Приложение 12
к Положению об
информационной безопасности

ПРАВИЛА ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

1. Общие положения

1. Настоящие Правила организации антивирусной защиты (далее Правила) в НАО «Евразийский Национальный Университет им. Л.Н. Гумилева» (далее Университет), регламентируют требования к организации защиты информационных ресурсов корпоративной сети передачи данных от воздействия вредоносного программного обеспечения (ПО) и определяют права, обязанности и ответственности пользователей.

2. При разработке настоящих Правил использовались следующие стандарты:

1) СТ РК ИСО/МЭК 17799-2006 Методы обеспечения защиты. Свод правил по управлению защитой информации;

2) СТ РК ИСО/МЭК 27001-2015 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности;

3) СТ РК 51188-2007 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Общие требования.

2. Определения и сокращения

3. В настоящих Правилах используются следующие термины, определения и сокращения:

1) Университет - НАО «Евразийский Национальный Университет им. Л.Н. Гумилева»

2) Администратор сервера – работник Университета, отвечающий за настройку серверной части антивирусного ПО;

3) Антивирусное ПО - программное обеспечение, предназначенное для обнаружения компьютерных вирусов, а также нежелательных вредоносных ПО и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики, предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

4) Вредоносное ПО - разновидность программного обеспечения со способностью к размножению (саморепликации) либо без таковой, используемая злоумышленником для сбора информации, ее разрушения или модификации, нарушения работоспособности компьютерной техники или использования его ресурсов в неблаговидных целях;

5) КСПД - корпоративная сеть передачи данных;

6) КВ - компьютерный вирус;

7) Компонента - часть автоматизированной системы, выделенная по определенному признаку или совокупности признаков и рассматриваемая как единое целое;

8) Пользователь - обучающийся или работник Университета, работник организации Университета;

9) Департамент информатизации - осуществляющее сервис в области внедрения информационных технологий.

10) Служба технической поддержки пользователей - подразделение Университета, осуществляющее сопровождение и эксплуатацию инфокоммуникационной инфраструктуры;

11) Отдел информационной безопасности – подразделение Университета осуществляющее контроль информационной безопасности в области информационных систем и технологий;

12) СВТ – средства вычислительной техники (портативные персональные компьютеры, рабочие станции, серверы, переносные устройства, ноутбуки, планшеты, коммуникаторы, мобильные телефоны, смартфоны и т.д.);

3. Установка и обновление средств защиты

4. К использованию в Университете допускается только лицензионное антивирусное ПО.

5. Антивирусная программа устанавливается в обязательном порядке, на все служебные СВТ, специалистом Службы технической поддержки пользователей.

6. Обучающиеся Университета за свой счет устанавливают и обновляют антивирусную программу на личных СВТ. Они могут получить рекомендации, а также помощь по настройке и обновлению антивирусной программы, подав заявку в соответствии с принятыми в Университете процедурами подачи заявок в Службу технической поддержки пользователей.

7. Настройка антивирусной программы должна включать в себя:

1) возможность автоматического запуска;
2) периодическое плановое сканирование по заданным параметрам;
3) возможность автоматического обновления программных компонент;
4) способность выявления и устранения выявленных угроз;
5) автоматическое сканирование съемных носителей при подключении.

4. Порядок проведения антивирусного контроля

8. Установка (изменение) пользователем системного и прикладного обеспечения компьютеров и выделенной сети должна осуществляться только в присутствии работника Службы технической поддержки пользователей.

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

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

11. Контроль информации на съемных носителях производится пользователем, непосредственно перед ее использованием.

12. Особое внимание следует обратить на съемные носители (USB-накопители, компакт-диски и т.д.).

5. Методы проведения испытаний программных средств на наличие компьютерных вирусов

13. При испытаниях программных средств на наличие КВ должны использоваться две группы методов обнаружения КВ и защиты программ от них: программные и аппаратно-программные.

К программным методам относятся:

1) сканирование;
2) обнаружение изменений;
3) эвристический анализ;
4) резидентные «сторожа»;
5) вакцинирование программных средств.

