**Об утверждении Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами, а также Требований, предъявляемых кредитными бюро к поставщикам информации и получателям кредитных отчетов в соответствии с подпунктом 11) пункта 2 и подпунктом 9) пункта 3 статьи 27 Закона Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан"**

Постановление Правления Национального Банка Республики Казахстан от 27 сентября 2018 года № 228. Зарегистрировано в Министерстве юстиции Республики Казахстан 6 ноября 2018 года № 17702

В соответствии с Законом Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан" Правление Национального Банка Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Утвердить:

1) Требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами, согласно приложению 1 к настоящему постановлению;

2) Требования, предъявляемые кредитными бюро к поставщикам информации и получателям кредитных отчетов в соответствии с подпунктом 11) пункта 2 и подпунктом 9) пункта 3 статьи 27 Закона Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан", согласно приложению 2 к настоящему постановлению.

2. Признать утратившими силу нормативные правовые акты Республики Казахстан, а также структурные элементы некоторых нормативных правовых актов Республики Казахстан по перечню согласно приложению 3 к настоящему постановлению.

3. Управлению информационных угроз и киберзащиты (Перминов Р.В.) в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом (Сарсенова Н.В.) государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) в течение десяти календарных дней со дня государственной регистрации настоящего постановления его направление на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения " Республиканский центр правовой информации" для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) размещение настоящего постановления на официальном интернет-ресурсе Национального Банка Республики Казахстан после его официального опубликования;

4) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент сведений об исполнении мероприятий, предусмотренных подпунктами 2), 3) настоящего пункта и пунктом 4 настоящего постановления.

4. Управлению по защите прав потребителей финансовых услуг и внешних коммуникаций (Терентьев А.Л.) обеспечить в течение десяти календарных дней после государственной регистрации настоящего постановления направление его копии на официальное опубликование в периодические печатные издания.

5. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Национального Банка Республики Казахстан Смолякова О.А.

6. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

*Председатель*
*Национального Банка* *Д. Акишев*

Приложение 1
к постановлению Правления
Национального Банка
Республики Казахстан
от 27 сентября 2018 года № 228

# Требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами

## Глава 1. Общие положения

1. Настоящие Требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами, (далее – Требования) разработаны в соответствии с Законом Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан" (далее - Закон о кредитных бюро) и устанавливают требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами.

2. В Требованиях используются понятия, предусмотренные Законом о кредитных бюро, а также следующие понятия:

1) поставщики информации - поставщики информации, указанные в подпункте 1) пункта 1 статьи 18 Закона о кредитных бюро;

2) информационный актив - совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки;

3) информационно-коммуникационная инфраструктура (далее - информационная инфраструктура) - совокупность объектов информационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

4) информационная безопасность - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

5) риск информационной безопасности - вероятное возникновение ущерба вследствие нарушения конфиденциальности, преднамеренного нарушения целостности или доступности информационных активов кредитного бюро;

6) обеспечение информационной безопасности - процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов кредитного бюро;

7) инцидент информационной безопасности - отдельно или серийно возникающие сбои в работе информационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов кредитного бюро;

8) привилегированная учетная запись - учетная запись в информационной системе, обладающая привилегиями создания, удаления и изменения прав доступа других учетных записей;

9) аудиторский след - хронологическая последовательность записей, которые содержат доказательства изменения данных в результате выполнения функции информационной системы;

10) аутентификация - подтверждение подлинности субъекта или объекта доступа к информационной системе путем определения соответствия предъявленных реквизитов доступа;

11) бизнес-процесс - совокупность взаимосвязанных мероприятий или задач, направленных на создание определенного продукта или услуги для внешнего (клиент) или внутреннего (работник, подразделение кредитного бюро, другой бизнес-процесс) потребителя;

12) виртуальная среда - вычислительные ресурсы или их логическое объединение, абстрагированное от аппаратной реализации, обеспечивающие логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе;

13) центр обработки данных - специально выделенное помещение, в котором размещено серверное и коммуникационное оборудование информационной инфраструктуры кредитного бюро. Центр обработки данных подразделяется на основной и резервный;

14) ответственное лицо - работник получателя кредитных отчетов, имеющий доступ к кредитным отчетам;

15) рабочая станция - персональный компьютер, используемый для доступа к информационной системе кредитного бюро;

16) бизнес-владелец информационной системы кредитного бюро - подразделение ( работник) кредитного бюро, являющееся (являющийся) владельцем основного бизнес-процесса, который автоматизирует информационная система кредитного бюро;

17) получатели кредитных отчетов - получатели кредитных отчетов, указанные в подпункте 1) части первой пункта 1 статьи 20 Закона о кредитных бюро;

18) доступ - возможность использования информационных активов;

