Министерство здравоохранения Республики Беларусь
Учреждение образования «Витебский государственный ордена Дружбы народов медицинский университет»

УТВЕРЖДЕНО
Ректором учреждения образования «Витебский государственный ордена Дружбы народов медицинский университет»
А.Н.Чукановым

Политика по организации антивирусной защиты

31 декабря 2025 № 02-08/65

г. Витебск

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика по организации антивирусной защиты (далее – Политика) является внутренним нормативным документом, который определяет требования к организации антивирусной защиты в учреждении образования «Витебский государственный ордена дружбы народов медицинский университет» (далее – Университет).

1.2. Документ разработан на основании:

1.2.1. Указа Президента Республики Беларусь от 16.04.2013 № 196 (защита информации);

1.2.1. Приказа ОАЦ от 20.02.2020 № 66 (технические требования к защите);

1.2.1. Закона Республики Беларусь № 99-З «О защите персональных данных» (в части обеспечения конфиденциальности и целостности данных обучающихся и персонала).

1.3 Действие настоящей Политики распространяется на все структурные подразделения Университета.

ГЛАВА 2
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств (далее – ИС).

2.2. Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах (далее – ИР).

2.3. Пользователь – физическое лицо, получившее в установленном порядке доступ к ИС, ИР и (или) информационной сети и пользующееся ими.

2.4 Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ресурсы информационных систем. Вредоносная программа способна выполнять ряд функций, в том числе: скрывать признаки своего присутствия в программной среде; обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти; разрушать (искажать произвольным образом) код программ в оперативной памяти; сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных); искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

2.5 В целях обеспечения защиты ИС от деструктивных воздействий компьютерных вредоносных программ осуществляется антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая в ИС либо передаваемая из ИС.

2.6 Основными задачами антивирусной защиты являются: исключение или существенное затруднение противоправных действий в отношении ИС; обеспечение условий для устойчивой бесперебойной работы ИС.

2.7 Объектами защиты (далее – ОЗ) являются средства вычислительной техники, системное и прикладное программное обеспечение.

2.8 Обеспечение антивирусной защиты включает: анализ ситуации проявления вредоносных программ и причины их появления; блокирование вредоносных программ на границе ОЗ; принятие мер по предотвращению появления вредоносных программ.

2.9 Для выполнения требований по антивирусной защите обязательно использование антивирусного специализированного программного обеспечения (далее – СПО), сертифицированного в

соответствии с законодательством Республики Беларусь в области защиты информации.

2.10 СПО на границе ОЗ обслуживается системным администратором.

2.11 Установку и настройку СПО проводят работники, занимающиеся сопровождением ИС Центра информационных технологий (далее – ЦИТ) Университета.

2.12 Ежедневный контроль за наличием актуальных обновление СПО и обновление СПО проводит системный администратор.

2.13 Пользователям ИС запрещается: разрабатывать, использовать и распространять вредоносное программное обеспечение (далее – ВПО), а также использовать электронные носители информации с ВПО; отключать средства антивирусной защиты информации во время работы на средствах вычислительной техники; самовольно, без согласования с работниками Центра информационных технологий, устанавливать или настраивать (изменять настройки) средства антивирусной защиты информации.

ГЛАВА 3
ТРЕБОВАНИЯ К АНТИВИРУСНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

3.1 К использованию в качестве СПО допускаются только средства защиты от ВПО, имеющие сертификат соответствия требованиям по защите информации (в соответствии с ТР 2013/027/BY).

3.2 СПО должно обеспечивать возможность обнаружения как можно большего числа известного ВПО, в том числе вирусов, деструктивного кода, а также максимальную готовность быстрого реагирования на появление новых видов вирусных угроз.

3.3 При использовании средств антивирусной защиты информации должны учитываться следующие факторы: средства антивирусной защиты должны быть совместимы с используемым системным и прикладным ПО, а также с применяемыми средствами защиты информации; использование средств антивирусной защиты не должно существенно снижать производительности прикладного ПО и программно-технических средств по их основному функциональному назначению; средства антивирусной защиты должны иметь режимы автоматизированного или автоматического тестирования.

