Приложение 5

Учреждение образования
«Гомельский государственный
медицинский университет»

УТВЕРЖДЕНО
Приказ ректора университета
09.06.2025 № 284

ПОЛОЖЕНИЕ
о защите от вредоносного
программного обеспечения

ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение о защите от вредоносного программного обеспечения (далее – Положение) учреждения образования «Гомельский государственный медицинский университет» (далее – Университет) разработано на основании требований законодательства Республики Беларусь в области защиты информации и приказа оперативно-аналитического центра при Президенте Республики Беларусь №66 от 20.02.2020 г.

2. Настоящее Положение входит в состав документации на систему защиты информации (далее – СЗИ) информационной системы Университета (далее – ИСУ).

3. Положение определяет порядок защиты от вредоносного программного обеспечения (далее – ВПО) в ИСУ, обработку ВПО, реагирование на обнаружение ВПО, а также требования к пользователям ИСУ, связанные с обеспечением защиты ИСУ от ВПО.

4. Требования Положения распространяются на все структурные подразделения и работников Университета, являющихся пользователями ИСУ.

ОБЩИЙ ПОРЯДОК ОРГАНИЗАЦИИ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

5. В целях обеспечения защиты ИСУ от деструктивных воздействий ВПО осуществляется антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая в ИСУ либо передаваемая из ИСУ.

6. Основными задачами антивирусной защиты являются:

исключение или существенное затруднение противоправных действий в отношении ИС;

обеспечение условий для устойчивой бесперебойной работы ИС.

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

8. Обеспечение антивирусной защиты включает:

анализ ситуации проявления ВПО и причины их появления;

блокирование вредоносных программ на границе ОЗ;

принятие мер по предотвращению появления вредоносных программ.

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.

10. Пользователям ИСУ запрещается:

разрабатывать, использовать и распространять ВПО

отключать средства антивирусной защиты информации во время работы на средствах вычислительной техники;

выполнять попытки получить несанкционированный и (или) неавторизованный доступ к управлению средствами антивирусной защиты или осуществлять доступ к управлению средствами антивирусной защиты с использованием чужой аутентификационной информации;

самовольно, без согласования с работниками ЦИТ, устанавливать или настраивать (изменять настройки) средства антивирусной защиты информации.

11. Пользователи ИСУ обязаны:

следить за сообщениями антивирусного СПО на предмет возможного заражения ИСУ;

немедленно оповещать инженера по защите информации или сотрудника отдела информационных технологий (далее – ОИТ) обо всех случаях срабатывания средств антивирусной защиты.

ТРЕБОВАНИЯ К АНТИВИРУСНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

12. 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).

13. СПО должно обеспечивать возможность обнаружения как можно большего числа известного ВПО, в том числе вирусов, деструктивного кода.

14. 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;

средства антивирусной защиты должны иметь режимы автоматизированного или автоматического тестирования.

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

МЕРОПРИЯТИЯ ПО УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

16. В штатном режиме работы системы администратор сетей 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.

17. Процесс контроля антивирусной защиты осуществляется работником, ответственным за обеспечение информационной безопасности 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.

18. В случае заражения ИС вредоносными программами сотрудник ОИТ незамедлительно с момента обнаружения заражения обязан выполнить следующие действия:

доложить об инциденте начальнику ОИТ;

обновить антивирусные базы;

проверить состояние ОЗ на предмет наличия вредоносного ПО;

провести действия, направленные на устранение ВПО на всех пораженных узлах ИС, а именно удаление зараженных файлов.

УНИЧТОЖЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ

19. Уничтожение критического ВПО выполняется сотрудниками ОИТ.

20. Если ВПО поразила какие-либо программы, то уничтожение ВПО выполняется путем уничтожения программы на носителе информации. После уничтожения зараженной программы восстанавливают программу, используя ее резервную копию.

21. 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 программы или файла с данными либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

22. После уничтожения ВПО и восстановления зараженных программ и файлов сотрудник ОИТ выполняется повторную проверку на наличие ВПО, используя антивирусную программу.

ТРЕБОВАНИЯ И ОТВЕТСТВЕННОСТЬ

23. На инженера по защите информации и администратора сетей возложена персональная ответственность за организацию и качество функционирования защиты от ВПО в ИСУ, в соответствии с действующим законодательством Республики Беларусь и с требованиями настоящего ЛПА.

24. Пользователи ИСУ должны быть ознакомлены под подпись с настоящим Положением в той части, которая необходима для безопасного выполнения своих функциональных обязанностей. Факт ознакомления работников ИСУ с настоящим Положением подтверждается личной подписью пользователя на Листе ознакомления.

25. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными правовым актами Университета.

ПЕРЕСМОТР ПОЛОЖЕНИЯ

26. При необходимости внесении изменений в Положение, изменения в существующий документ не вносятся, Положение переиздается и утверждается заново.

27. Плановое изменение Положения должно осуществляться не реже одного раза в год.

28. Внеплановое изменение Положения может производиться в случае изменения структуры, изменения процессов ИБ, подходов к защите информации или изменения законодательства Республики Беларусь в области защиты информации.

29. Пересмотр Положения инициируется проректором по безопасности, режиму и кадрам (в случае планового изменения) или инженером по защите информации (в случае внепланового изменения).

30. Пересмотр Положения согласовывается с проректором по безопасности, режиму и кадрам, после чего утверждается ректором.