19) оператор - работник, отвечающий за корректность ввода информации в информационную систему кредитного бюро;

20) резервная копия - копия данных на носителе информации, предназначенная для восстановления данных в оригинальном или новом месте их расположения в случае необходимости;

21) обеспечение технической безопасности - процесс обеспечения безопасности кредитного бюро с использованием технических средств (системы охранной и

пожарной сигнализации, контроля и управления доступом, видеонаблюдения, пожаротушения, контроля температурного режима и влажности в центре обработки данных);

22) технологическая учетная запись - учетная запись в информационной системе, предназначенная для аутентификации между информационными системами;

23) корректирующая мера - набор организационных и технических мероприятий, направленных на исправление существующей проблемы в процессе обеспечения информационной безопасности либо последствий ее нарушения;

24) уполномоченный орган - уполномоченный орган по регулированию, контролю и надзору финансового рынка и финансовых организаций.

## Глава 2. Требования к использованию информационно-коммуникационных технологий

3. Кредитное бюро осуществляет разработку информационной системы (далее – информационная система кредитного бюро), обеспечивающей:

1) получение информации от поставщика информации;

2) формирование базы данных кредитных историй;

3) формирование, выдачу и хранение кредитных отчетов;

4) идентификацию и аутентификацию пользователей информационной системы кредитного бюро;

5) ведение аудиторского следа информационной системы кредитного бюро.

4. Информационная система кредитного бюро соответствует следующим требованиям:

1) осуществление разработки, внедрения и сопровождения информационной системы кредитного бюро (или адаптация готового продукта) на основании технического задания и в соответствии с внутренними документами кредитного бюро, регламентирующими этапы и порядок разработки, внесения изменений, тестирования, приема и ввода в промышленную эксплуатацию, а также документирование всех этапов;

2) обеспечение разграничения прав доступа пользователей информационной системы кредитного бюро;

3) обеспечение управления учетными записями информационной системы кредитного бюро;

4) обеспечение информационной безопасности защищаемых данных информационной системы кредитного бюро.

5. Кредитное бюро обеспечивает наличие и разделение сред разработки, тестирования и промышленной эксплуатации информационной системы кредитного бюро таким образом, чтобы изменения, внесенные в информационную систему

кредитного бюро в любой из этих сред, не оказывали влияния на информационную систему кредитного бюро, расположенную в другой среде. Разработка и доработка информационной системы кредитного бюро не осуществляется в среде промышленной эксплуатации.

6. Сторонние организации и работники подразделения по информационным технологиям, осуществляющие разработку программного обеспечения, не имеют доступ к переносу изменений информационной системы кредитного бюро в среде промышленной эксплуатации, а также не имеют администраторский доступ к информационной системе кредитного бюро в среде промышленной эксплуатации.

7. Перед вводом информационной системы кредитного бюро в промышленную эксплуатацию настройки, установленные в ней по умолчанию, изменяются на настройки, соответствующие требованиям к информационной безопасности, определенным внутренними документами кредитного бюро. Указанные настройки включают замену паролей, используемых при тестировании, а также удаление всех тестовых учетных записей.

8. Исходные коды (при наличии) и исполняемые модули информационной системы кредитного бюро хранятся в защищенном хранилище программного обеспечения, которое ведется в пригодном для их восстановления виде.

9. В информационной системе кредитного бюро обеспечивается ведение аудиторского следа, который отражает следующее:

1) события установления соединений, идентификации, аутентификации и авторизации (успешные и неуспешные);

2) события изменения хранящихся данных;

3) события модификации настроек безопасности;

4) события модификации групп пользователей и их полномочий;

5) события модификации учетных записей пользователей и их полномочий;

6) события, отражающие установку обновлений и (или) изменений в информационной системе;

7) события изменения параметров ведения аудиторского следа;

8) события изменений системных параметров.

10. Формат аудиторского следа включает следующую информацию:

1) идентификатор (логин) пользователя, совершившего действие;

2) дата и время совершения действия;

3) наименования объектов, с которыми проводилось действие;

4) тип или название совершенного действия администратора или конечного пользователя информационной системы;

5) результат действия (успешно или не успешно).

11. Срок хранения аудиторского следа составляет не менее 3 (трех) месяцев в оперативном доступе и не менее 1 (одного) года в архивном доступе. Допускается

хранение аудиторского следа в специализированной информационной системе хранения, обработки и анализа событий.

12. Кредитное бюро обеспечивает неизменность аудиторского следа как организационными, так и техническими средствами. Администраторам информационной системы предоставляется доступ только на перенос журналов аудиторского следа в архив.

