Приложение № 2
к приказу ООО «Техно-Телеком»
от 02.10.2024 г. № 33

Положение по организации антивирусной защиты

1. Общие положения

1.1. Настоящее Положение определяет порядок приобретения, установки, настройки, обновления и использования средств антивирусной защиты в ООО «Техно-Телеком» (далее – Общество), а также обязанности и ответственность работников Общества.

1.2. Соблюдение требований настоящего Положения обязательно для всех работников Общества (далее – пользователи).

1.3. В настоящем Положении используются следующие термины и определения:

Автоматизированное рабочее место (АРМ) – комплекс средств вычислительной техники и программного обеспечения, предназначенный для выполнения определенных задач, приобретено на средства Общества и состоящий на бухгалтерском учете.

Локально-вычислительная сеть (ЛВС) – комплекс оборудования и программного обеспечения, обеспечивающий передачу, хранение и обработку информации.

Администратор ЛВС – технический работник отдела безопасности и режима.

Вредоносное программное обеспечение – программа, предназначенная для нанесения вреда (ущерба) обладателю информации, хранящейся на средстве вычислительной техники, путем ее несанкционированного копирования, уничтожения, модификации, блокирования или нейтрализации используемых на средстве вычислительной техники средств защиты информации, или для получения доступа к вычислительным ресурсам самого средства вычислительной техники с целью их несанкционированного использования.

Средство антивирусной защиты – программное средство, реализующее функции обнаружения вредоносных программ либо иной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

2. Организация антивирусной защиты

2.1. Для защиты информации, информационных ресурсов и систем Общества от вредоносных программ, их обнаружения, блокирования, изолирования и удаления используются средства антивирусной защиты.

2.2. Первичная проверка поступающей извне информации на наличие в ней вредоносного программного обеспечения осуществляется на программно-аппаратном комплексе, обеспечивающем подключение ЛВС Общества к сети Интернет.

2.3. Проверка входящих и исходящих сообщений электронной почты на наличие в них вредоносного программного обеспечения и спама, проверка хранилища почтовых сообщений осуществляется на корпоративном почтовом сервере.

2.4. Проверка открываемых, сохраняемых и запускаемых файлов, получаемых входящих и отправляемых исходящих сообщений электронной почты, открываемых веб-сайтов сети Интернет на наличие в них вредоносного программного обеспечения осуществляется на АРМ и серверах ЛВС Общества.

2.5. Приобретение, установка, настройка, обновление и контроль работоспособности средств антивирусной защиты в Обществе осуществляется работниками отдела безопасности и режима.

2.6. В Обществе разрешается использование лицензионных, централизовано приобретенных, управляемых средств антивирусной защиты.

2.7. На всех АРМ и серверах ЛВС Общества устанавливаются средства антивирусной защиты, если иное не предусмотрено технологическим процессом. Средства антивирусной защиты запускаются автоматически при включении оборудования.

2.8. Антивирусные базы средств антивирусной защиты в ЛВС Общества обновляются автоматически не реже одного раза в сутки.

2.9. Модули средств антивирусной защиты в ЛВС Общества обновляются автоматически после одобрения обновлений администратором ЛВС.

2.10. Проверка целостности модулей средств антивирусной защиты в ЛВС Общества на наличие повреждений или изменений выполняется автоматически не реже одного раза в неделю.

2.11. Антивирусная проверка важных областей (памяти, объектов автозапуска, системных папок) в ЛВС Общества выполняется автоматически ежедневно.

2.12. Полная антивирусная проверка (памяти, объектов автозапуска, всех внутренних дисков) в ЛВС Общества выполняется автоматически не реже одного раза в неделю.

2.13. Поиск уязвимостей и требуемых обновлений используемого программного обеспечения в ЛВС Общества выполняется автоматически не реже одного раза в неделю.

2.14. Установка требуемых обновлений и закрытие уязвимостей используемого программного обеспечения выполняется автоматически после одобрения обновлений администратором ЛВС.

2.15. В случае если после установки обновлений пользователю выдается сообщение о необходимости перезагрузки операционной системы, пользователь обязан перезагрузить АРМ до конца рабочего дня.

2.16. Пользователи обязаны не реже одного раза в неделю подключать АРМ к ЛВС Общества до завершения обновления средств антивирусной защиты, политик антивирусной безопасности, поиска уязвимостей и требуемых обновлений программного обеспечения, установки обновлений.

2.17. Администраторы ЛВС после установки или обновления программного обеспечения на АРМ или сервере ЛВС Общества запускают полную антивирусную проверку АРМ или сервера ЛВС Общества.

3. Использование средств антивирусной защиты

3.1. Работа на АРМ допускается только при работающем средстве антивирусной защиты.

