«УТВЕРЖДЕНО»
Решением Правления
НАО «Университет Нархоз»
Протокол №_8_от
«_15_»._06_.20_23_ г.

Правила организации антивирусного контроля информационных ресурсов IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Правила организации антивирусного контроля информационных ресурсов IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Краткое описание:	Правила организации антивирусного контроля информационных ресурсов IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Тема:	Информационная безопасность
Статус:	Новый
Дата утверждения:	«___» _____2023г.
Дата завершения действия:	
Дата аудита:	Ежедневно
Ответственный за аудит:	Эксперт по информационной безопасности

Лист согласования

Должность	Ф.И.О.	Подпись
Директор Административного департамента	Бисенгали Л	
Советник по цифровизации	Тебаев Д.Б.	
и.о. Директора Департамента информационных технологий	Жумажанов Б.Ж.	

1 Общие положения

1.1 Настоящие Правила организации антивирусного контроля информационных ресурсов IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз» (далее – «Правила») определяют требования к организации антивирусной защиты информационных ресурсов IT инфраструктуры НАО «Университет Нархоз» (далее – Общество») от воздействия компьютерных вирусов и вредоносного программного обеспечения и устанавливает ответственность пользователей персональных компьютеров, подключенных IT инфраструктуре НАО «Нархоз» (далее – «ITA»).

1.2 Защита от вредоносного программного обеспечения представляет собой действия, обеспечивающие предотвращение проникновения вредоносного программного обеспечения (далее – «вирусы») к информационным системам и ресурсам организации посредством использования антивирусных средств.

2 Ссылки

2.1 Настоящие Правила разработаны в соответствии со следующими нормативно-правовыми актами и документами:

- Закон Республики Казахстан «Об информатизации» от 24.11.2015г.;
- Постановление Правительства Республики Казахстан от 20.12.2016г.№832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;
- СТ РК ИСО/МЭК 27002 «Методы обеспечения защиты. Свод правил по управлению защитой информации»;
- СТ РК ИСО/МЭК 27001 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- СТ РК ГОСТ Р 50739 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

3 Порядок проведения контроля от проникновения вредоносного программного обеспечения

3.1 Порядок проведения контроля от проникновения вредоносного программного обеспечения:

- к использованию допускается только лицензионные средства для защиты от проникновения вредоносного программного обеспечения;
- программы по защите от проникновения вредоносного программного обеспечения устанавливаются на все компьютеры и сервера корпоративной вычислительной сети с обязательным предохранением настроек от изменения паролем;
- в начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление баз сигнатур;
- пользователям запрещается отключать средства защиты и самостоятельно вносить изменения в настройки программного обеспечения (далее – «ПО»);
- актуализация баз сигнатур должна осуществляться ежедневно (по рабочим дням) в автоматическом режиме через серверы обновлений;
- периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей – ежедневно, в ночное время по расписанию;

3.2 Внеочередной контроль всех дисков и файлов персонального компьютера должен выполняться:

• 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.);

• при отправке и получении электронной почты проверять электронные письма и их вложения на наличие вирусов.

3.4 В случае обнаружения зараженных файлов или электронных писем пользователи обязаны:

• приостановить работу;

• немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты;

• совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

• провести лечение или уничтожение зараженных файлов;

• в случае отсутствия возможности восстановления информации необходимо провести мероприятия согласно Регламенту резервного копирования и восстановления информации ITA Общества;

• 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 (магнитные диски, ленты, CD-ROM, флеш носители и т.п.), получаемых от сторонних лиц и организаций;

• контроль информации на съемных носителях производится непосредственно перед ее использованием;

• особое внимание следует обратить на съемные носители (флэшки, компакт-диски), принадлежащие лицам, временно допущенных к работе на рабочих станциях пользователей (студенты- практиканты, временно замещающие работники и т.п.). Работа этих лиц должна проводиться под непосредственным контролем, особенно если работа происходит с использованием ресурсов локальной вычислительной сети.

3.5 Пользователю на своем персональном компьютере запрещено:

• изменять настройки и конфигурацию антивирусных приложений;

• удалять или добавлять какие-либо антивирусные программы;

• работать со съемными дисками без предварительной их проверки, установленной на персональном компьютере антивирусной программы;

• запускать неизвестные приложения, пришедшие по электронной почте.

4 Защита от вредоносного и подвижного кода

4.1 Необходимо принимать меры предотвращения и обнаружения внедрения вредоносного кода и несанкционированного подвижного кода.