13. Центр обработки данных кредитного бюро соответствует следующим требованиям:

1) система бесперебойного электроснабжения обеспечивается двумя или более независимыми вводами электрических сетей, а также автоматически подключаемыми резервными устройствами питания, обеспечивающими автономное электроснабжение в течение не менее двадцати четырех часов;

2) наличие двух или более каналов передачи данных от независимых провайдеров телекоммуникационных услуг, подведенных в здание разными путями, в основном центре обработки данных, а также не менее двух каналов связи в резервном центре обработки данных. Пропускная способность каналов связи обеспечивает предоставление услуг в соответствии с условиями договоров о предоставлении информации и договоров о получении кредитных отчетов.

14. Кредитное бюро в целях обеспечения устойчивого функционирования информационной системы кредитного бюро соблюдает следующие требования:

1) информационная система кредитного бюро функционирует на серверной системе , обеспечивающей возможность проведения профилактических работ без прерывания функционирования ее основных сервисов. При использовании технологий виртуализации аппаратных мощностей, виртуальные основные и резервные серверы подлежат размещению на раздельных физических серверах;

2) резервный центр обработки данных кредитного бюро размещается вне местонахождения кредитного бюро и обеспечивает восстановление работы информационной системы кредитного бюро в срок, не превышающий двенадцати часов с момента прекращения работы основного центра обработки данных.

15. Поставщик информации при подключении к информационной системе кредитного бюро использует рабочую станцию:

1) соответствующую требованиям кредитного бюро, отраженным в договоре о предоставлении информации;

2) защищенную лицензионным антивирусным программным обеспечением с актуальными антивирусными базами.

16. Получатель кредитных отчетов при подключении к информационной системе кредитного бюро:

1) обеспечивает наличие одной или нескольких рабочих станций, используемых для подключения только к информационной системе кредитного бюро;

2) обеспечивает защиту рабочих станций лицензионным антивирусным программным обеспечением с актуальными антивирусными базами.

17. В случае автоматизации процессов передачи информации поставщиком информации кредитному бюро и передачи кредитных отчетов кредитным бюро получателю кредитных отчетов, требования пунктов 15 и 16 Требований не распространяются на поставщиков информации и получателей кредитных отчетов.

## Глава 3. Требования к обеспечению информационной безопасности при организации деятельности кредитных бюро

### Параграф 1. Требования к организации системы управления информационной безопасностью

18. Кредитное бюро обеспечивает информационную безопасность защищенной информации при ее получении, хранении и обработке, а также при подготовке и выдаче кредитных отчетов.

19. Кредитное бюро обеспечивает создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления кредитного бюро, предназначенной для управления процессом обеспечения информационной безопасности.

20. Система управления информационной безопасностью обеспечивает защиту информационных активов кредитного бюро, допускающую минимальный уровень потенциального ущерба для бизнес-процессов кредитного бюро.

21. Кредитное бюро в целях обеспечения надлежащего уровня системы управления информационной безопасностью, ее развития и улучшения, обеспечивает наличие внутренних документов, определяющих:

1) политику информационной безопасности, включающую:

цели, задачи и основные принципы построения системы управления информационной безопасностью;

область действия системы управления информационной безопасностью;

ответственность в рамках системы управления информационной безопасностью;

распространение и обеспечение доступности политики информационной безопасности;

условия к пересмотру политики информационной безопасности;

2) правила управления информационными активами, включающие:

основные требования к информации с указанием уровней конфиденциальности;

требование по маркировке и паспортизации активов;

порядок обращения с информацией с учетом уровней конфиденциальности;

3) порядок резервного копирования (архивирования), включающий:

требования к резервному и архивному копированию;

порядок тестирования резервных копий;

4) методику оценки и управления рисками информационной безопасности, включающую:

процесс оценки и обработки рисков информационной безопасности;

критерии приемлемости рисков информационной безопасности;

план обработки рисков информационной безопасности;

отчет об оценке и обработке рисков информационной безопасности;

5) процедуры по ограничению доступа и обязанности пользователей информационной системы (операторов, администраторов информационных систем), включающие:

порядок прекращения или изменения функциональных обязанностей, включающий требования о неразглашении конфиденциальной информации после завершения действия трудового договора;

порядок обучения и повышения осведомленности;

порядок контроля доступа к информации, информационным системам, сетям, сервисам, оборудованию и в помещения;

условия регулярного пересмотра прав доступа;

требование к управлению пользовательскими и привилегированными правами доступа;

порядок технической реализации предоставления, изменения, удаления прав доступа;

6) порядок работы с информационной системой кредитного бюро, включающий:

процедуры разработки и управления изменениями информационной системы кредитного бюро;

права и обязанности операторов и администраторов информационной системы кредитного бюро;

7) процедуры управления инцидентами информационной безопасности, включающие:

классификацию инцидентов, порядок оповещения об инцидентах с указанием лиц, подлежащих оповещению;

порядок реагирования и обработки инцидентов;

правила защиты информационных активов от вредоносного программного обеспечения.

