Правила обращения с входящими электронными письмами,

содержащими подозрительные вложения (фишинговые

письма)

Для снижения возможных рисков и обеспечения безопасности на рабочем месте, просим проявлять осторожность при работе с письмами, содержащими подозрительные электронные вложения (архивы, ссылки). Перед открытием такого письма убедитесь, что вы соблюдаете правила работы с входящими электронными письмами.

• Производите проверку почтовых вложений с использованием средств антивирусной защиты. Это поможет защитить ваши данные от вредоносных программ (\*см. Руководство пользователя при работе с антивирусным программным обеспечением и проверкой файлов);

• Проверяйте имя домена отправителя электронного письма в целях идентификации отправителя. Для этого необходимо обращать внимание на наименование почтового

адреса (домена), указанного после символа «@», и сопоставлять его с адресами (доменами) органов (организаций), с которыми осуществляется служебная переписка;

• Для обмена информацией с коллегами, рекомендуется использовать только те адреса электронной почты организаций, с которыми вы регулярно взаимодействуете, и вести список таких адресов;

• Обратите внимание на тему письма. Она должна быть связана с содержанием и актуальна для вас. Злоумышленники могут использовать привлекательные темы, чтобы побудить вас открыть вложение или перейти по ссылке;

• Не открывайте подозрительные вложения, особенно если они имеют незнакомые форматы (doc, .exe, .xlx-файлы) или необычные названия;

• Будьте осторожны с подозрительными запросами или ссылками, которые приходят к вам по электронной почте или через сообщения от незнакомых отправителей. Вирусы и шпионские программы часто распространяются через электронные письма и ссылки;

• Перед тем как перейти по ссылке, убедитесь, что она ведёт на нужный сайт и не содержит подозрительных символов (#, $, ?). Такие ссылки могут быть опасными. Для проверки безопасности сайта воспользуйтесь специализированными сервисами (https://yandex.ru/safety, https://vms.drweb.ru);

• Ограничьте доступ к личной информации – не разглашайте свои личные данные и информацию о своей работе на публичных ресурсах и социальных сетях.

Если вы подозреваете, что получили фишинговое письмо, сообщите о нем на электронный адрес: [ozi@cit.gov35.ru](mailto:ozi@cit.gov35.ru)

* **\* Руководство пользователя при работе с антивирусным программным обеспечением и проверкой файлов Для Kaspersky Internet Security**

Шаг 1 Запустите Kaspersky Internet Security на вашем

Шаг 2 Кликните на иконку «Настройки» (шестеренка) в правом нижнем углу окна программы.

Шаг 3 В открывшемся окне выберите пункт «Проверка», затем «Проверка файлов».

Шаг 4 Выберите файл, который хотите проверить, нажав на кнопку «Обзор...» и указав путь к файлу.

Шаг 5 Нажмите на кнопку «Открыть», а затем «ОК».

Шаг 6 Файл будет добавлен в список для проверки. Нажмите на кнопку «Запустить проверку».

Шаг 7 Ожидайте окончания проверки. Время проверки зависит от размера файла и мощности вашего компьютера.

Шаг 8 По окончании проверки вы увидите результат - файл чист от вредоносного ПО или содержит вирусы.

Шаг 9 При обнаружении вирусов вы можете выбрать действие, которое необходимо выполнить с вредоносным файлом: удалить, поместить на карантин или игнорировать.

Шаг 10 После выбора действия нажмите на кнопку «Применить», чтобы подтвердить свой выбор.

**Для Dr.Web**

Шаг 1 Запустите антивирусное программное обеспечение Dr.Web на своем компьютере.

Шаг 2 В главном окне программы нажмите на кнопку «Выбрать объекты для проверки».

Шаг 3 В открывшемся окне нажмите на кнопку «Добавить файл» и выберите файл, который вы хотите проверить.

Шаг 4 После выбора файла нажмите на кнопку «ОК», а затем на кнопку «Начать проверку».