытие или закрытие лотка CD-ROM или DVD-ROM, самопроизвольное движение курсора мыши);

- медленная работа браузера сети Интернет (открытие веб-страниц, просмотр видеофайлов, прослушивание аудиофайлов);

- знакомые говорят о сообщениях от имени пользователя, которые пользователь не отправлял (отправка сообщений в интернет-мессенджерах, электронных писем);

- большое количество сообщений в почтовом ящике без обратного адреса и заголовка;

- отказ работы антивирусного средства;

- самопроизвольное создание файлов на жестком диске компьютера;

- самопроизвольное исчезновение файлов и каталогов или искажение их содержимого;

- предупреждение монитора (антивирусного ПО) об атаке.

Данный перечень не является полным.

6.3. При обнаружении вируса или подозрении на вирусное заражение следует:

- приостановить работу на своем СВТ и возобновлять ее только после удаления вирусной программы и нейтрализации последствий вирусного заражения;

- сообщить ответственному главному инженеру по защите информации отдела информационных технологий администрации об обнаруженном вирусе или подозрении на вирусное заражение, и источнику, откуда был получен зараженный файл (владелец), если источник получения имеет высокий уровень доверия.

7. Обращение с мобильными устройствами связи

7.1. При переписке в интернет-мессенджерах и посредством СМС возможна подмена адресата, поэтому при получении нестандартных сообщений от коллег, в особенности руководителей, следует уточнить действительно ли от них приходило сообщение.

Нестандартным сообщением может быть:

- сообщение, содержащее текст, написанный не в обычном стиле адресата, хотя легальный автор обычно пишет грамотно, и наоборот;

- сообщение, в котором слишком много грамматических ошибок;

- сообщение, содержащее неожиданный призыв к определенным действиям. Например, просьба или приказ зайти на веб-ресурс, позвонить по определенным номерам, выслать ту или иную информацию на указываемый адрес.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_