NAZARBAYEV UNIVERSITY

Правила применения антивирусной защиты в автономной организации образования «Назарбаев Университет» и ее организациях

Категория: Правила

Дата утверждения: 03.06.2025

Дата вступления в силу: 03.06.2025

Уровень доступа: Публичный доступ

Номер по классификатору: 7. IT

Утверждающий орган: Управляющий совет

Регистрационный номер: 03.06.25

Владелец: Частное учреждение «Nazarbayev University IT Support»

Дата пересмотра: 05.06.2028

Применение: НУ и его организации

Утратившие силу документы:

Наименование: Правила организации антивирусной защиты в автономной организации образования «Назарбаев Университет»

Дата: 25.04.2013

Регистрационный номер: 4.4.1

Утверждающий орган: Исполнительный совет

Раздел 1. Цель и применение

1.1 Настоящие Правила применения антивирусной защиты в автономной организации образования «Назарбаев Университет» и ее организациях (далее – Правила) регламентируют требования к организации защиты виртуальных и физических серверов и корпоративных устройств автономной организации образования «Назарбаев Университет» (далее – Университет) от вредоносного программного обеспечения.

1.2 Целью настоящих Правил является обеспечение надлежащей защиты виртуальных и физических серверов и корпоративных устройств Университета от вредоносного программного обеспечения.

1.3. Действие и требования настоящих Правил распространяются на все виртуальные и физические сервера и корпоративные устройства Университета, а также личные устройства физических лиц, подключенные к корпоративной сети Университета и его организаций.

Раздел 2. Термины / Определения

2.1. В настоящих Правилах применяются следующие термины, определения и сокращения:

1) **Администратор сервера** – работник структурного подразделения Университета или его организации, обеспечивающий настройку и поддержку физического или виртуального сервера, а также обеспечивающий безопасность корпоративных устройств Университета;

2) **Антивирусное ПО** – программное обеспечение или набор программных обеспечений, предназначенных для обнаружения, предотвращения распространения и удаления вредоносного программного обеспечения (вирусов, троянов, шпионских программ и других видов вредоносных программных обеспечений) с компьютеров и других корпоративных устройств;

3) **Вредоносное ПО** – это любое программное обеспечение, разработанное с целью нанесения вреда, получения несанкционированного доступа, нарушения работы систем, кражи данных или совершения других злонамеренных действий на компьютерах, серверах, мобильных устройствах или в сетях;

4) **Корпоративное устройство** – компьютер или иное устройство Университета, на котором находятся данные, включая виртуальные машины, развернутые на серверах Университета;

5) **Корпоративная сеть** – частная вычислительная сеть Университета, объединяющая её информационные ресурсы, пользователей, устройства и системы для обеспечения безопасного обмена данными, совместной работы и управления бизнес-процессами;

6) **Объекты защиты -** виртуальные и физические сервера, а также корпоративные устройства, подлежащие защите от вредоносных ПО;

7) **Пользователь** – лицо, имеющее в распоряжении корпоративное устройство, которое находятся на балансе Университета, а также лицо чье

личное устройство подключено к Корпоративной сети Университета;

8) **Учреждение –** частное учреждение «Nazarbayev University IT Support», отвечающее за техническую поддержку и сопровождение информационных систем и пользователей Университета и его организаций.

2.2. Термины, применяемые, но не определенные настоящими Правилами, используются в том смысле, в котором они используются в законодательстве Республики Казахстан и внутренних нормативных документах Университета.

Раздел 3. Основные положения

3.1. Установка Антивирусного ПО

3.1.1. К использованию в Университете допускается только лицензионное Антивирусное ПО, одобренное Службой информационной безопасности Учреждения.

3.1.2. Для Объектов защиты применяются средства защиты, закупаемые Службой информационной безопасности Учреждения.

3.1.3. Антивирусное ПО устанавливается в обязательном порядке на все Объекты защиты работниками Учреждения или Администраторами сервера.

3.1.4. В случае затруднения установки Антивирусного ПО, Администраторы могут направить заявку в службу технической поддержки – на портал IT Helpdesk Университета (https://helpdesk.nu.edu.kz/support/home).

3.1.5. Если Пользователь подключает личное устройство к Корпоративной сети, на нем должно быть установлено любое функционирующее Антивирусное ПО актуальной версии.

3.1.6. В случае использования личного устройства, подключенного к Корпоративной сети, без наличия установленного Антивирусного ПО, Служба информационной безопасности Учреждения имеет право отключить такое устройство от Корпоративной сети.

При этом, владельцу такого личного устройства будет направлено соответствующее уведомление посредством корпоративной электронной почты.

3.1.7. В случае невозможности установки Антивирусного ПО по техническим или иным объективным причинам, Пользователь обязан согласовать «исключение» для устройства со Службой информационной безопасности Учреждения, предоставив письменное обоснование, и обеспечив альтернативные меры защиты.

3.2. Ограничения, права и обязанности Пользователей

3.2.1. Ограничения для Пользователей:

1) запрещается изменять, удалять Антивирусное ПО, установленное на Объектах защиты;

2) запрещается использовать Корпоративные устройства без Антивирусного ПО;

3) не рекомендуется использование съемных носителей информации без предварительной их проверки Антивирусным ПО;

4) запрещается открывать файлы (в т.ч. пиратские копии ПО), полученные от неизвестных или неблагонадежных источников/сайтов или отправителей.

5) запрещается препятствовать работе Антивирусного ПО, выполняющего процедуру сканирования Корпоративного устройства на наличие Вредоносного ПО;

3.2.2. Пользователю требуется самостоятельно запускать внеплановую проверку Антивирусным ПО на Объектах защиты при возникновении подозрения на наличие Вредоносного ПО (нетипичная работа программ, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и других признаков заражения).

3.2.3. В случае обнаружения Вредоносного ПО, не поддающегося воздействию Антивирусного ПО, Пользователь должен незамедлительно направить соответствующую заявку Службе информационной безопасности Учреждения.

3.3. Ответственность за нарушения

3.3.1. Пользователи должны соблюдать требования настоящих Правил. В случае нарушения требования настоящих Правил Пользователи могут быть привлечены к ответственности.

3.3.2. В зависимости от характера и тяжести нарушения, в том числе, могут применяться следующие меры:

1) предупреждение – в случае первого нарушения, если оно не привело к существенным последствиям;

2) ограничение доступа – временная блокировка Корпоративного устройства до устранения нарушения.

3.3.3. Контроль за соблюдением требований настоящих Правил осуществляется Службой информационной безопасности Учреждения.

Раздел 4. Освобождение

4.1. Неприменимо.

Раздел 5. Временные положения

5.1. Неприменимо.

Раздел 6. Пересмотр

6.1. Настоящие Правила должны проверяться каждый год в течение трех лет после их утверждения и пересматриваться при необходимости

Раздел 7. Взаимосвязанные документы

7.1. Неприменимо.