3.4 Поставщики СПО должны обеспечивать возможность обновлений, консультаций и других форм сопровождения эксплуатации СПО.

ГЛАВА 4
МЕРОПРИЯТИЯ ПО ШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

4.1 В штатном режиме работы системы системный администратор осуществляет: контроль наличия связи между сервером СПО и ОЗ; контроль автоматических обновлений баз данных сигнатур СПО; контроль над выполнением задач постоянной защиты; контроль актуальности версий антивирусных баз и модулей сканирования СПО сервера администрирования; мониторинг информационного обмена в средствах защиты с целью выявления проявлений программно-математических воздействий; обработку сведений, поступающих от средств антивирусной защиты; формирование сводных отчетов о работе средств антивирусной защиты, инцидентах; обработку отчетов о состоянии логических сетей; формирование отчетов о работе средств антивирусной защиты.

4.2 Процесс контроля антивирусной защиты осуществляется работником, ответственным за обеспечение информационной безопасности или начальником Центра информационных технологий и включает в себя следующие действия: внесение изменений в Политику антивирусной защиты; управление средствами антивирусной защиты, входящими в состав системы антивирусной защиты; мониторинг событий, информация о которых поступает от средств антивирусной защиты с ОЗ.

4.3 Начальник ЦИТ ежемесячно разрабатывает отчет в произвольной форме о работе средств антивирусной защиты. В отчете о состоянии системы антивирусной защиты отражается следующая информация: количество обнаруженных вредоносных программ за данный период; наиболее активные обнаруженные вредоносные программы; ОЗ, где наблюдается наибольшая частота обнаружения вредоносных программ; список зараженных ОЗ.

ГЛАВА 5
МЕРОПРИЯТИЯ ПО НЕШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

5.1 В случае заражения ИС вредоносными программами ведущий администратор сетей незамедлительно с момента обнаружения

заражения обязан выполнить следующие действия: доложить об инциденте начальнику ЦИТ; обновить антивирусные базы; проверить состояние всех ОЗ на предмет наличия вредоносного ПО; оперативно принять меры по предотвращению распространения заражения ВПО в пределах своей компетенции; провести действия, направленные на устранение ВПО на всех пораженных узлах ИС, а именно удаление зараженных файлов; по завершении мероприятий по устранению последствий заражения восстановить работоспособность ОЗ.

ГЛАВА 6
ПОРЯДОК ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ ПРИ ОБНАРУЖЕНИИ ЗАРАЖЕНИЯ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА

6.1 Работники Университета обязаны следить за сообщениями антивирусного СПО на предмет возможного заражения ИС.

6.2 Работники обязаны незамедлительно сообщить о факте обнаружения заражения работнику Центра информационных технологий.

ГЛАВА 7
УНИЧТОЖЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ

7.1 Уничтожение критического ВПО выполняется ведущим администратором сетей.

7.2 Если ВПО поразила какие-либо программы, то уничтожение ВПО выполняется путем уничтожения программы на жестком диске либо на ином магнитном носителе. После уничтожения зараженной программы восстанавливают программу, используя ее резервную копию.

7.3 Если ВПО поразила файлы, то вредоносная программа уничтожается либо путем стирания этих файлов, либо путем использования специального "лечащего" режима антивирусного ПО. Использование "лечащего" режима не дает полной гарантии восстановления файла, поэтому после "лечения" необходима проверка восстановления данного файла. "Лечащие" программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной 4 программы или файла с данными либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

7.4 После уничтожения вредоносных программ и восстановления зараженных программ и файлов ведущим системным администратором еще раз выполняется проверка наличия ВПО, используя антивирусную программу с установленными последними обновлениями.

ГЛАВА 8
ОТВЕТСТВЕННОСТЬ

8.1 Организация мероприятий по централизованной антивирусной защите Университета возлагается на начальника Центра информационных технологий.

8.2 Системный администратор несет ответственность за организацию и выполнение технических мероприятий по своевременной инсталляции средств антивирусной защиты информации и централизованное обновление баз данных вирусных описаний на комплексе ОЗ ИС.

8.3. Ответственным за внесение изменений в настоящую Политику является начальник Центра информационных технологий.