ПРАВИЛА
ОРГАНИЗАЦИИ АНТИВИРУСНОГО КОНТРОЛЯ

Астана
2023 г.

1. Термины и сокращения

Организация – ОЮЛ Ассоциация ВИЭ «Qazaq Green»;

Правила – Правила организации антивирусного контроля.

Специалист по информационной безопасности – сотрудник Организации, ответственный за обеспечение защиты информационных ресурсов и обеспечение информационной безопасности Организации;

Антивирус – специальное программное обеспечение, которое обеспечивает защиту от вирусов и других вредоносных программ;

Компьютерный вирус – это специально написанная программа (т.е. некоторая совокупность выполняемого кода), которая может «приписывать» себя к другим программам («заражать» их) создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере;

Вредоносное программное обеспечение – это любое программное обеспечение, предназначенное для получения несанкционированного доступа к информации и/или с целью причинения иного вреда (ущерба) Организации и/или пользователю ПК;

Пользователь – лицо, участвующее в функционировании корпоративной вычислительной сети Организации и использующее информационные ресурсы Организации.

ПК – персональный компьютер.

2. Общие Правила

1. Настоящие Правила определяют требования к организации антивирусной защиты информационных ресурсов корпоративной вычислительной сети Организации от разрушающего воздействия компьютерных вирусов и вредоносного программного обеспечения; устанавливает ответственность работников Организации – пользователей персональных компьютеров, подключенных к информационным ресурсам корпоративной вычислительной сети Организации, Специалиста по информационной безопасности.

2. Работоспособность, эффективность антивирусной защиты, выполнение требований к ее организации обеспечивается системным администратором.

3. Установка и обновление антивирусных средств

3. Антивирусные программы необходимы для:

1) защиты информационных ресурсов от заражения вирусами;

2) выявления и восстановления файлов, зараженных вирусами;

3) поддержания в актуальном состоянии серверов, различных сервисов, эксплуатируемых задач и систем.

4. К использованию в Организации допускаются только лицензионные антивирусные средства, закупленные самостоятельно.

5. Обязательному антивирусному контролю подлежит любая информация, получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях.

6. Антивирусные программы устанавливаются системным администратором на все персональные компьютеры и сервера корпоративной вычислительной сети Организации.

7. Настройка антивирусных средств должна обеспечивать:

1) при каждой перезагрузке компьютера (для серверов – при перезапуске) автоматический запуск антивирусного монитора;

2) в определенное время дня полную антивирусную проверку (сканирование) локальных дисков, установленных на компьютере;

3) обновление антивирусных баз в определенное время дня;

4) лечение зараженных вирусов файлов или удаление при невозможности лечения.

5) проверку web-страниц на наличие вредоносного кода.

6) выполнять проверку вложений электронной почты и файлов, полученных из общедоступных сетей, на наличие вирусов

4. Порядок проведения антивирусного контроля

8. Установка (изменение) системного и прикладного обеспечения компьютеров и локальной вычислительной сети должна осуществляться только в присутствии системного администратора.

9. Устанавливаемое (изменяемое) на компьютер программное обеспечение должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

10. Установка, настройка, конфигурирование параметров, администрирование средств антивирусного контроля на компьютерах (серверах ЛВС) осуществляется системным администратором, в соответствии с руководствами по применению конкретных антивирусных средств.

11. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация со съемных носителей (магнитные диски, CD-ROM, флешки и т.п.), получаемых от сторонних лиц и организаций

12. Контроль информации на съемных носителях производится непосредственно перед ее использованием

13. Особое внимание следует обратить на съемные носители (флеш-карты, компакт-диски), принадлежащие лицам, временно допущенным к работе на ПК в Организации (студенты-практиканты, временно замещающие и т.п.). Работа этих лиц должна проводиться под непосредственным контролем со стороны работников Организации, особенно если работа происходит с использованием ресурсов локальной вычислительной сети.

14. Пользователю на своем персональном компьютере запрещено:

1) изменять настройки и конфигурацию антивирусных приложений;
2) удалять или добавлять какие-либо антивирусные программы;
3) работать со съемными носителями без предварительной их проверки, установленной на персональном компьютере антивирусной программы;
4) запускать неизвестные приложения, пришедшие по электронной почте.

15. Пользователь обязан:

1) ежедневно в начале работы при загрузке компьютера убедиться в наличии резидентного (находящегося в оперативной памяти компьютера) антивирусного монитора (справа на панели задач должен быть значок с логотипом программы антивирусной защиты и всплывающим над ним наименованием этой программы), и в случае его отсутствия уведомить об этом системного администратора.

2) самостоятельно запускать внеплановую антивирусную проверку локальных дисков своего персонального компьютера при получении уведомления от службы информационных технологий о наличии вируса в корпоративной вычислительной сети Организации, а также при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);

3) в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, незамедлительно сообщить об этом системного администратора.

16. Системный администратор обязан:

1) устанавливать антивирусные программы на персональных компьютерах и серверах и инструктировать пользователей по произведенным настройкам;

2) контролировать состояние серверов и корпоративной сети на наличие вирусов;

3) рассылать всем пользователям предупреждение о проникновении в корпоративную сеть вирусов и указания по проведению мер антивирусной защиты;

17.Системный администратор, ответственный за антивирусную защиту, обязан:

1) обеспечить автоматический мониторинг ежедневного обновления антивирусных баз;

3) проводить не реже одного раза в неделю анализ работы антивирусного шлюза;

4) составлять расписания и порядок работы модулей антивирусной программы;

5) контролировать состояние антивирусной защиты в корпоративной сети Организации, а также выполнение требований настоящего Правила пользователями;

6) незамедлительно оповещать специалиста по информационной безопасности о факте обнаружения заражения вирусом корпоративной сети, предположительный источник зараженного файла (сообщения), характер содержащейся в файле (сообщении) информации и выполняемых антивирусных мероприятиях.

18. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль загрузочных файлов ПК.

19. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных (отчуждаемых) носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема или при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо «чистой» (не зараженной вирусами) и защищенной от записи системного диска, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо

проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

20. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

21. Системный администратор обязан не реже одного раза в неделю предоставлять репозитории с антивирусными базами для обновления антивирусных баз в организации.

22. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов системный администратор обязан:

- приостановить работу;
- отключить зараженный ПК от локальной сети;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на сайт производителя антивируса, по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

23. Ответственность за организацию антивирусного контроля в Организации, в соответствии с требованиями настоящего Правила возлагается на системного администратора.

24. Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований Правила возлагается на системного администратора.

5. Контроль соблюдения Правила

25. Контроль соблюдения настоящего Правила осуществляет, Специалист по информационной безопасности.

26. За нарушение норм настоящего Правила, к работникам Организации по представлению Специалиста по информационной безопасности, могут быть применены меры дисциплинарного взыскания.

6. Рассылка

С данным Правилам знакомятся все сотрудники Организации под роспись (далее - Лист ознакомления).

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Личная подпись	Дата
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				