22. Участниками системы управления информационной безопасностью кредитного бюро являются:

1) орган управления;

2) исполнительный орган;

3) коллегиальный орган, уполномоченный принимать решения по задачам обеспечения информационной безопасности (далее – коллегиальный орган);

4) подразделение по управлению рисками;

5) подразделение по информационной безопасности;

6) подразделение по информационным технологиям;

7) подразделение по безопасности;

8) подразделение по работе с персоналом;

9) юридическое подразделение;

10) иные подразделения.

Допускается осуществление функций подразделений, указанных в подпунктах 4), 5) , 6), 7), 8) и 9) настоящего пункта, ответственными работниками в соответствии с их функциональными обязанностями.

23. Кредитное бюро при создании и функционировании системы управления информационной безопасностью обеспечивает независимость подразделений по информационной безопасности и подразделения по информационным технологиям посредством их подчинения разным членам исполнительного органа кредитного бюро или напрямую руководителю исполнительного органа кредитного бюро.

24. Орган управления кредитного бюро утверждает политику информационной безопасности.

25. Орган управления кредитного бюро утверждает перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну (далее – защищаемая информация), и порядок работы с защищаемой информацией.

26. Исполнительный орган кредитного бюро утверждает внутренние документы, регламентирующие процесс управления информационной безопасностью, порядок и периодичность пересмотра которых определяется внутренними документами кредитного бюро.

27. Кредитное бюро создает коллегиальный орган, в состав которого входят представители подразделения по информационной безопасности, подразделения по управлению рисками, подразделения по информационным технологиям, а также при необходимости представители других подразделений кредитного бюро. Руководителем коллегиального органа назначается руководитель исполнительного органа кредитного бюро либо член исполнительного органа кредитного бюро, курирующий деятельность подразделения по информационной безопасности.

28. Подразделение по управлению рисками отвечает за организацию и координацию процесса управления рисками информационной безопасности и осуществляет следующие функции:

1) разработка, внедрение и постоянное развитие системы управления рисками информационной безопасности;

2) разработка процедур по управлению рисками информационной безопасности;

3) анализ процессов в области информационной безопасности;

4) мониторинг и оценка уровня рисков информационной безопасности.

29. Подразделение по информационной безопасности в целях обеспечения конфиденциальности, целостности и доступности информации кредитного бюро осуществляет следующие функции:

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений кредитного бюро по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) разрабатывает политику информационной безопасности кредитного бюро;

3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности кредитного бюро;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности кредитного бюро, в рамках своих полномочий;

5) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

6) осуществляет анализ информации об инцидентах информационной безопасности;

7) подготавливает предложения для принятия коллегиальным органом решения по вопросам информационной безопасности;

8) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности кредитного бюро, а также предоставление доступа к ним;

9) определяет ограничения по использованию привилегированных учетных записей;

10) организует и проводит мероприятия по обеспечению осведомленности работников кредитного бюро в вопросах информационной безопасности;

11) осуществляет мониторинг состояния системы управления информационной безопасностью кредитного бюро;

12) осуществляет информирование руководства кредитного бюро о состоянии системы управления информационной безопасностью кредитного бюро.

30. Подразделение по информационным технологиям кредитного бюро разрабатывает внутренние документы определяющие:

1) общую схему информационной инфраструктуры с указанием физического расположения ее элементов;

2) перечень ответственных администраторов узлов информационной инфраструктуры (телекоммуникационных устройств, серверов и размещенных на них

операционных систем, систем управления базами данных и прикладного программного обеспечения пользователя информационной системы).

31. Кредитное бюро определяет возможность возложения на подразделение по информационной безопасности функций по обеспечению технической безопасности. Подразделение по информационной безопасности не осуществляет функции, влекущие конфликт интересов с их основными функциями.

32. Кредитное бюро определяет возможность делегирования другим подразделениям следующих функций подразделения по информационной безопасности :

1) внедрение и администрирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности кредитного бюро – подразделению по информационным технологиям;

2) организация и проведение мероприятий по обеспечению осведомленности работников кредитного бюро в вопросах информационной безопасности – подразделению по работе с персоналом;

3) учет и обработка событий и инцидентов информационной безопасности, связанных с нарушениями состояния информационной безопасности – подразделению по безопасности или иному подразделению, независимому от подразделения по информационным технологиям.

33. Подразделение по информационным технологиям осуществляет следующие функции:

1) разрабатывает схемы информационной инфраструктуры кредитного бюро;

2) обеспечивает предоставление доступа пользователям к информационным активам кредитного бюро;

3) обеспечивает конфигурирование системного и прикладного программного обеспечения кредитного бюро;

4) обеспечивает исполнение установленных внутренними документами кредитного бюро требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем кредитного бюро (включая резервирование и (или) архивирование и резервное копирование информации);

5) обеспечивает соблюдение требований информационной безопасности при выборе , внедрении, разработке и тестировании информационных систем.

