Приложение 2

Учреждение образования
«Гомельский государственный
медицинский университет»

УТВЕРЖДЕНО
Приказ ректора университета
09.06.2025 № 284

ПОЛОЖЕНИЕ
об использовании средств
криптографической защиты
информации

ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение об использовании средств криптографической защиты информации (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 регламентирует порядок учета, хранения и использования средств криптографической защиты информации (далее – СКЗИ), криптографических ключей и ключевых документов, а также порядок изготовления, смены, уничтожения и порядок действий в случае компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

4. Требования Положения распространяются на всех работников Университета, являющихся пользователями ИСУ.

ОРГАНИЗАЦИЯ ХРАНЕНИЯ И ЭКСПЛУАТАЦИИ

5. Для реализации функций выработки электронной цифровой подписи (далее – ЭЦП), проверки ЭЦП или открытого ключа должны использоваться средства ЭЦП должны использоваться только сертифицированные, в соответствии с действующим законодательством, средства ЭЦП.

6. Для обеспечения порядка учета, хранения и использования СКЗИ приказом ректора назначается ответственный работник.

7. К работе с СКЗИ работники Университета допускаются только после соответствующего инструктажа ответственным работником.

8. Правила использования в ИСУ СКЗИ и средств ЭЦП определяются

требованиями действующего законодательства Республики Беларусь и надзорных органов.

Управление и настройка СКЗИ и средств ЭЦП должна осуществляться в строгом соответствии с эксплуатационной документацией.

9. Безопасность хранения и обработки информации с использованием СКЗИ достигается:

соблюдением пользователями СКЗИ конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ;

точным выполнением пользователями СКЗИ требований к обеспечению безопасности информации;

надежным хранением эксплуатационной и технической документации к СКЗИ, носителей информации, распространение и (или) предоставление которой ограничено;

своевременным выявлением работниками Университета попыток получения сведений об информации, распространение и предоставление которой ограничено, об используемых СКЗИ лицами, не обладающими правом доступа к таким сведениям;

немедленным принятием мер по предупреждению разглашения информации, распространение и предоставление которой ограничено, а также возможной ее утечки при выявлении фактов утраты или недостачи СКЗИ, пропусков, ключей от помещений, сейфов и т. п.

УЧЕТ, ХРАНЕНИЕ И ПЕРЕДАЧА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

10. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы и ключевые носители подлежат обязательному учету. Программные СКЗИ учитываются совместно с аппаратными средствами, на которых осуществляется их штатная эксплуатация. Учет осуществляется ответственным работником.

11. Работники Университета несут персональную ответственность за сохранность СКЗИ и ключевых документов.

12. Дистрибутивы СКЗИ, эксплуатационная и техническая документация к ним хранятся у ответственного работника.

13. Хранение СКЗИ осуществляется в ящиках, шкафах, сейфах (хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

14. В случае отсутствия у работника Университета индивидуального хранилища, ключевые носители с криптографическими ключами по окончании рабочего дня сдаются ответственному работнику под роспись.

15. Ключевые носители с неработоспособными криптографическими

ключами передаются ответственному работнику. Неработоспособные ключевые носители подлежат уничтожению.

16. Аппаратные средства, с которыми осуществляется штатное использование СКЗИ, а также аппаратные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ и аппаратных средств должно быть визуально контролируемым.

ИСПОЛЬЗОВАНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

17. В Университете СКЗИ используется с целью обеспечения конфиденциальности и целостности электронных документов и сетевого трафика.

18. В случае обнаружения неразрешенного программного обеспечения или факта повреждения целостности печати (пломбы) на техническом средстве с СКЗИ, работа с СКЗИ на таком техническом средстве должна быть прекращена.

19. Вскрытие технического средства с СКЗИ для проведения ремонта или технического обслуживания осуществляется только в присутствии ответственного работника.

20. При работе с СКЗИ запрещается:

оставлять без присмотра (контроля) технические средства, на которых эксплуатируется СКЗИ;

самостоятельно вносить изменения в программную часть СКЗИ;

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, не допущенным к работе с СКЗИ;

использовать ключевые носители в режимах, не предусмотренных штатными функциями СКЗИ;

осуществлять несанкционированное копирование криптографических ключей;

изменять настройки или пытаться изменить настройки СКЗИ или операционной системы, сделанные ответственным работником;

использовать бывшие в работе ключевые носители для записи новой информации без предварительного гарантированного уничтожения на них ключевой информации;

осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.

УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

21. Неиспользованные, неработоспособные или выведенные из действия криптографические ключи подлежат уничтожению.

22. Уничтожение криптографических ключей на ключевых носителях

производятся комиссией в составе председателя и членов комиссии, назначенной ректором Университета.

23. Криптографические ключи, записанные на машинные ключевые носители, уничтожаются методом гарантированного стирания информации на машинном носителе в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

24. Перед уничтожением криптографических ключей и/или ключевых носителей, комиссия обязана:

установить наличие оригинала и количество копий криптографических ключей;

проверить внешнюю целостность каждого ключевого носителя; идентифицировать каждый ключевой носитель;

убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

произвести уничтожение криптографических ключей.

25. По факту уничтожения криптографических ключей составляется Акт уничтожения.

26. Акт подписывается председателем и членами комиссии.

27. Акты уничтожения криптографических ключей хранятся у ответственного работника.

ОБЯЗАННОСТИ РАБОТНИКОВ ПРИ ОБРАЩЕНИИ С СКЗИ

28. При работе с СКЗИ работник Университета, осуществляющий их эксплуатацию, обязан:

не разглашать информацию, распространение которой ограничено, в том числе сведения о криптографических ключах и сами криптографические ключи, в том числе устаревшие;

соблюдать требования к обеспечению безопасности информации распространение и предоставление которой ограничено при использовании СКЗИ;

сдать в случае прекращения трудовых отношений или прекращения договорных отношений с Университетом используемые СКЗИ, эксплуатационную и техническую документацию к ним;

обеспечивать сохранность и конфиденциальность ключевой информации при хранении;

сообщать ответственному работнику о попытках посторонних лиц получить сведения об СКЗИ или ключевых документах к ним;

незамедлительно уведомлять ответственного работника о фактах утраты или недостачи СКЗИ, криптографических ключей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

ОТВЕТСТВЕННОСТЬ

29. 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.

30. 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

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

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

33. 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.

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

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