

УТВЕРЖДЕНО
Приказ ректора университета
«10» декабря 2025 № 389-од

Перечень разрешённого программного обеспечения

1. Общие положения

1.1. Настоящий перечень определяет программное обеспечение (ПО), разрешённое к установке и использованию на рабочих станциях, серверах и иных вычислительных средствах университета.

1.2. Установка ПО, не включённого в перечень, без согласования с Центром информационных технологий и специалистом по защите информации запрещена.

1.3. ПО классифицируется по классам [1], [2], [3] (примечания). Приоритет - отечественные, доверенные и сертифицированные продукты.

2. Перечень ПО

№	Тип ПО	Наименование ПО	Класс ПО	Примечание
1.	Операционные системы	Microsoft Windows (ОЕМ, академические лицензии)	[1]	Приоритет отечественные и доверенные дистрибутивы
2.	Средства защиты (СЗИ)	Kaspersky Endpoint Security for Business - Advanced Belarus Edition; Kaspersky Embedded Systems Security Belarus Edition; криптографические средства Avest	[1]	Обязательно наличие сертификата соответствия ОАЦ

№	Тип ПО	Наименование ПО	Класс ПО	Примечание
3.	Офисные пакеты	Microsoft Office (академическая лицензия); LibreOffice	[2]	Проверка лицензионной чистоты
4.	Работа с ЭЦП	ПО для работы с порталами государственных органов; ПО для СМДО	[2]	–
5.	Браузеры	Google Chrome; Mozilla Firefox	[2]	Использовать актуальные версии и политики безопасности
6.	Архиваторы	7-Zip	[2]	–
7.	Научное/статистическое ПО	Statistica	[3]	Для научного анализа данных
8.	СУБД	Microsoft SQL Server (версии 8, 14, 15) PostgreSQL (доверенная сборка);	[1,2]	PostgreSQL доверенная сборка; MS SQL - версии указаны
9.	Информационно-правовые системы	ИПС «Эталон»; ИПС «КонсультантПлюс»	[2]	Доступ по лицензиям организации
10.	Аудио-оборудование и DAW	DANTE VIA DVS BUNDLE; STEINBERG Cubase Pro 9 EE DaVinci Resolve	[3]	Для звукозаписи и обработки

№	Тип ПО	Наименование ПО	Класс ПО	Примечание
11.	Аудио/видео монтаж	VEGAS Pro; RE-VOICE PRO Standard; FABFILTER PRO-Q 2 (плагин) DaVinci Resolve	[3]	Плагины и лицензии обязательны
12.	Графика и верстка, просмотр изображений	CorelDRAW Graphics Suite; Adobe InDesign CC Paint.Net Gimp Notepad++ XnView AIMP VLC media player WinDjView	[3]	Лицензии и версии должны быть подтверждены
13.	Вспомогательное (технологическое) программное обеспечение	Double Commander	[3]	–
14.	PDF и документооборот	Acrobat Pro DC	[2]	Для создания и защиты PDF
15.	Развёртывание образов	Acronis Snap Deploy	[1]	Для массового развёртывания эталонных образов
16.	Электронное обучение / авторинг	iSpring Suite	[3]	Для создания электронных курсов и тестов
17.	Системы обнаружения плагиата	«Антиплагиат»	[3]	Для проверки учебных работ

№	Тип ПО	Наименование ПО	Класс ПО	Примечание
18.	АСУ кадровые	АСУ «Кадры. Сотрудники»	[1]	Обработка персональных данных сотрудников - повышенные требования
19.	АС ДОУ / документооборот	АС ДОУ «Медиум»	[2]	Электронный документооборот
20.	Бюджет/зарплата	«ИС: Управление бюджетным учреждением 8. Зарплата»	[1]	Финансовые данные и персональные данные - повышенная защита
21.	СКУД	Perco-Web (СКУД)	[1]	Данные контроля доступа/идентификаторы
22.	Сетевые/инфраструктурные решения	Traffic Inspector Special	[1]	Фильтрация и контроль трафика
23.	Удалённый доступ	Radmin 3	[2]	Использовать только по согласованию и через защищённые каналы

№	Тип ПО	Наименование ПО	Класс ПО	Примечание
24.	Сертифицированное средство защиты информации	«КАНОЭ»	[1]	Специализированные решения.
25.	Прочие специализированные комплекты	Комплект программных продуктов, не перечисленных выше (по заявке)	[2/3]	Включение по процедуре (раздел 5)

3. Примечания по классификации и примечания

3.1. Класс [1] системное и критичное ПО, влияющее на безопасность и целостность ИС (ОС, СЗИ, СУБД, бухгалтерские и кадровые системы, СКУД).

3.2. Класс [2] прикладное ПО общего назначения (офисные пакеты, почта, браузеры, PDF-редакторы, утилиты).

3.3. Класс [3] специализированное учебное, научное и творческое ПО (среды разработки, инженерные пакеты, DAW, графика).

При отнесении ПО к классу учитываются: влияние на безопасность, обработка персональных данных, критичность для бизнес-процессов, наличие сертификатов и лицензий.

4. Требования по лицензированию и сертификации

4.1. Лицензии. Все ПО должно иметь подтверждённую лицензию; использование пиратского ПО запрещено.

4.2. Сертификация СЗИ. Средства защиты (антивирусы, криптография) должны иметь сертификат соответствия ОАЦ Республики Беларусь, если это требуется регулятором.

4.3. Совместимость. Новое ПО проверяется на совместимость с существующей инфраструктурой и на отсутствие угроз безопасности.

5. Порядок внесения изменений

5.1. Актуализация перечня проводится ежегодно или по мере необходимости.

5.2. Для включения нового ПО руководитель структурного подразделения подаёт докладную записку с обоснованием необходимости, подтверждением лицензионной чистоты, оценкой совместимости и заключением специалиста по защите информации.

5.3. Решение о включении принимает Центр информационных техноло-

гий совместно со специалистом по защите информации; при необходимости - с участием юридического отдела и владельца ИС.

5.4. ПО, не прошедшее проверку или не имеющее лицензии, к использованию не допускается.