34. Подразделение по безопасности осуществляет следующие функции:

1) реализует меры физической и технической безопасности в кредитном бюро, в том числе организует пропускной и внутриобъектовый режим;

2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников кредитного бюро.

35. Подразделение по работе с персоналом осуществляет следующие функции:

1) обеспечивает подписание работниками кредитного бюро, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;

2) участвует в организации процесса повышения осведомленности работников кредитного бюро в области информационной безопасности.

36. Юридическое подразделение осуществляет правовую экспертизу внутренних документов кредитного бюро по вопросам обеспечения информационной безопасности.

37. Руководители структурных подразделений кредитного бюро:

1) обеспечивают ознакомление работников с внутренними документами кредитного бюро, содержащими требования к информационной безопасности (далее – требования к информационной безопасности);

2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях.

38. Кредитное бюро определяет бизнес-владельца информационной системы кредитного бюро, который отвечает за соблюдение требований к информационной безопасности при создании, внедрении, модификации, предоставлении клиентам продуктов и услуг.

39. Работники структурных подразделений кредитного бюро:

1) отвечают за соблюдение требований к информационной безопасности, принятых в кредитном бюро;

2) контролируют исполнение требований к информационной безопасности третьими лицами, с которыми они взаимодействуют в рамках своих функциональных обязанностей, в том числе путем включения указанных требований в договоры с третьими лицами;

3) извещают своего непосредственного руководителя и подразделение по информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

## Параграф 2. Требования к организации доступа к информационным активам

40. Доступ к информации предоставляется работникам в объеме, необходимом для исполнения их функциональных обязанностей.

41. Доступ к информационной системе кредитного бюро осуществляется после идентификации и аутентификации пользователей.

42. Идентификация и аутентификация пользователей информационной системы кредитного бюро производится одним из следующих способов:

1) посредством ввода пары "учетная запись (идентификатор) – пароль" и с применением способов двухфакторной аутентификации;

2) с использованием способов биометрической и (или) криптографической и (или) аппаратной аутентификации.

43. В информационной системе кредитного бюро используются только персонализированные пользовательские учетные записи.

44. Использование технологических учетных записей допускается в соответствии с перечнем таких учетных записей для каждой информационной системы с указанием лиц, персонально ответственных за их использование и актуальность, утверждаемым руководителем подразделения по информационным технологиям по согласованию с руководителем подразделения по информационной безопасности.

45. В информационной системе кредитного бюро применяются функции по управлению учетными записями и паролями, а также блокировке учетных записей пользователей, определяемые внутренним документом кредитного бюро.

46. Предоставление физического доступа к информационным активам кредитного бюро осуществляется в соответствии с внутренними документами кредитного бюро.

## Параграф 3. Требования к обеспечению информационной безопасности информационной системы кредитного бюро

47. Информационная безопасность информационной системы кредитного бюро обеспечивается путем:

1) защиты информации при ее обработке, хранении и передаче;

2) резервирования данных на стороне кредитного бюро;

3) наличия процедур восстановления информационной системы кредитного бюро после сбоев и отказов оборудования;

4) установления криптографической защиты трафика между кредитным бюро и поставщиком информации и (или) получателем кредитных отчетов.

48. Кредитное бюро обеспечивает антивирусную защиту информационной инфраструктуры в порядке, установленном внутренним документом кредитного бюро.

49. Подразделение по информационным технологиям определяет порядок внесения изменений информационных систем по согласованию с подразделением по информационной безопасности.

50. Обновления безопасности информационных систем, устраняющие критичные уязвимости, устанавливаются не позднее одного месяца со дня их публикации и распространения производителем, за исключением случаев, согласованных с подразделением по информационной безопасности.

51. Обновления информационной системы кредитного бюро до установки в промышленную среду проходят испытания в тестовой среде.

52. Кредитное бюро обеспечивает резервное хранение данных информационной системы кредитного бюро, ее файлов и настроек, которое обеспечивает восстановление ее работоспособной копии.

53. Порядок и периодичность резервного копирования, хранения, восстановления информации, периодичность тестирования восстановления работоспособности информационной системы кредитного бюро из резервных копий определяются внутренним документом кредитного бюро.

## Параграф 4. Требования к процессу обеспечения защиты рабочих станций кредитного бюро

54. Кредитным бюро определяется перечень программного обеспечения и оборудования, разрешенных к использованию для работы с информационной системой кредитного бюро.

55. На рабочие станции не устанавливается программное обеспечение, не предназначенное для исполнения функциональных обязанностей работников кредитного бюро.

