**Памятка**

**по соблюдению мер безопасности при использовании**

**служебной электронной почты**

Электронная почта давно стала представлять собой среду для распространения вирусов, троянских программ. Если не обеспечен надлежащий контроль над ее использованием, это может привести к крайне серьезным последствиям.

1. **Для системных администраторов и администраторов безопасности информации органов и организаций**

1.1. Рассмотреть возможность перехода на отечественные решения или сервисы по защите электронной почты.

1.2. Если организация не взаимодействует с иностранными контрагентами, запретить коммуникации на сетевом уровне по протоколу SMTP с зарубежными IP-адресами (при возможности), или настроить уведомления пользователей в тексте сообщения при получении от зарубежного отправителя (при возможности).

1.3. Активировать механизмы проверки подлинности домена отправителя с использованием технологий SPF, DKIM, DMARC (при возможности).

1.4. Настроить функции уведомления пользователей в тексте сообщения при получении от внешнего отправителя (при возможности).

 1.5. Запретить использование почтового сервера в качестве открытого *relay*.

1.6. Пересылку всей подозрительной электронной почты на специально созданный адрес электронной почты **«*threat@it.e-zab.ru»*** для анализа.

1.7. Использовать почтовую «песочницу».

1.8. Заблокировать получение пользователями систем и сетей электронных писем, имеющих вложения с расширениями ADE, ADP, .АРК, АРРХ, APPXBUNDLE, ВАТ, CAB, СНМ, CMD, COM, CPL, DLL, DMG, EX, ЕХ\_, EXE, НТА, 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.

1.9. Обеспечить антивирусную защиту всех входящих сообщений и вложений в них.

