Приложение 3

Учреждение образования
«Гомельский государственный
медицинский университет»

УТВЕРЖДЕНО
Приказ ректора университета
09.06.2025 № 284

ПОЛОЖЕНИЕ
о порядке использования и
хранения электронной
цифровой подписи

ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение о порядке использования и хранения электронной цифровой подписи (далее – Положение) учреждения образования «Гомельский государственный медицинский университет» (далее – Университет) разработано в соответствии с Законом Республики Беларусь от 28.12.2009 № 113-З «Об электронном документе и электронной цифровой подписи».

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

3. Настоящее Положение определяет:

порядок обеспечения правовых условий, при соблюдении которых электронная цифровая подпись (далее – ЭЦП) в электронном документообороте признается равнозначной собственноручной подписи в документе на бумажном носителе;

порядок использования и хранения носителей ключевой информации; порядок выдачи и возврата носителей ключевой информации;

основные организационно-технические мероприятия, направленные на обеспечение безопасности при работе со средствами криптографической защиты информации.

4. Требования Положения распространяются на работников Университета, использующих ЭЦП.

ПОРЯДОК ИСПОЛЬЗОВАНИЯ И ХРАНЕНИЯ НОСИТЕЛЕЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ

5. В Университете используются только сертифицированные средства ЭЦП.

Использование несертифицированных средств ЭЦП и созданных ими ключей ЭЦП не допускается.

6. ЭЦП используется строго в соответствии со сведениями, указанными в сертификате открытого ключа.

7. Для обмена электронными документами между Университетом с государственными органами, органами местного самоуправления, организациями, не являющимися участниками информационной системы Университета, используется система межведомственного документооборота (далее – СМДО), а также иные программные средства.

8. Учет криптоключей и сертификатов открытого ключа осуществляется сотрудниками ЦИТ в журнале. Если один и тот же USB-флеш-накопитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно, при этом указывается новый сертификат открытого ключа.

9. Криптоключи (ЭЦП) приобретаются через отдел материально-технического снабжения, после согласования с проректором по безопасности, режиму и кадрам и начальником ЦИТ. Пользователь ЭЦП после получения криптоключа (ЭЦП), обязан зарегистрировать криптоключ (ЭЦП) в ЦИТ в журнале (см. п. 8), в день получения.

10. Установка сертификата открытого ключа осуществляется только на рабочие (служебные) ПЭВМ. Пользователь криптоключа (ЭЦП) несет персональную ответственность за его сохранность, в соответствии с актуальной инструкцией, размещённой на сайте удостоверяющего центра.

11. Пользователи ЭЦП хранят их в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

12. Пользователям ЭЦП запрещается:

осуществлять копирование ключевой информации на носители, не являющиеся ключевыми;

выводить ключевую информацию на дисплей и принтер;

вставлять ключевой носитель в порты ПЭВМ, не являющихся рабочими (служебными);

записывать на ключевой носитель постороннюю информацию.

13. Плановая смена криптоключей производится в связи с истечением установленного срока их действия.

14. В случае кадровых изменений относительно работника (пользователя ЭЦП), касающихся использования ЭЦП, отдел кадров незамедлительно сообщает об этом в ЦИТ, и направляет такого работника с принадлежащим ему криптоключом для оформления заявления на отзыв сертификата открытого ключа. При этом криптоключ предаётся начальнику ЦИТ.

15. В случаях прекращение действия ЭЦП криптоключи передаются начальнику ЦИТ.

ДЕЙСТВИЯ В СЛУЧАЕ КОМПРОМЕТАЦИИ КРИПТОКЛЮЧЕЙ

16. К событиям, связанным с компрометацией криптоключей, относятся следующие:

потеря криптоключей;

потеря криптоключей с их последующим обнаружением;

прекращение полномочий или увольнение сотрудников, имевших доступ к ключевой информации;

нарушение правил хранения и уничтожения (после окончания срока действия) криптоключа;

случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями с записанными на них криптоключами (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

другие события, вызывающие подозрения на утечку ключевой информации или ее искажение.

При наступлении любого из перечисленных выше событий пользователь ЭЦП должен немедленно прекратить обмен электронными данными и сообщить о факте компрометации (или предполагаемой компрометации) своему непосредственному руководителю и начальнику ЦИТ.

17. Скомпрометированные криптоключи немедленно выводятся из работы, проводится их экстренная замена.

ОТВЕТСТВЕННОСТЬ ВЛАДЕЛЬЦЕВ КЛЮЧЕЙ ЭЦП

18. За неисполнение или ненадлежащее исполнение обязанностей в соответствии с настоящим Положением работники Университета несут ответственность в соответствии с законодательством Республики Беларусь.

19. Пользователь ЭЦП несет ответственность за сохранность своих криптоключей.

20. Пользователь ЭЦП обязан:

не разглашать информацию, к которой они допущены, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности информации; сообщать непосредственному руководителю о ставших им известными

попытках посторонних лиц получить сведения об используемых ЭЦП и сертификатов открытого ключа или документах к ним;

немедленно сообщать непосредственному руководителю и начальнику ЦИТ о фактах утраты или недостачи ЭЦП и сертификатов открытого ключа, ключевых документов к ним, ключей от помещений, хранилищ и о других фактах, которые могут привести к разглашению защищаемых

сведений, а также о причинах и условиях возможной утечки таких сведений.

21. В случае если пользователь ЭЦП допустил компрометацию криптоключей, и не уведомил об этом факте непосредственного руководителя и начальника ЦИТ, то всю ответственность за возможные последствия несет допустивший компрометацию пользователь ЭЦП.

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

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.