56. Внутренними документами кредитного бюро определяются организационные и технические меры, обеспечивающие защиту рабочих станций, а также носителей информации и сетевых ресурсов, используемых для работы с информационной системой кредитного бюро.

57. В кредитном бюро определяются и внедряются организационные и технические меры, запрещающие пользователям проводить самостоятельно установку и настройку программного обеспечения, рабочих станций и периферийного оборудования.

58. Пользователям информационной системы кредитного бюро не предоставляются права локального администратора или аналогичные им права, за исключением случаев, когда такие права необходимы для функционирования программного обеспечения, автоматизирующего функции, исполняемые пользователями.

59. Отдельным группам пользователей предоставляется право самостоятельной установки и настройки программного обеспечения и оборудования в случаях, когда это необходимо для исполнения служебных обязанностей. Указанным группам пользователей предоставляются права локального администратора или аналогичные им права.

60. Перечень пользователей, указанных в пунктах 58 и 59 Требований, формируется , актуализируется и утверждается руководителем подразделения по информационным технологиям по согласованию с подразделением по информационной безопасности. В случае предоставления пользователям дополнительных прав в соответствии с пунктами 58 и 59 Требований подразделение по информационной безопасности осуществляет контроль их использования.

## Параграф 5. Требования к процессу обеспечения физической безопасности центров обработки данных кредитных бюро

61. Порядок обеспечения физической безопасности центров обработки данных определяется внутренним документом.

62. Центр обработки данных оснащается следующими системами технической безопасности:

1) система контроля и управления доступом;

2) охранная сигнализация;

3) пожарная сигнализация;

4) система автоматического пожаротушения;

5) система поддержания заданных параметров температуры и влажности;

6) система видеонаблюдения;

7) система бесперебойного электропитания.

63. Доступ в центр обработки данных предоставляется работникам кредитного бюро, перечень которых утверждается руководителем подразделения по информационным технологиям по согласованию с подразделением по информационной безопасности.

64. Кредитное бюро ведет журнал системы контроля и управления доступом в центр обработки данных, который хранится не менее 1 (одного) года.

65. Система автоматического пожаротушения центра обработки данных обеспечивает устранение возгорания по всему объему помещения и имеет резервный запас.

66. Система видеонаблюдения центра обработки данных обеспечивает наблюдение за всеми входами в центр обработки данных. В центре обработки данных расстановка видеокамер исключает наличие зон внутри помещения центра обработки данных и перед его входом, не покрытых видеонаблюдением.

67. Запись событий системой видеонаблюдения центра обработки данных ведется непрерывно или с использованием детектора движения.

68. Архив системы видеонаблюдения центра обработки данных хранится не менее 3 (трех) месяцев.

69. В целях предотвращения несанкционированного физического доступа к серверам и активному сетевому оборудованию, находящемуся вне центра обработки данных, внутренними документами кредитного бюро определяются меры по обеспечению их безопасности.

## Параграф 6. Требования к порядку мониторинга и обработки информации об инцидентах информационной безопасности в кредитных бюро

70. Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации и систематизации.

71. Кредитное бюро обеспечивает целостность информации об инцидентах информационной безопасности.

72. В случае, если кредитным бюро определена необходимость мониторинга отдельных источников событий информационной безопасности во внерабочее время, создается круглосуточная служба мониторинга.

73. Кредитным бюро определяется порядок информирования о произошедшем инциденте информационной безопасности руководящих работников и подразделений кредитного бюро.

74. Кредитным бюро определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий.

75. В кредитном бюро ведется журнал учета инцидентов информационной безопасности с отражением информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах, на бумажном носителе либо в электронном виде.

76. По результатам обработки инцидента информационной безопасности кредитным бюро проводится всесторонний анализ причин возникновения инцидента информационной безопасности, его механизма и последствий. При сборе технических данных с программно-технических средств, вовлеченных в инцидент информационной безопасности, обеспечивается сохранность и неизменность собранных данных.

77. Информация об инциденте информационной безопасности, а также предложения по принятию корректирующих мер в целях снижения вероятности и возможного ущерба от повторного инцидента информационной безопасности хранятся в кредитном бюро.

78. Для инцидентов информационной безопасности, вероятность возникновения которых высока и не может быть снижена в короткие сроки, кредитным бюро разрабатываются внутренние документы, описывающие алгоритм обработки данных инцидентов информационной безопасности, типовых неотложных мер по локализации инцидентов информационной безопасности и их последствий, методов обработки инцидентов информационной безопасности.

## Параграф 7. Требования к предоставлению информации о состоянии информационной безопасности кредитных бюро

79. Кредитное бюро ежегодно, не позднее 20 января года, следующего за отчетным годом, представляет в уполномоченный орган информацию о состоянии системы

управления информационной безопасностью и ее соответствии Требованиям (далее - Информация).

