МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Горно-Алтайский государственный университет»
(ФГБОУ ВО ГАГУ, ГАГУ, Горно-Алтайский государственный университет)

ПРИЛОЖЕНИЕ №4
к приказу № 155 от 08.06.2026

РЕГЛАМЕНТ
08.06.2026 № 01-05-64

антивирусной защиты информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Горно-Алтайский государственный университет»

1. Общие положения

1.1. Настоящий Регламент определяет цели, задачи, порядок организации и обеспечения антивирусной защиты информации (далее – АВЗ) в ФГБОУ ВО «Горно-Алтайский государственный университет» (далее – Университет), разграничение полномочий ответственных подразделений, а также требования к используемым программным и техническим средствам.

1.2. Регламент разработан в соответствии со следующими нормативно-правовыми актами:

- Указ Президента РФ от 01.05.2022 № 250 (ред. от 13.06.2024) «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных»;
- Приказ ФСТЭК России от 20.03.2012 № 28 «Об утверждении Требований к средствам антивирусной защиты»;
- Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

1.3. Настоящий Регламент обязателен для исполнения всеми структурными подразделениями и работниками Университета, имеющими доступ к

автоматизированным рабочим местам (АРМ), серверному оборудованию, информационным системам и иным ресурсам Университета.

2. Термины и определения

Антивирусная защита – комплекс организационных и технических мер, направленных на обнаружение, блокирование и ликвидацию вредоносного программного обеспечения (ВПО), а также на восстановление последствий его воздействия.

Средство антивирусной защиты (САВЗ) – программное или программно-аппаратное средство, предназначенное для реализации мер антивирусной защиты, прошедшее сертификацию в установленном порядке.

Вредоносное программное обеспечение (ВПО) – компьютерная программа или иная компьютерная информация, предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации.

Инцидент информационной безопасности – факт обнаружения ВПО, нарушающий установленный режим антивирусной защиты.

3. Разграничение полномочий и обязанности

3.1. В Университете определены следующие структурные подразделения и сотрудники, отвечающие за организацию и обеспечение антивирусной защиты информации:

- Специалист по информационной безопасности (далее – специалист по ИБ), осуществляющее функции контроля и методологического сопровождения системы АВЗ;
- Центр цифрового развития, ответственный за эксплуатацию и техническую поддержку средств вычислительной техники (далее – ЦЦР), осуществляющее функции настройки, управления и технического обслуживания САВЗ.

3.2. Специалист по ИБ:

- разрабатывает и актуализирует локальные нормативные акты в сфере АВЗ (Регламент, Инструкции, Политики);
- организует и проводит внутренний контроль за соблюдением требований АВЗ;
- анализирует отчёты и журналы событий, предоставляемые ЦЦР, для оценки состояния защищённости и выработки предложений по её улучшению;

— координирует действия структурных подразделений при локализации и ликвидации последствий вирусных атак;
— взаимодействует с ФСТЭК России, Минцифры России и другими уполномоченными органами по вопросам АВЗ;
— проводит служебные расследования по фактам нарушений режима АВЗ (при необходимости);
— оценивает соответствие САВЗ требованиям законодательства, включая сертификацию и необходимость импортозамещения.

3.3. ЦЦР:

— осуществляет установку, развёртывание и централизованное управление сертифицированными САВЗ на всех серверах, АРМ и иных устройствах Университета;
— обеспечивает автоматическое регулярное обновление антивирусных баз и версий программного обеспечения;
— настраивает средства антивирусной защиты в масштабе времени, близком к реальному, для проверки файлов из внешних источников, включая съёмные носители, сетевые подключения и электронную почту;
— осуществляет мониторинг работоспособности САВЗ, выявляет и устраняет сбои в их работе;
— проводит плановые и внеплановые антивирусные проверки оборудования;
— изолирует заражённые устройства от корпоративной сети при обнаружении активных угроз;
— предоставляет в подразделение УКБ отчёты о результатах мониторинга и выявленных инцидентах.