14. Аппаратно-программные методы основаны на реализации любого (любых) из указанных выше программных методов защиты программных средств от КВ с помощью специальных технических устройств.

15. В конкретных испытаниях могут быть использованы способы и средства обнаружения КВ, реализующие один из методов, в соответствии со СТ РК 51188-2007 или их комбинации.

6. Ограничения, права и обязанности пользователей

16. Ограничения для пользователей Университета:

1) запрещается изменять настройки и конфигурацию антивирусных программ, установленных на служебных устройствах СВТ;

2) запрещается использовать личные устройства СВТ, в КСПД без антивирусного ПО, тем самым, подвергая инфраструктуру Университета возможному риску распространения вредоносного ПО;

3) запрещается удалять антивирусные программы, установленные на служебных СВТ;

4) не рекомендуется работать со съемными носителями информации (USB-накопители, CD/DVD-диски), без предварительной их проверки антивирусной программой;

5) не рекомендуется запускать неизвестные приложения, получаемые по электронной почте, на съемном носителе, в файловых ресурсах КСПД, сомнительные ссылки, сайты на интернет-ресурсе;

17. Пользователь обязан:

1) не препятствовать работе антивирусной программы, выполняющей процедуру сканирования в запланированном режиме;

2) самостоятельно запускать внеплановую антивирусную проверку на устройствах СВТ 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 вируса, не поддающегося лечению антивирусной программой, незамедлительно сообщить об этом в Службу технической поддержки пользователей.

18. Пользователь имеет право:

1) обращаться в Службу технической поддержки пользователей в соответствии с принятыми в Университете процедурами подачи заявок, обращений;

2) получать необходимые консультации (инструктаж, рекомендации), инструкции, материалы по работе с антивирусной программой, от Службы технической поддержки пользователей.

7. Обязанности, права Службы технической поддержки пользователей, а также администратора сервера

19. Работники Службы технической поддержки пользователей, администратор сервера, осуществляя работу, согласно своим функциям обязаны:

1) своевременно применять меры по защите серверного и прикладного программного обеспечения КСПД от проникновения вредоносных кодов и хакерских атак;

2) устанавливать и настраивать только лицензионные антивирусные программы на устройствах СВТ и инструктировать пользователей по вопросам эксплуатации;

3) при первых признаках обнаружения хакерских атак, вредоносного ПО, рассылать пользователям предупреждение и принимать все необходимые меры по защите КСПД, информационных ресурсов;

4) проводить инструктаж по работе с антивирусной программой на устройствах СВТ по заявке пользователя;

5) обеспечивать своевременное обновление антивирусных баз и программных компонент антивирусного ПО на серверах;

6) составлять расписания и порядок работы модулей антивирусного ПО;

7) осуществлять проверку всех файлов на электронных или оптических носителях информации на общедоступных ресурсах;

8) осуществлять проверку любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения на серверах электронной почты, или при входе в сеть Университета;

9) осуществлять проверку web-страниц на наличие вредоносного кода;

10) информировать пользователей о разновидностях вирусов и действиях при их получении;

11) проводить анализ работы серверного антивирусного ПО.

20. Работники Службы технической поддержки: пользователей, администратор сервера имеют право:

1) требовать от пользователей соблюдения пунктов настоящих Правил;

2) информировать устно или письменно о нарушении пользователем пунктов настоящих Правил руководителя структурного подразделения, в котором работает работник, а также Отдел информационной безопасности;

3) приостанавливать работу пользователя при неоднократных нарушениях им пунктов настоящих Правил (более 3-х раз) при согласовании с непосредственным руководителем работника и Отделом информационной безопасности в целях проведения служебного расследования.

8. Заключительные положения

21. Ознакомление пользователей Университета и его организаций с настоящими Правилами проводится руководителями структурных подразделений Университета, а также Отделом информационной безопасности с оформлением подписи в «Листе ознакомления к Правилам организации антивирусной защиты в Университете (Приложение 1).

22. Пользователи, нарушившие требования настоящих Правил, могут быть привлечены к ответственности в соответствии с законодательством Республики Казахстан и внутренними документами Университета.