ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ ВОЛОГОДСКОЙ ОБЛАСТИ
бюджетное учреждение здравоохранения Вологодской области
«ВОЛОГОДСКАЯ ОБЛАСТНАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА»
(БУЗ ВО «ВОКБ»)

ПРИКАЗ

26 апреля 2024 № 446

г. Вологда

Об внесении изменений в приказ № 1112 от 27.11.2017г. «Об утверждении «Инструкции по обеспечению антивирусной безопасности в БУЗ ВО «Вологодская областная клиническая больница»

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Приказа ФСТЭК России от 18 февраля 2013 г. №21» Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Дополнить Приложение 1 Памятка по антивирусной безопасности **Инструкции по обеспечению антивирусной безопасности в БУЗ ВО «Вологодская областная клиническая больница»** следующим содержанием:

По электронной почте могут приходить письма, якобы от лица администратора соцсети или от сотрудников банка — с просьбой прислать свои логин и пароль, например якобы для восстановления после сбоя базы данных, или с просьбой перейти по ссылке для подтверждения адреса электронной почты. Зачастую, перейдя по ссылке, можно обнаружить запрос на ввод данных (пароля, логина, номера банковской карты и т. п.). При этом страница сайта внешне может быть похожа на ресурс, которым вы привыкли пользоваться (соцсеть, интернет-банкинг). Однако если обратить внимание на адрес такой страницы, то можно заметить, что он незначительно отличается от оригинального, например вместо «o» может стоять «0» или вместо «l» — «I» или b на d, использовать сочетание букв (rn вместо буквы m, cl вместо d, vv вместо w) и т.д. Пример: 0nlinedank.ru вместо onlinebank.ru.

Как только запрашиваемые данные будут введены на такой лжестранице, они сразу же попадут в руки злоумышленника, который сможет воспользоваться ими в своих корыстных целях.

Признаки в письмах, которым не стоит доверять:

- в тексте более чем одна ашибка или писка;
- ссылка в виде цифр. Пример: 178.248.232.27;
- ссылка содержит символ «@»; Пример: http://bank.ru@phish.ru ;
- ссылка с двумя и более адресами. Пример: https://bank.ru/bitrix/rd.php?go=https://bitly.com/bank
- письма с отсутствующими дополнительными контактами (ФИО, должность, телефон, почтовый адрес);
- если в начале адреса сайта есть www, но нет точки или стоит тире. Пример: wwwbank.ru или www-bank.ru
- если в начале адреса сайта есть http или https, но нет «://». Пример: httpsbank.ru
- когда в адресе сайта несколько точек, смотрите то, что написано в правой части, до первого символа «/», там вы обнаружите исходный сайт и если он вам не знаком — ссылка подозрительна. Пример: www.bank.ru.zlodey.ru/login?id=12/aa/bank.ru
- email в поле «Отправитель» может быть подделан или самого отправителя могли взломать;
- если при наведении указателя «мыши» ссылка выглядит по-другому. Пример: в тексте письма написано tele2.ru, а при наведении мыши, в нижнем левом углу браузера отображается teie2.ru
- ссылка может быть не кликабельна, но содержать подмененные символы. Злоумышленник надеется, что вы скопируете ссылку и вставите в браузер. Пример: в письме указана ссылка teIe2.ru, копируете и вставляете в браузер, но оказывается, что это teie2.ru
- если ссылка начинается с https:// — это не значит, что она безопасна;

Для того чтобы этого избежать, необходимо руководствоваться несколькими простыми правилами:

– не отвечайте на письма от неизвестных отправителей;

– не переходите по ссылкам, содержащимся в письмах;

– не сообщайте приватную информацию, запрашиваемую в письмах, приходящих по электронной почте.