3.2. Ежедневно перед началом работы на АРМ пользователи обязаны убедиться в успешности загрузки средства антивирусной защиты и актуальности антивирусных баз, подтверждением загрузки является наличие в правом нижнем углу на панели задач иконки используемого средства антивирусной защиты, дата обновления антивирусных баз отображается при наведении указателем мыши на иконку.

3.3. В случае если средство антивирусной защиты не загружено или антивирусные базы не обновлялись более двух дней, пользователь обязан создать заявку на техническую поддержку в отдел безопасности и режима в соответствии с Регламентом технической поддержки пользователей локально-вычислительной сети.

3.4. В случае если средство антивирусной защиты уведомляет пользователя об обнаружении вредоносного программного обеспечения в каком-либо файле, сообщении электронной почты или на сайте сети Интернет, пользователь обязан немедленно удалить вредоносный файл, сообщение

электронной почты, закрыть вредоносный сайт, после чего запустить полную антивирусную проверку АРМ.

3.5. При подключении носителей информации (флеш-карты, SD-карты, жесткие и твердотельные диски, оптические диски, мобильные устройства и др.) к АРМ пользователи обязаны проверить их средствами антивирусной защиты. Проверка запускается автоматически, пользователь обязан дождаться завершения проверки до начала работы с носителем информации.

3.6. В случае обнаружения на носителях информации вредоносного программного обеспечения, использование носителей информации разрешается только после удаления вредоносных программ.

3.7. Пользователи обязаны проверять средствами антивирусной защиты все сохраняемые на АРМ файлы, получаемые по каналам связи сети Интернет, через облачные сервисы, электронную почту. Для проверки необходимо выбрать действие проверить на вирусы в контекстном меню выделенных файлов.

3.8. В случае необходимости создания архивного файла пользователи перед архивированием обязаны проверить файлы средствами антивирусной защиты. Для проверки необходимо выбрать действие проверить на вирусы в контекстном меню выделенных файлов.

3.9. Пользователям запрещается:

- изменять настройки, отключать, приостанавливать, нарушать целостность, удалять средства антивирусной защиты;
- устанавливать какие-либо дополнительные средства антивирусной защиты;
- открывать файлы и ссылки, запускать программы, полученные от неизвестного отправителя, либо подозрительного содержания;
- загружать на АРМ и запускать исполняемые файлы с расширениями .exe, .bat, .vbs, .js, .scr, .com и др., файлы с двойными расширениями, например, document.pdf.exe, reglament.doc.js;
- отправлять, пересылать, копировать, запускать файлы и открывать ссылки, содержащие вредоносное программное обеспечение.

3.10. При возникновении подозрения на наличие вредоносного программного обеспечения на АРМ (ошибки при загрузке операционной системы, медленная работа, частые зависания и сбои АРМ, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, исчезновение файлов и папок и т.п.) пользователь обязан немедленно отключить АРМ от ЛВС Общества, запустить полную антивирусную проверку АРМ, уведомить администратора ЛВС.

3.11. В случае обнаружения на АРМ или сервере ЛВС Общества вредоносного программного обеспечения администратор ЛВС с использованием средств антивирусной защиты и специализированного программного обеспечения выполняет удаление вредоносного программного обеспечения в режиме лечение. В случае если лечение не возможно – удаляет поврежденные файлы с их последующим восстановлением из резервных копий (при наличии). Запускает полную внеплановую антивирусную проверку ЛВС Общества.

4. Ответственность

4.1. Ответственность за выполнение мероприятий в соответствии с требованиями настоящего Положения в структурных подразделениях возлагается на руководителей структурных подразделений.

4.2. Ответственность за выполнение мероприятий в соответствии с требованиями настоящего Положения на АРМ возлагается на пользователей АРМ.

4.3. Ответственность за выполнение мероприятий в соответствии с требованиями настоящего Положения в ЛВС Общества возлагается на администраторов ЛВС.

4.4. Работники Общества, нарушившие требования настоящего Положения могут быть привлечены к ответственности в соответствии с действующим законодательством и локальными нормативными актами Общества.

4.5. Форма и степень ответственности определяется исходя из вида и размера ущерба, нанесенного Обществу действиями либо бездействием соответствующего работника.

4.6. Отдел безопасности и режима контролирует исполнение работниками Общества требований настоящего Положения.

4.7. О выявленных нарушениях настоящего Положения начальник отдела безопасности и режима докладывает генеральному директору Общества и заместителю генерального директора Общества по безопасности.

4.8. Работники Общества должны быть ознакомлены с настоящим Положением под роспись в журнале ознакомления.

Начальник отдела безопасности и режима Б.Б. Бобурченко
ООО «Техно-Телеком»

СОГЛАСОВАНО
Заместитель генерального директора Р.Р. Ромашков
ООО «Техно-Телеком»