



**«УТВЕРЖДЕНО»**  
**Решением Правления**  
**НАО «Университет Нархоз»**  
**Протокол № \_\_\_\_\_ от**  
**«\_\_» \_\_\_\_\_ 20\_\_ г.**

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

Алматы, 2023

Оглавление

Паспорт документа .....	3
Лист согласования.....	4
1. Общие положения .....	5
2. Ссылки.....	5
3. Порядок проведения контроля от проникновения вредоносного программного обеспечения .....	5
4. Защита от вредоносного и подвижного кода .....	7

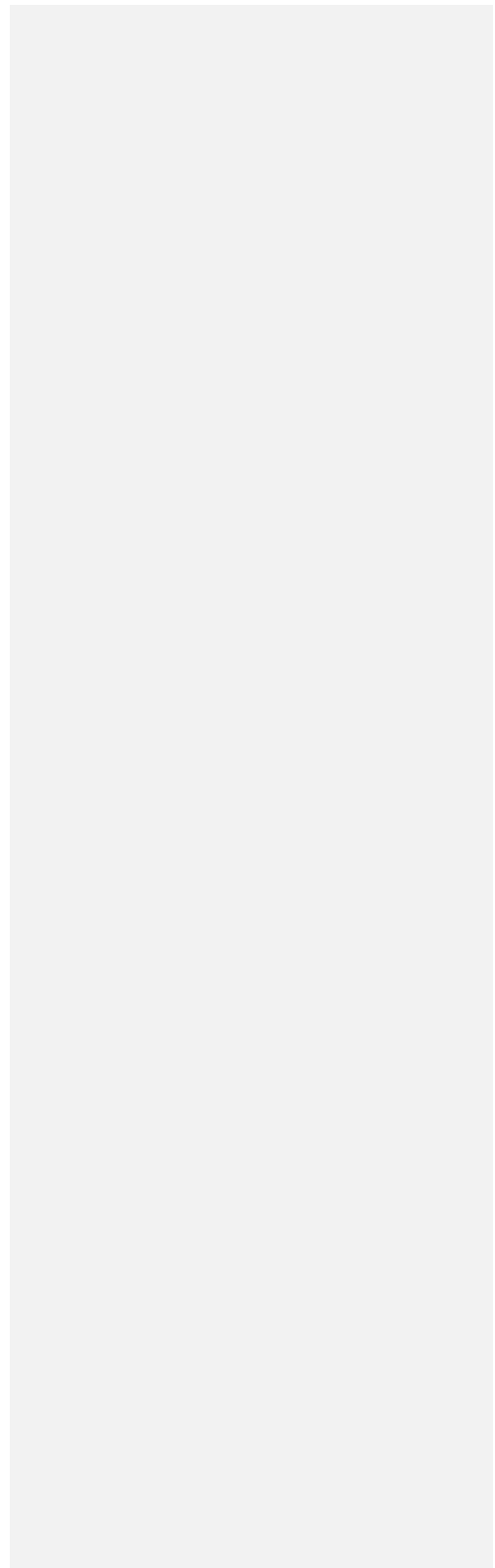
## Паспорт документа

---

<b>Наименование документа:</b>	Правила организации антивирусного контроля информационных ресурсов ИТ инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
<b>Краткое описание:</b>	Правила организации антивирусного контроля информационных ресурсов ИТ инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
<b>Тема:</b>	Информационная безопасность
<b>Статус:</b>	Новый
<b>Дата утверждения:</b>	«__» _____ 2023г.
<b>Дата завершения действия:</b>	
<b>Дата аудита:</b>	Ежедневно
<b>Ответственный за аудит:</b>	Эксперт по информационной безопасности

~~Лист согласования~~

Лист согласования



## 1 Общие положения

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

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 ~~Настоящий документ~~ Настоящие Правила разработаны в соответствии со следующими нормативно-правовыми актами и документами:

- Закон Республики Казахстан «Об информатизации» от 24.11.2015г., ~~ноября 2015 года № 418-V~~;
- Постановление Правительства Республики Казахстан от 20.12.2016г., ~~декабря 2016 года № №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

Отформатировано: справа: 1,5 см, Расстояние от края до нижнего колонтитула: 1,53 см

Отформатировано: Шрифт: 12 пт

Отформатировано: По центру

Отформатировано

Отформатировано

Отформатировано: Шрифт: 12 пт

Отформатировано: По центру

Отформатировано

Отформатировано: Шрифт: 12 пт

Отформатировано

Отформатировано: По центру

Отформатировано

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.

**3.5.3.4** 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 ИТА НАО «Нархоз» 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 (флэш-ки, компакт-диски), принадлежащие лицам, временно допущенным 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.

**3.6.3.5** 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**

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

4.5 Программное обеспечение и средства обработки информации уязвимы к внедрению вредоносного программного обеспечения. Администраторы ИТА НАО «Нархоз» 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.

4.6 С целью обнаружения и предотвращения проникновения вредоносного ПО, эксперт по ИБ должен планировать мероприятия по управлению информационной

Отформатировано: Шрифт: 12 пт

Добавлено примечание (ЛБ1): Добавить разделы Ответственность и Заключительные положения

Отформатировано: Шрифт: 12 пт

Отформатировано: По центру

Отформатировано: Шрифт: 12 пт

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.

4.7 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.

4.8 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.

4.9 Для защиты от подвижного кода, выполняющего несанкционированные действия, администратор ИТА [НАО «Наржэз» 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.

Отформатировано: Шрифт: 12 пт