- не фотографируйте свое рабочее место и компьютер и тем более не выкладывайте эти фото в интернет.
- проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
- 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;

Не рекомендуется сообщать пароль от почты кому бы то ни было. Если в какой-то момент вам пришлось предоставить друзьям или коллегам доступ к своему электронному ящику или если у вас возникло подозрение, что кто-то посторонний узнал ваш пароль, — необходимо как можно скорее его сменить. К любым письмам с вложениями обязательно применяйте другие правила из памятки;

При подключении к незащищенным точкам доступа передаваемые данные не шифруются, поэтому злоумышленник может перехватить их при помощи ноутбука с Wi-Fi-адаптером. Используя специальную программу для «перехвата трафика», злоумышленник сможет увидеть все данные, передаваемые по такой сети, в частности пароль от электронной почты. Для того чтобы обезопасить себя от перехвата паролей рекомендуется:

– не пользоваться открытыми Wi-Fi-сетями для доступа к электронной почте, соцсетям и прочим ресурсам, требующим ввода пароля;

– использовать VPN при подключении к открытым точкам доступа Wi-Fi;

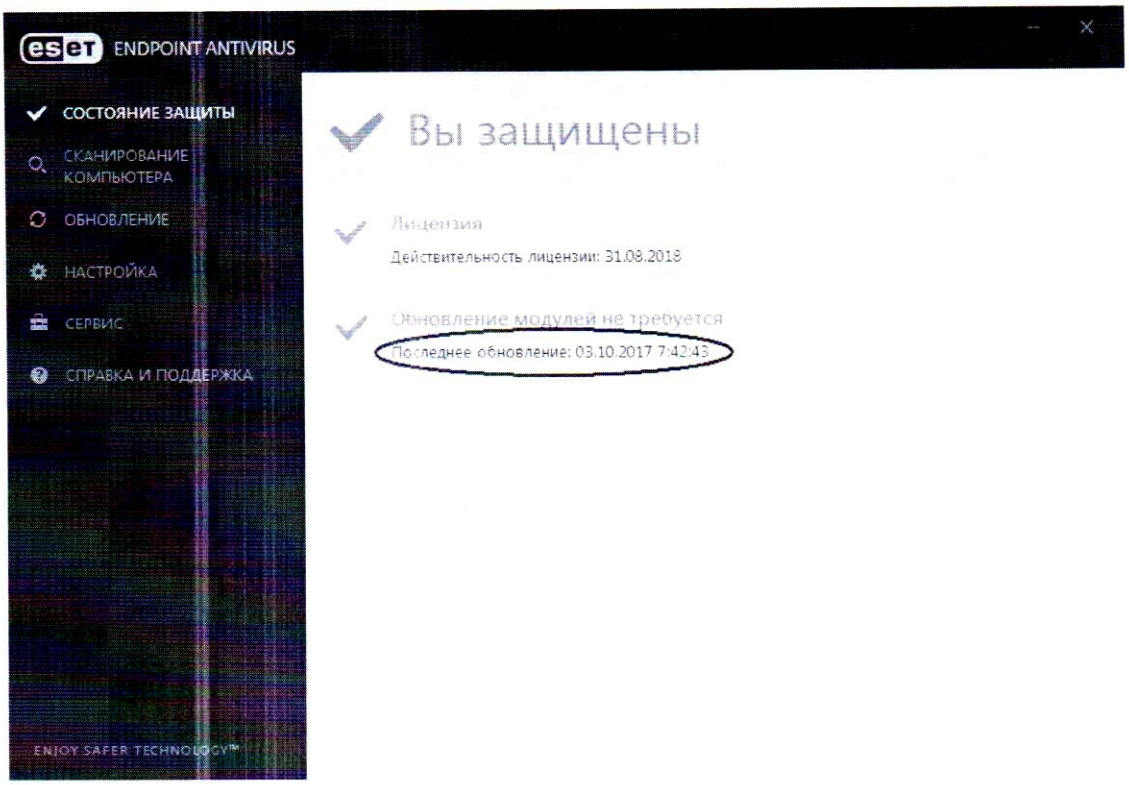
– отключить общий доступ к файлам на устройстве.