4.2 Программное обеспечение и средства обработки информации уязвимы к внедрению вредоносного программного обеспечения. Администраторы ITA Общества должны быть осведомлены об опасности использования неавторизованного или вредоносного программного обеспечения, а соответствующие руководитель ДИТ должен обеспечить внедрение специальных средств контроля с целью обнаружения и/или предотвращения проникновения подобных программ. В частности, важно принятие мер предосторожности с целью обнаружения и предотвращения заражения компьютерными вирусами персональных компьютеров.

4.3 С целью обнаружения и предотвращения проникновения вредоносного ПО, эксперт по ИБ должен планировать мероприятия по управлению информационной безопасностью, а также формирование процедур, обеспечивающих соответствующую осведомленность пользователей. Защита от вредоносного программного обеспечения должна основываться на понимании требований безопасности, соответствующих мерах контроля доступа к системам

и надлежащем управлении изменениями. Ниже перечислены основные и наиболее эффективные меры защиты от вредоносного кода:

• документированную политику защиты от рисков, связанных с получением файлов и программного обеспечения из внешних сетей, через внешние сети или из любой другой среды;

• установку и регулярное обновление антивирусного программного обеспечения для обнаружения и сканирования компьютеров и носителей информации, запускаемого в случае необходимости в качестве превентивной меры или рутинной процедуры;

• проверку всех файлов на носителях информации сомнительного или неавторизованного происхождения, или файлов, полученных из общедоступных сетей, на наличие вирусов перед работой с этими файлами;

• проверку любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования;

• проверку web-страниц на наличие вредоносного кода;

• определение управленческих процедур и обязанностей, связанных с защитой от вредоносного кода, обучения применению этих процедур, а также вопросов оповещения и восстановления после атак вредоносного кода;

• реализация процедур регулярного сбора такой информации, как подписка на список адресатов и/или проверку web-сайтов, предоставляющую информацию о новом вредоносном коде.

4.4 Подвижный код является кодом программного обеспечения, который переходит из одного компьютера в другой, затем автоматически реализуется и выполняет специфическую функцию с незначительным участием пользователя или вообще без него. Подвижный код связан с несколькими промежуточными программными обеспечениями.

4.6 При наличии санкционированного подвижного кода конфигурация должна обеспечить функционирование санкционированного подвижного кода в соответствии с четко определенной политикой безопасности, а подвижный несанкционированный код должен быть защищен от реализации.

4.7 Для защиты от подвижного кода, выполняющего несанкционированные действия, администратор ITA Общества должен рассмотреть следующие меры:

• реализацию подвижного кода в логически изолированной среде;

• блокирование использования подвижного кода;

• блокирование приёма подвижного кода;

• задействование технических мер, предусмотренных в специальных системах, для обеспечения управления подвижным кодом;

• контроль за ресурсами, доступными для подвижного кода;

• применение криптографических средств контроля для определения подлинности подвижного кода.

5 Ответственность

4.1 Все пользователи IT инфраструктуры обязаны соблюдать политику использования антивирусного программного обеспечения и соблюдать меры безопасности, связанные с антивирусной защитой.4.2 Администраторы системы обязаны устанавливать, обновлять и настраивать антивирусное программное обеспечение на всех устройствах IT инфраструктуры.

4.3 Администраторы системы обязаны проводить регулярные проверки на наличие вирусов и вредоносного программного обеспечения, а также предпринимать меры по их удалению или карантинированию.

4.4 Администраторы системы должны обеспечить резервное копирование важных данных и системных файлов с целью предотвращения потери данных в результате вирусной атаки.

4.5 Пользователи должны немедленно сообщать обнаруженные подозрительные или вредоносные файлы, или активности администраторам системы.

6 Заключительные положения

6.1 Администраторы системы должны регулярно мониторить и обновлять список известных вредоносных программ, а также следить за актуальностью антивирусных баз данных.

6.2 В случае обнаружения серьезных уязвимостей или новых видов вредоносного программного обеспечения, администраторы системы должны принять срочные меры по обеспечению безопасности IT инфраструктуры и информационных ресурсов.

6.3 После проведения антивирусного контроля информационных ресурсов IT инфраструктуры, необходимо провести анализ результатов и составить отчет о выявленных уязвимостях и предпринятых мерах по обеспечению безопасности.

6.4 Руководство организации должно рассмотреть отчет и принять дополнительные меры по улучшению антивирусного контроля и обеспечению безопасности информационных ресурсов.

6.5 Проведение периодического антивирусного контроля является обязательным и должно выполняться в соответствии с установленным графиком.

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Подпись	Дата
1	2	3	4	5