80. Информация включает сведения о (об):

1) сфере действия системы управления информационной безопасностью кредитного бюро и ее участниках с указанием соответствия их функционала Требованиям;

2) наличии документов, регламентирующих создание и функционирование системы управления информационной безопасностью;

3) наличии и количественном составе программно-технических средств, используемых для обеспечения информационной безопасности;

4) имеющихся в договорах о предоставлении услуг, заключенных с операторами связи, условиях и обязательствах по обеспечению информационной безопасности;

5) наличии, материально-технической обеспеченности и готовности резервных центров обработки данных;

6) проведенных мероприятиях по приведению системы управления информационной безопасностью и информационных активов кредитного бюро в соответствие с Требованиями.

81. Информация составляется в произвольной форме и представляется в уполномоченный орган в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.

## Глава 4. Требования к обеспечению информационной безопасности при организации деятельности поставщиков информации

82. Поставщик информации обеспечивает целостность и конфиденциальность информации, передаваемой в информационную систему кредитного бюро.

83. Поставщик информации обеспечивает надлежащий уровень информационной безопасности в соответствии с условиями договора о предоставлении информации.

84. Поставщик информации обеспечивает исполнение организационно-технических , технологических требований и мер, необходимых для функционирования и защиты системного и прикладного программного обеспечения, используемого для взаимодействия с информационной системой кредитного бюро.

85. При использовании оборудования для работы с информационной системой кредитного бюро учитывается необходимость его защиты от несанкционированного доступа, а также защиты носителей информации и сетевых ресурсов.

86. Поставщик информации назначает оператора (операторов).

87. Поставщик информации обеспечивает наличие подписанных обязательств оператора (операторов) о неразглашении и нераспространении информации, ставшей им известной в процессе исполнения ими функциональных обязанностей.

88. Поставщик информации обеспечивает наличие внутренних документов ( включая должностные инструкции), определяющих порядок назначения оператора ( операторов), его (их) права и ответственность.

89. Доступ к информации предоставляется работникам поставщиков информации в объеме, необходимом для исполнения их функциональных обязанностей.

90. Учетная запись оператора, по которой он идентифицируется в информационной системе кредитного бюро, принадлежит конкретному физическому лицу.

91. Поставщик информации по запросу уполномоченного органа предоставляет сведения, подтверждающие его соответствие требованиям, предусмотренным договором о предоставлении информации.

92. Операционная система рабочей станции обеспечивает функции идентификации и аутентификации пользователя, а также разграничения прав доступа пользователей и авторизацию в соответствии с назначенными правами.

93. При использовании рабочей станции для подключения к информационной системе кредитного бюро одновременное подключение к другим ресурсам сети Интернет не производится.

94. Работники поставщика информации обеспечивают конфиденциальность персональных идентификационных и аутентификационных данных, используемых для доступа к информационным системам.

95. Работники поставщика информации обеспечивают конфиденциальность информации, ставшей им известной в процессе использования информационной системы кредитного бюро.

## Глава 5. Требования к обеспечению информационной безопасности при организации деятельности получателей кредитных отчетов

96. Получатель кредитного отчета обеспечивает конфиденциальность и целостность информации, получаемой из информационной системы кредитного бюро.

97. Получатель кредитного отчета обеспечивает надлежащий уровень информационной безопасности в соответствии с условиями договора о получении кредитных отчетов.

98. Получатель кредитного отчета обеспечивает исполнение организационно-технических, технологических требований и мер, необходимых для функционирования и защиты системного и прикладного программного обеспечения, используемого для взаимодействия с информационной системой кредитного бюро и обработки получаемой из нее информации.

99. При использовании оборудования для работы с информационной системой кредитного бюро учитывается необходимость его защиты от несанкционированного доступа, а также защиты носителей информации и сетевых ресурсов, используемых для работы с информационной системой кредитного бюро.

100. Получатель кредитного отчета определяет и утверждает перечень ответственных лиц.

101. Получатель кредитного отчета обеспечивает наличие подписанных ответственными (ответственным) лицами (лицом) организации обязательств о неразглашении и нераспространении информации, ставшей им известной в процессе исполнения ими функциональных обязанностей.

102. Получатель кредитного отчета обеспечивает наличие внутренних документов, определяющих порядок определения и утверждения перечня ответственных лиц, их права и ответственность (включая должностные инструкции).

103. Доступ к информации предоставляется работникам в объеме, необходимом для исполнения их функциональных обязанностей.

104. Учетная запись ответственного лица, по которой он идентифицируется в информационной системе кредитного бюро, соответствует конкретному физическому лицу.

105. Получатель кредитного отчета проводит плановые и внеплановые проверки соответствия рабочих станций Требованиям и внутренним документам получателя кредитного отчета, регламентирующим информационную безопасность.

