Министерство здравоохранения Республики Беларусь
Учреждение образования «Витебский государственный ордена Дружбы народов медицинский университет»

УТВЕРЖДЕНО

Приказ ректора университета

«10» декабря 2025 № 389-од

Политика управления криптографическими ключами

г. Витебск

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика управления криптографическими ключами учреждения образования «Витебский государственный ордена Дружбы народов медицинский университет» (далее – Политика) определяет 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.

1.2. Настоящая Политика входит в состав документации на систему защиты информации информационной системы (далее – ИС) учреждения образования «Витебский государственный ордена Дружбы народов медицинский университет» (далее – Университет).

1.3. В Университете используются только сертифицированные в соответствии с требованиями законодательства Республики Беларусь СКЗИ.

1.4. Требования настоящей политики распространяются на всех работников Университета, работающих с компьютерной техникой.

1.5. Общий контроль за соблюдением работниками Университета норм настоящей политики осуществляется начальником центра информационных технологий Университета.

ГЛАВА 2
ОРГАНИЗАЦИЯ ХРАНЕНИЯ И ЭКСПЛУАТАЦИИ

2.1. Для обеспечения защиты информации, распространение и/или

предоставление которой ограничено, не отнесенной к государственным секретам, при ее передаче по открытым каналам связи в Университете должны использоваться средства защиты информации (в том числе средства СКЗИ), прошедшие сертификацию или имеющие положительное экспертное заключение в соответствии с действующим законодательством Республики Беларусь.

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

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

2.4. Правила использования в Университете 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.

2.5. В ИС Университета допускается использовать только учтенные в соответствии с требованиями бухгалтерского учета СКЗИ.

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

2.7.1. 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;

2.7.2. точным выполнением пользователями СКЗИ требований к обеспечению безопасности информации;

2.7.3. надежным хранением эксплуатационной и технической документации к СКЗИ, носителей информации, распространение и/или предоставление которой ограничено, не отнесенной к государственным секретам;

2.7.4. своевременным выявлением работниками попыток получения сведений о защищаемой информации, об используемых СКЗИ лицами, не обладающими правом доступа к таким сведениям;

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

ГЛАВА 3
УЧЕТ, ХРАНЕНИЕ И ПЕРЕДАЧА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

3.1. 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 Университета.

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

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

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

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

3.6. Ключевые носители с неработоспособными криптографическими ключами передаются ответственному работнику. Неработоспособные ключевые носители подлежат уничтожению.

3.7. 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.

ГЛАВА 4
ИСПОЛЬЗОВАНИЕ СКЗИ

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

4.2. Для шифрования/расшифрования электронного документа и/или сетевого трафика работник Университета использует свой собственный закрытый криптографический ключ и открытый криптографический ключ.

4.3. 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.

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

4.5. При работе с СКЗИ запрещается:

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

4.5.2. самостоятельно вносить изменения в программную часть СКЗИ;

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

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

4.5.5. осуществлять несанкционированное копирование криптографических ключей;

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

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

4.5.8. осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.

ГЛАВА 5
ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

5.1. Криптографические ключи считаются скомпрометированными в следующих случаях:

5.1.1. потеря ключевых носителей (в том числе с последующим обнаружением);

5.1.2. увольнение работников Университета, имевших доступ к ключевым носителям;

5.1.3. возникновение подозрений об утечке информации или ее искажении в информационной системе;

5.1.4. нарушение печати на хранилище с ключевыми носителями или на техническом средстве с СКЗИ;

5.1.5. временный бесконтрольный доступ посторонних лиц к ключевым носителям или техническим средствам с СКЗИ;

5.1.6. иные случаи подозрения компрометации криптографических ключей.

5.2. В случае подозрения в компрометации криптографических ключей, работник Университета должен немедленно прекратить эксплуатацию СКЗИ и сообщить об этом ответственному работнику. Возобновление работы возможно только после замены криптографических ключей.

5.3. Скомпрометированные криптографические ключи подлежат уничтожению.

ГЛАВА 6
УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

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

6.2. Уничтожение криптографических ключей на ключевых носителях производятся комиссией в составе председателя и членов комиссии, назначенной ректором Университета.

6.3. 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.

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

6.4.1. установить наличие оригинала и количество копий криптографических ключей;

6.4.2. проверить внешнюю целостность каждого ключевого носителя;

6.4.3. идентифицировать каждый ключевой носитель;

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

6.4.5. произвести уничтожение криптографических ключей.

6.5. По факту уничтожения криптографических ключей составляется Акт уничтожения.

6.6. Акт подписывается председателем и членами комиссии.

6.7. Акты уничтожения криптографических ключей хранятся у специалиста по защите информации.

ГЛАВА 7
ОБЯЗАННОСТИ РАБОТНИКОВ ПРИ ОБРАЩЕНИИ С СКЗИ

7.1. При работе с СКЗИ работник Университета, осуществляющий эксплуатацию СКЗИ, выполняет следующие функции:

7.1.1. производит учет СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей и ключевых документов;

7.1.2. производит учет работников Университета, имеющих разрешение на работу с СКЗИ;

7.1.3. контролирует соблюдение условий использования СКЗИ;

7.1.4. проводит расследования и составляет заключения по фактам нарушений условий использования СКЗИ;

7.1.5. осуществляет разработку и обеспечение мер по предотвращению возможных нежелательных последствий таких нарушений;

7.1.6. обучает работников Университета правилам работы с СКЗИ и правилам хранения СКЗИ, ключевых носителей и ключевых документов;

7.1.7. не разглашает конфиденциальную информацию, к которой он допущен, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;

7.1.8. соблюдает требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;

7.1.9. обеспечивать сохранность и конфиденциальность ключевой информации при хранении;

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

7.1.11. незамедлительно уведомляет ответственного работника о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, в которых хранятся СКЗИ, и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

ГЛАВА 8
ТРЕБОВАНИЯ И ОТВЕТСТВЕННОСТЬ

8.1. 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.

8.2. В случае изменения действующего законодательства Республики Беларусь в части, касающейся настоящей Политики, Политика подлежит приведению в соответствие с нормами законодательства. Изменения в существующий документ не вносятся, Политика переиздается и утверждается заново. Ответственным за поддержание настоящей Политики в актуальном состоянии является начальник центра информационных технологий.