4. Требования к средствам антивирусной защиты

4.1. На серверах и АРМ Университета подлежат установке только лицензионные САВЗ, имеющие действующие сертификаты ФСТЭК России. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

4.2. САВЗ должны выбираться с учётом класса защищённости информационной системы. Университету следует ориентироваться на САВЗ 4 класса защиты (при обработке информации ограниченного доступа) и 5–6 классов – для иных систем.

4.3. В соответствии с политикой импортозамещения и требованиями Указа Президента РФ № 250 (с изменениями от 13.06.2024), с 1 января 2025 года организациям запрещается использовать средства защиты информации,

предоставляемые организациями из недружественных стран. Приоритет при выборе САВЗ отдаётся программному обеспечению российского происхождения, включённому в Единый реестр отечественного ПО (Минцифры России).

4.4. Администрирование САВЗ должно осуществляться централизованно, с консолидацией информации о состоянии защищённости на выделенном сервере управления. На всех АРМ и серверах должна быть обеспечена защита в реальном масштабе времени.

5. Организационные и технические меры

5.1. Меры по контролю и обновлению

5.1.1. Антивирусные базы должны обновляться автоматически в соответствии с регламентом обновлений разработчика САВЗ, но не реже одного раза в сутки.

5.1.2. ЦЦР осуществляет ежедневный мониторинг состояния АВЗ и принудительно обновляет базы на устройствах, не получивших обновления в автоматическом режиме более 24 часов.

5.2. Меры по защите от внешних угроз

5.2.1. На серверах электронной почты Университета должна быть организована эшелонированная антивирусная фильтрация всего входящего и исходящего трафика.

5.2.2. В САВЗ должна быть настроена проверка всех сменных носителей информации (USB-накопители, внешние диски) перед предоставлением к ним доступа.

5.2.3. Все вновь устанавливаемое программное обеспечение и его обновления перед внедрением обязательно проверяются на отсутствие ВПО.

5.3. Меры по регистрации и хранению

5.3.1. САВЗ должны осуществлять регистрацию всех событий, связанных с обнаружением (попыткой обнаружения) ВПО: наименование угрозы, дата и время события, наименование заражённого объекта, предпринятое действие (лечение, удаление, карантин).

5.3.2. Регистрационные журналы подлежат хранению в течение одного года, а при участии в расследовании инцидента – до его полного завершения.

6. Порядок действий при обнаружении вредоносного программного обеспечения

6.1. При обнаружении вирусной угрозы САВЗ в автоматическом режиме должно:

— попытаться вылечить заражённый объект;

— при невозможности лечения – поместить объект в карантин или удалить;
— заблокировать доступ пользователя к файлу до принятия решения.

6.2. При массовом распространении вируса или сбое автоматических механизмов:

— Пользователь АРМ обязан незамедлительно (не более 15 минут) отключить устройство от локальной сети и сообщить о факте заражения в ЦЦР.
— ЦЦР изолирует сегмент сети, идентифицирует распространение угрозы и докладывает подразделению УКБ.
— Подразделение УКБ координирует действия по локализации угрозы, назначает ответственных за ликвидацию последствий и, при необходимости, инициирует служебное расследование.

6.3. По окончании ликвидации последствий ЦЦР проводит внеплановую проверку всех АРМ в пострадавшем сегменте сети.

6.4. Ответственность за невыполнение или нарушение требований настоящего Регламента устанавливается локальными актами Университета и может влечь за собой дисциплинарную, административную и (или) гражданско-правовую ответственность в соответствии с законодательством РФ.

7. Заключительные положения

7.1. Настоящий Регламент вступает в силу с даты его утверждения ректором Университета.

7.2. Внесение изменений и дополнений в Регламент осуществляется при изменении законодательства РФ в области информационной безопасности, появлении новых угроз безопасности информации, а также по результатам периодического анализа эффективности системы антивирусной защиты Университета.

7.3. Контроль за исполнением Регламента возлагается на подразделение, ответственное за обеспечение информационной безопасности Университета.