**2. Для пользователей**

* внимательно проверять адрес отправителя сообщения, в случае возникновения подозрений в истинности отправителя необходимо связаться с ним по телефону или другим способом и уточнить факт отправки сообщения. Желательно, контакт для связи взять не из письма, а из других источников: собственная записная книжка, визитка, спросить у коллег, узнать на официальных сайтах;
* не доверять даже «известным» адресам. Адрес отправителя очень легко подделать (см. ниже - Признаки в письмах, которым не стоит доверять);
* все полученные вложения проверять антивирусными средствами на предмет наличия вредоносного программного обеспечения;
* никогда не запускать полученные по электронной почте программы, даже если письмо пришло от известного лица;
* никому не давать свой пароль, даже хорошо знакомым коллегам, сотрудникам из ИТ-подразделений и службе безопасности. Не делиться данными об аккаунте с другими;
* открывая полученные документы, не разрешать использование макросов;
* по возможности пользоваться почтовыми клиентами последних версий;
* использовать только корпоративные почтовые ящики в домене  \*.*e-zab.ru.* Не допустимо использование коммерческой электронной почты (ya.ru, mail.ru, gmail.com и т.д.) в служебных целях;
* не просматривать на работе свою личную почту на бесплатных почтовых сервисах и не посещать сайты, не связанные с выполнением служебных обязанностей;
* не вводить пароль если почтовое сообщение запрашивает его, или требует пароль взамен на получение какой-либо услуги. Чаще всего к таким действиям прибегают злоумышленники;
* не использовать и не устанавливать не разрешенные к использованию в вашем органе (организации) программы и программы, не предназначенные для выполнения должностных обязанностей;
* особое внимание обращать на сообщения, поступающие от неизвестных адресатов, а также от федеральных органов (ФСБ России, прокуратуры, следственного комитета, банковских структур и др.) так как кибермошенниками используются адреса электронной почты похожие на истинные адреса существующих органов и организаций и тексты вложений похожи на документы истинных адресатов (см. ниже - Признаки в письмах, которым не стоит доверять);
* с использованием электронной почты запрещается пересылать информацию ограниченного доступа (персональные данные, информацию для служебного пользования), а также пересылать нелегально распространяемые материалы (аудио-, видеоданные, программное обеспечение);
* считать вредоносными электронные письма направленные со следующих почтовых серверов: «mx.roztec.ru», «mx.nacimibio.ru», «mail.kazkad.ru», «mlrmailer.com», «mail.mlrmailer.com», «sender-gosuslugi.ru», «mail.sender-gosuslugi.ru», «mail.gazpromlpg.ruoe.ru», «mail.npoem.ruoe.ru», «email.tpprf.ruoe.ru», «dionis.r31.rosreestr.ruoe.ru», «mx.vertical.ruoe.ru», «mail.muctr.ruoe.ru», «mail.tcm-u.ruoe.ru», «mail.it-vbc.ruoe.ru», «mail.ktrv.ruoe.ru», «mail.hi-tech.ruoe.org», «mail.acti.ruoe.ru», «mail.am-tec.ruoe.ru», «mail.sevastopolteplo.ruoe.ru», «olymp.deloports.ruoe.ru», «outlook.ekassir.uercus.com», «post.sberbank-tele.uercus.com», «mail-kras.bbr.ruoe.ru», «email.okb-nouator.ru», «mail.kronshadt.ru», «mail.tscrimea.ruoe.ru», «mail.gazpromviet.uercus.com», «mail.volnamobile.ruoe.ru», «mail.5-tv.ruoe.ra», «exchange-log.rzdlog.ruoe.ru», «mail.rossiya-airlines.uercus.com», «mail.dynasystems.ruoe.ru», «mail.ventocloud.ruoe.ru», «mail.omg.transneft.ruoe.ru», «mail.digital.gov.ruoe.ru», «mail.tass.ruoe.ru», «post2.interfax.ruoe.ru», «mail.iz.ruoe.ru», «app.aif.ruoe.ru», «mail.tvrain.ruoe.ru», «mail.life.ruoe.ru», «mail.vniiem.ruoe.ru», «mail.aviaremont.ruoe.ru», «smtp.mikron.ruoe.ru», «mail.kmz.ruoe.ru», «mail.vympel-ybinsk.ruoe.ru», «mail.goz.ruoe.ru», «mail.ach.gov.ruoe.ru», «mail.fadm.gov.ruoe.ru», «mail.rst.gov.ruoe.ru», «mail.minstroyrf.ruoe.ru», «mail.minobmauki.gov.ruoe.ru», «postman.rosleshoz.ruoe.ru», «mail.21.mchs.gov.ruoe.ru», «email.mkrf.ruoe.ru», «mail.knaaz.Jruoe.org», «mail.nicevt.ruoe.ru», «mail.gardatech.ruoe.ru», «mail.dtln.ruoe.ru», «webmail.planar-elements.ruoe.ru», «mxl3.ml3.ruoe.ru», «mail.informseti.ruoe.ru», «mail.cloud.mts.ruoe.ru», «exchange.avito.ruoe.ru».
* считать подозрительными письма, у которых в поле «Тема» содержится призыв к действиям (например «открой», «прочитай», «ознакомься»), а также упоминаются финансы, банки, геополитическая обстановка или содержатся угрозы, письма, содержащие документы с макросами, архивы с паролями, а также файлы с расширениями .rtf, .lnk, .chm, .vhd;
* если при открытии файла-вложения показывается «ошибка открытия» или показываются непонятные символы, существует большая вероятность того что данный файл содержит вредоносную программу и в это время идет шифрование информации на компьютере (даже после закрытия файла). Файл может автоматически рассылаться коллегам с просьбой помочь открыть его. В итоге зашифрованными могут оказаться все информационные ресурсы организации;
* **в случае возникновения вопросов и выявления инцидентов информационной безопасности необходимо немедленно обратиться к ответственному за информационную безопасность или должностному лицу, на которое возложены полномочия по обеспечению информационной безопасности, в том числе обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты органа (организации).**

**Признаки в письмах, которым не стоит доверять:**

* в тексте более чем одна ашибка или аписка;
* ссылка в виде цифр. Пример: 178.248.232.27;
* ссылка содержит символ «@»; Пример: http://bank.ru@phish.ru ;
* ссылка c двумя и более адресами.
* 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
* злоумышленник может заменить букву “o” на цифру “0” или маленькую латинскую букву L — “l”, на большую букву i — “I” или b на d, использовать сочетание букв (rn вместо буквы m, cl вместо d, vv вместо w) и т.д. Пример: 0nIinedank.ru вместо onlinebank.ru
* если ссылка начинается с https:// — это не значит, что она безопасна.