106. Получатель кредитного отчета по запросу уполномоченного органа представляет сведения, подтверждающие его соответствие требованиям, предусмотренным в договоре о получении кредитных отчетов.

107. Операционная система рабочей станции обеспечивает функции идентификации и аутентификации пользователя, а также разграничения прав доступа пользователей и авторизации в соответствии с назначенными правами.

108. Получатель кредитных отчетов использует собственную рабочую станцию.

109. При использовании рабочей станции для подключения к информационной системе кредитного бюро одновременное подключение к другим ресурсам сети Интернет не производится.

110. Работники получателя кредитных отчетов обеспечивают конфиденциальность персональных идентификационных и аутентификационных данных, используемых для доступа к информационным системам.

111. Работники получателя кредитных отчетов обеспечивают конфиденциальность информации, ставшей им известной в процессе использования информационной системы кредитного бюро.

Приложение 2
к постановлению Правления

Национального Банка
Республики Казахстан
от 27 сентября 2018 года № 228

# Требования, предъявляемые кредитными бюро к поставщикам информации и получателям кредитных отчетов в соответствии с подпунктом 11) пункта 2 и подпунктом 9) пункта 3 статьи 27 Закона Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан"

1. Настоящие Требования, предъявляемые кредитными бюро к поставщикам информации и получателям кредитных отчетов в соответствии с подпунктом 11) пункта 2 и подпунктом 9) пункта 3 статьи 27 Закона Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан (далее – Требования) разработаны в соответствии с Законом Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан" (далее - Закон о кредитных бюро) и определяют требования, предъявляемые кредитными бюро к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности поставщиков информации, являющихся индивидуальными предпринимателями или юридическими лицами, реализующими товары и услуги в кредит либо предоставляющими отсрочку платежей, систематизированные признаки которых определяются постановлением Правительства Республики Казахстан от 18 января 2005 года № 25 "Об утверждении систематизированных признаков индивидуальных предпринимателей или юридических лиц, реализующих товары и услуги в кредит либо предоставляющих отсрочки платежей" (далее – постановление № 25), субъектами естественной монополии, оказывающими коммунальные услуги, иными лицами на основании договоров о предоставлении информации (далее – поставщики информации), а также получателей кредитных отчетов, являющихся индивидуальными предпринимателями или юридическими лицами, реализующими товары и услуги в кредит либо предоставляющими отсрочку платежей, систематизированные признаки которых определяются постановлением № 25, иными лицами на основании договоров о предоставлении информации, представителями держателей облигаций в отношении кредитного отчета эмитента облигаций, с которыми заключен договор о представлении интересов держателей облигаций (далее – получатели кредитных отчетов) в соответствии с подпунктом 11) пункта 2 и подпунктом 9) пункта 3 статьи 27 Закона о кредитных бюро.

2. Требования, предъявляемые кредитными бюро к поставщикам информации и получателям кредитных отчетов, включаются в договор о предоставлении информации и договор о получении кредитных отчетов.

3. Требования, предъявляемые кредитными бюро к использованию информационно-коммуникационных технологий при организации деятельности поставщиков информации и получателей кредитных отчетов, соответствуют требованиям пунктов 15, 16 и 17 Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами, утвержденных настоящим постановлением.

4. Требования, предъявляемые кредитными бюро к обеспечению информационной безопасности при организации деятельности поставщиков информации и получателей кредитных отчетов, соответствуют требованиям глав 4 и 5 Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами, утвержденных настоящим постановлением.

Приложение 3
к постановлению Правления
Национального Банка
Республики Казахстан
от 27 сентября 2018 года № 228

## Перечень нормативных правовых актов Республики Казахстан, а также структурных элементов некоторых нормативных правовых актов Республики Казахстан, признаваемых утратившими силу

1. Постановление Правления Национального Банка Республики Казахстан от 27 мая 2015 года № 91 "Об утверждении Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 11669, опубликовано 30 июля 2015 года в информационно-правовой системе "Әділет").

2. Пункт 2 постановления Правления Национального Банка Республики Казахстан от 30 мая 2016 года № 146 "О внесении изменений и дополнения в некоторые нормативные правовые акты Республики Казахстан по вопросам сокращения разрешительных документов и упрощения разрешительных процедур ( зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14208, опубликовано 5 октября 2016 года в информационно-правовой системе "Әділет").

3. Постановление Правления Национального Банка Республики Казахстан от 14 июня 2017 года № 102 "О внесении изменений и дополнения в постановление Правления Национального Банка Республики Казахстан от 27 мая 2015 года № 91 "Об утверждении Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 15608, опубликовано 15 сентября 2017 года в Эталонном контрольном банке нормативных правовых актов Республики Казахстан).

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан