Руководство пользователя по соблюдению информационной безопасности на рабочем месте и во время работы в сети «Интернет»

I. Правила по соблюдению информационной безопасности при получении электронного сообщения

1. **Антивирусная защита.** Используйте антивирусное программное обеспечение на всех компьютерах и устройствах, с которыми вы работаете. Это поможет защитить ваши данные от вредоносных программ.
2. **Адрес отправителя.** Проверьте адрес отправителя и убедитесь, что он является официальным и знакомым. Вы можете проверить адрес электронной почты на официальном сайте учреждения, чтобы убедиться в его подлинности. Мошенникам свойственно использовать поддельные адреса электронной почты.
3. **Тема письма.** 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.
4. **Текст письма.** Внимательно прочитайте текст письма. Если в нём содержатся непонятные запросы или предложения, это может говорить о мошенничестве.
6. **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).
7. **Подозрительные вложения.** Избегайте открытия вложений и перехода по ссылкам от незнакомых отправителей. Вирусы и шпионские программы часто распространяются через электронные письма и ссылки.

II. Правила безопасной работы при скачивании файлов

1. Перед загрузкой файла убедитесь, что источник является надёжным. Чтобы проверить это, изучите репутацию сайта в Интернете, почитайте отзывы или воспользуйтесь специальными сервисами для проверки безопасности, такими как Yandex.ru/safety и vms.drweb.ru.
2. После загрузки файла проверьте его на вирусы с помощью антивирусной программы. Это обеспечит безопасность вашего компьютера от потенциальных угроз. (См. Руководство пользователя при работе с антивирусным программным обеспечением и проверкой файлов);
3. Соблюдайте правила конфиденциальности и безопасности. Не передавайте важную информацию через открытые сети и не открывайте подозрительные ссылки или вложения от незнакомых отправителей по электронной почте.

В случае получения подозрительного письма от неизвестного отправителя, сообщите о нем на электронный адрес: **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 компьютере.
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».
Шаг 5. Дождитесь окончания проверки и получите результаты. Если файл содержит вирусы, Dr.Web предложит удалить их. Если файл чист, вы получите соответствующее сообщение.