Что делать при получении подозрительного письма:

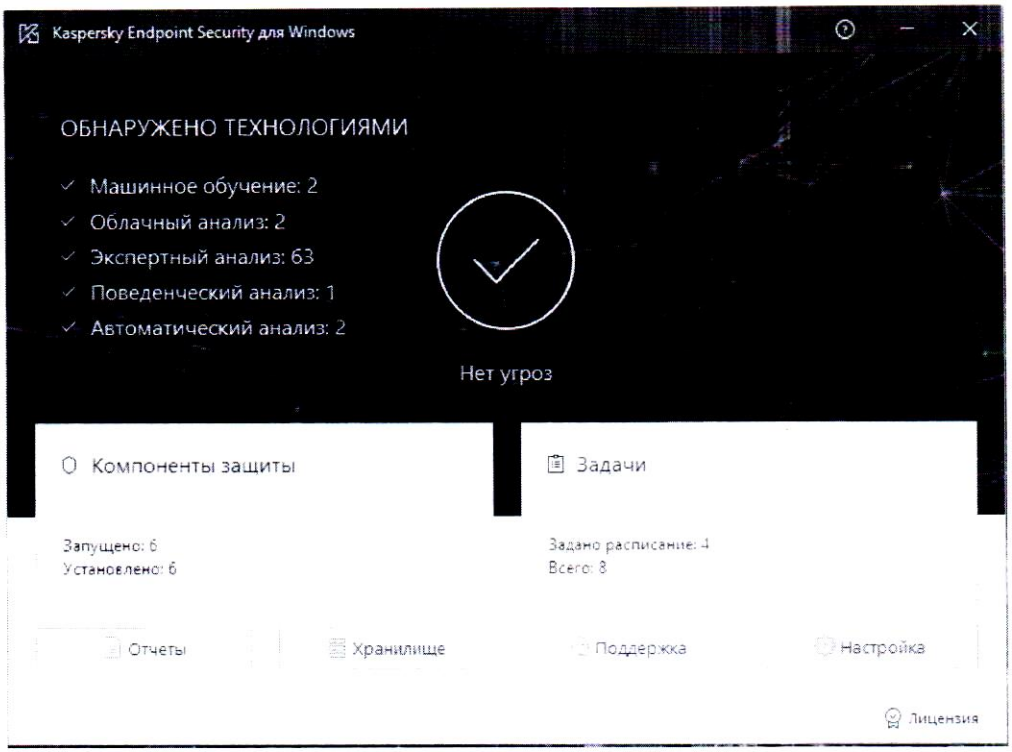
- лично, по телефону, через мессенджер уточнить факт отправки такого письма. Желательно, контакт для связи взять не из письма, а из других источников: собственная записная книжка, визитка, спросить у коллег, узнать на официальных сайтах;
- перешлите письмо для проверки в отдел АСУ на адрес antivirus@vokb35.ru

2. Заменить в Приложении 1 Памятка по антивирусной безопасности **Инструкции по обеспечению антивирусной безопасности в БУЗ ВО «Вологодская областная**

клиническая больница» абзац «Проверьте наличие антивирусной программы на вашем компьютере. Для этого запустите антивирусную программу (выберите мышкой «ПУСК → Программы → ESET → ESET Endpoint Antivirus→ Eset Endpoint Antivirus»). У вас откроется окно, как показано на рисунке ниже.



На «Проверьте наличие антивирусной программы на вашем компьютере. Для этого запустите антивирусную программу (выберите мышкой «ПУСК → Программы → Kaspersky → Kaspersky Endpoint Security. У вас откроется окно, как показано на рисунке ниже.



3. Ответственному за размещение информации на официальном сайте учреждения Уланову Д.В. загрузить актуальную версию **Инструкции по обеспечению антивирусной безопасности в БУЗ ВО «Вологодская областная клиническая больница»** в соответствующий раздел сайта.

4. Заведующим отделений ознакомить с инструкцией персонал структурного подразделения.

5. Заведующей канцелярией О.В. Аверьяновой ознакомить с настоящим приказом всех ответственных

6. Контроль за исполнением приказа оставляю за собой.

Главный врач Д.В. Ваньков

Исп. Огнерубова Ю.Н.
8(8172) 51-52-19