Приложение 6

Учреждение образования
«Гомельский государственный
медицинский университет»

УТВЕРЖДЕНО
Приказ ректора университета
09.06.2025 № 284

ПОЛОЖЕНИЕ
об организации и разграничении доступа пользователей к информационной системе

ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение об организации и разграничению доступа пользователей к информационной системе (далее – Положение) учреждения образования «Гомельский государственный медицинский университет» (далее – Университет) разработана на основании Закона Республики Беларусь «Об информации, информатизации и защите информации», Закона Республики Беларусь «О защите персональных данных» и иных нормативных правовых актов Республики Беларусь в области информационной безопасности.

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

3. Положение разработано с целью регламентации порядка предоставления, изменения и аннулирования прав доступа работников Университета к информационным ресурсам и объектам Университета.

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

ОРГАНИЗАЦИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ

5. Доступ к информационным ресурсам и информационным объектам ИСУ обеспечивается путем формирования и выдачи пользователю учетной записи, содержащей уникальные имя пользователя и пароль для последующей аутентификации пользователя в ИСУ.

Имена пользователей ИСУ формируются в соответствии с правилами, изложенными в Приложении 1 к настоящему Положению.

6. Основанием для формирования учетной записи пользователя ИСУ является служебная записка (на бумажном носителе или в электронном виде) на имя инженера по защите информации от руководителя структурного подразделения Университета, работнику которого необходимо предоставить учетную запись. В заявке также указывается

список информационных ресурсов и объектов ИСУ, к которым необходимо обеспечить доступ указанному пользователю.

В случае необходимости создания (удаления/изменения) учетной записи инженера по защите информации, указанная служебная записка пишется на имя проректора по безопасности, режиму и кадрам.

7. Инженер по защите информации регистрирует указанную заявку (на создание, корректировку, блокировку) учетной записи. После чего инженер по защите информации, передает указанную заявку администратору сетей, который создает (изменяет) учетную запись пользователя ИСУ с учетом ограничений по доступу к информационным ресурсам ИСУ.

8. В целях обеспечения контроля за действиями ИСУ администратором сети во взаимодействии с инженером по защите информации настроена система централизованного аудита (фиксации в виде отдельных лог файлов) действий пользователей ИСУ при их обращении к информационным ресурсам и объектам ИСУ.

Хранение лог файлов осуществляется не менее 1 года.

9. В случае необходимости предоставления пользователю ИСУ дополнительных полномочий для доступа к уже используемым им информационным ресурсам и (или) объектам ИСУ осуществляются действия в соответствии с п. 6-7 настоящего Положения.

10. Обязанность по своевременному информированию инженера по защите информации о переходе работников Университета из одного подразделения в другое или об окончании работы в нем (увольнении работника) возлагается на отдел кадров и руководителей соответствующих структурных подразделений Университета.

11. Доступ увольняемого работника к ИСУ прекращается в последний день работы в Университете.

Конкретное время прекращения доступа увольняемого работника к ИСУ согласовывается руководителем соответствующего структурного подразделения Университета с администратором сетей. Блокирование учетной записи увольняемого работника Университета производится администратором сетей на основании служебной записки руководителя подразделения, из которого увольняется работник Университета. Служебная записка пишется на имя инженера по защите информации, согласовывается проректором по безопасности, режиму и кадрам.

12. При увольнении работника Университета необходимо:

руководителю соответствующего структурного подразделения уточнить факт передачи необходимых информационных ресурсов ИСУ, которые находились под управлением увольняемого работника;

сотруднику отдела информационных технологий проверить полноту, целостность и доступность информационных ресурсов ИСУ, к которым

увольняемый работник имел доступ, провести их проверку с использованием антивирусного программного обеспечения (далее – ПО);

администратору сетей блокировать (не удалять) в ИСУ все учетные записи увольняемого работника.

13. При увольнении работника Университета, имевшего в ИСУ учетные записи с расширенными правами (администратор сетей, инженер по защите информации), проректором по безопасности, режиму и кадрам принимается решение о необходимости переустановки операционных систем на соответствующих серверах ИСУ и (или) внеплановой полной смене паролей всех пользователей ИСУ.

14. В случае обнаружения неправомерных действий увольняемого работника в отношении информационных ресурсов или объектов ИСУ, инженер по защите информации докладывает об этом проректору по безопасности, режиму и кадрам.

15. Инженер по защите информации проводит периодический контроль (1 раз в год) соответствия перечня объектов и информационных ресурсов, к которым имеет доступ каждый пользователь ИСУ, перечню объектов и информационных ресурсов.

РАЗГРАНИЧЕНИЕ ДОСТУПА К ОБЪЕКТАМ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

16. Разграничение доступа пользователей к информационным ресурсам и/или объектам ИСУ осуществляется с использованием:

групповых политик (GPO) службы каталогов Microsoft (Active Directory);

средств управления доступом ОС семейства Linux;

средств управления доступом к серверу обмена данными;

средств управления доступом к системе хранения данных;

средств управления доступом к ресурсам локальной сети.

17. Разграничение доступа всех категорий пользователей к ИСУ выполняется на основании следующих правил:

все механизмы защиты серверов ИСУ находятся под монопольным управлением администраторов сетей;

обеспечено сегментирование (изоляция) сети управления от сети передачи данных;

обеспечено безопасное конфигурирование сетевого оборудования за счет ограничения доступа к портам управления посредством MAC-фильтрации, программного отключения неиспользуемых портов и ограничения физического доступа к оборудованию;

обеспечено разграничение доступа к виртуальным и физическим серверам на уровне сети и на уровне операционных систем;

пользователи НЕ используют назначенные им идентификаторы

совместно;

обучение ИБ проводится в необходимом объеме со всеми категориями пользователей ИСУ (например, в рамках программы вводных инструктажей).

ПАРОЛЬНАЯ ЗАЩИТА

18. Основой для аутентификации всех категорий пользователей ИСУ являются пароли. Точное выполнение всеми категориями пользователей ИСУ требований по формированию и использованию паролей непосредственно влияет на обеспечение заданного уровня ИБ.

19. Для аутентификации пользователей ИСУ используют пароли, соответствующие следующим обязательным условиям:

длина пароля не менее 8 символов (рекомендуется 12 и более);

пароль не должен совпадать со словарными словами, а также содержать личные данные пользователя, которые бы позволяли вычислить значение пароля, например: ФИО, номера телефонов, памятные даты (дни рождения и т.д.); последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.); общепринятые сокращения («USER», «TEST», «ADMIN» и т.п.);

пароль должен содержать не менее одной латинской буквы верхнего и нижнего регистра, не менее одной цифры (0-9), не менее одного специального символа (! @#$%&*() -_ + = ~[] { } |\ ^: ; «» ?);

20. Пользователям ИСУ запрещается:

хранить пароль способом, позволяющим другим лицам получить информацию о нем;

сообщать и (или) передавать пароль другим лицам, включая непосредственного начальника, администратора сетей, инженера по защите информации;

использовать для доступа к ИСУ скомпрометированный пароль.

21. В случае компрометации пароля пользователя ИСУ (или наличия у пользователя ИСУ подозрений о компрометации пароля) он обязан уведомить инженера по защите информации о факте компрометации (подозрении на компрометацию пароля).

ОТВЕТСТВЕННОСТЬ

22. 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.

23. Работники Университета несут ответственность за разглашение, несоответствующее использование и хранение своих криптографических

ключей и ключевых документов. Привлечение работника Университета к ответственности осуществляется в соответствии с действующим законодательством Республики Беларусь.

ПЕРЕСМОТР ПОЛОЖЕНИЯ

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

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

26. 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.

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

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

Приложение 1

Правила формирования учетных записей пользователей ИСУ

Создание учетных записей пользователей ИСУ в Active Directory и (или) других информационных системах, входящих в состав ИСУ, производится администратором сетей по нижеописанным правилам:

для создания учетной записи пользователя ИСУ должна использоваться первая буква имени пользователя (заменяется по правилам транслитерации) и фамилия (на латинице из паспорта);

логин пользователя в домене должен формироваться следующим образом: [первая буква имени][фамилия] (например, avetrov и т.д.). В случае полного совпадения логинов добавляется вторая буква имени.

Таблица транслитерации

БУКВА	ТРАНСЛИТ	БУКВА	ТРАНСЛИТ
А	A	П	P
Б	B	Р	R
В	V	С	S
Г	G	Т	T
Д	D	У	U
Е	E	Ф	F
Ё	E	Х	H
Ж	ZH	Ц	C
З	Z	Ч	CH
И	I	Ш	SH
Й	J	Щ	SCH
К	K	Ъ	опускается
Л	L	Ы	Y
М	M	Э	E
Н	N	Ю	YU
О	O	Я	YA