

Закон Китайской Народной Республики о борьбе с мошенничеством в телекоммуникационных сетях

(Принято на 36-м заседании Постоянного комитета 13-го Всекитайского собрания народных представителей 2 сентября 2022 г.)

оглавление оглавление

Глава 1 ОБЩИЕ
СВЕДЕНИЯ Глава II
Управление в сфере
телекоммуникаций Глава III
 Финансовое
управление Глава IV
Управление Интернетом
Глава V Комплексные
меры Глава VI
Юридическая
ответственность Глава VII

Дополнительные положения
 Правила

Глава 1 ОБЩИЕ СВЕДЕНИЯ ОБЩИЕ СВЕДЕНИЯ

Статья 1 Настоящий закон принят в соответствии с Конституцией в целях предупреждения, пресечения и наказания мошеннических действий в телекоммуникационных сетях, усиления борьбы с мошенничеством в телекоммуникационных сетях, защиты законных прав и интересов граждан и организаций, а также поддержания социальной стабильности и национальной безопасности.

Статья 2 Мошенничество с телекоммуникационными сетями, о котором говорится в настоящем Законе, означает использование незаконного владения с

целью.

Использование технологии телекоммуникационных сетей позволяет дистанционно, бесконтактно и т. д. мошенничать с государственной и частной собственностью.

Статья 3 Настоящий Закон применяется для борьбы и управления мошенническими действиями в телекоммуникационных сетях, совершенными на территории Китайской Народной Республики или гражданами Китайской Народной Республики за пределами территории Китайской Народной Республики.

Если организация или физическое лицо за пределами страны совершает мошенничество с телекоммуникационными сетями на территории Китайской Народной Республики, или предоставляет продукты, услуги или другую помощь другим лицам для совершения мошенничества с телекоммуникационными сетями на территории Китайской Народной Республики, такая организация или физическое лицо должны быть рассмотрены и привлечены к ответственности в соответствии с положениями настоящего Закона.

Статья IV борьба с мошенничеством в телекоммуникационных сетях придерживается ориентированного на людей, комплексного развития и безопасности; придерживается системной концепции, верховенства закона, сосредоточившись на источнике управления, всестороннего управления; придерживается координации, контроля толпы, полного осуществления мер по борьбе, предотвращению и контролю, а также усилению социальной пропаганды, образования и профилактики; придерживается профилактики и лечения точности, и для обеспечения нормальной производственной и деловой деятельности и удобства жизни людей.

Статья 5 Борьба с мошенничеством в телекоммуникационных сетях должна осуществляться в соответствии с законом и обеспечивать соблюдение законных прав и интересов граждан и организаций.

Соответствующие департаменты и подразделения, отдельные лица должны быть в процессе борьбы с мошенничеством в телекоммуникационных сетях известны государственные секреты, коммерческие тайны и личная жизнь, личная информация должна быть конфиденциальной.

Статья 6 Государственный совет создает рабочий механизм по борьбе с мошенничеством в телекоммуникационных сетях для координации работы по борьбе с мошенничеством и управлению им.

Местные народные правительства всех уровней организуют и возглавляют работу по борьбе с мошенничеством в телекоммуникационных сетях на своих административных территориях, определяют цели, задачи и механизмы работы по борьбе с мошенничеством в телекоммуникационных сетях, а также осуществляют комплексное управление.

Органы общественной безопасности возглавляют работу по борьбе с мошенничеством в телекоммуникационных сетях, финансах, телекоммуникациях и интернет-информации,

Надзор за рынком и другие соответствующие департаменты в соответствии со своими обязанностями выполняют основные обязанности по надзору, отвечая за лидера отрасли (с) работа по борьбе с мошенничеством в телекоммуникационных сетях в этом домене.

Народные суды и народные прокуратуры выполняют функции суда и прокуратуры, предотвращают и наказывают мошеннические действия в телекоммуникационных сетях в соответствии с законом.

Операторы телекоммуникационного бизнеса, банковские финансовые учреждения, небанковские платежные учреждения и поставщики интернет-услуг взяли на себя ответственность за предотвращение и контроль рисков, создали механизмы внутреннего контроля и системы ответственности за противодействие мошенничеству в телекоммуникационных сетях, а также усилили оценку риска мошенничества в новом бизнесе с точки зрения безопасности.

Статья 7 Соответствующие департаменты и подразделения, занимающиеся борьбой с мошенничеством в телекоммуникационных сетях, должны тесно сотрудничать для достижения межотраслевого и межрегионального взаимодействия, быстрого установления связей и укрепления профессиональных команд для эффективной борьбы с мошенничеством в телекоммуникационных сетях и управления этой деятельностью.

Статья 8 Народные правительства всех уровней и соответствующие ведомства усиливают пропаганду борьбы с мошенничеством в телекоммуникационных сетях, популяризируют соответствующие законы и знания, повышают осведомленность населения о различных видах мошенничества в телекоммуникационных сетях и способность выявлять мошенничество.

Администрация образования, надзор за рынком, гражданские дела и другие соответствующие департаменты и комитеты сельских жителей, комитеты жителей, должны быть объединены с распределением жертв мошенничества телекоммуникационных сетей и другими характеристиками, усилить пропаганду и обучение пожилых людей, молодежи и других групп, повысить актуальность и точность пропаганды и обучения против мошенничества телекоммуникационных сетей, и проводить пропаганду и обучение против мошенничества телекоммуникационных сетей в школах, предприятиях, сообществах, сельских районах, семьях и других мероприятиях.

Подразделения должны усилить внутреннюю профилактику мошенничества в телекоммуникационных сетях и обучать персонал предотвращению мошенничества в телекоммуникационных сетях; частные лица должны усилить осведомленность о предотвращении мошенничества в телекоммуникационных сетях. Подразделения и отдельные лица должны помогать и сотрудничать с соответствующими департаментами в проведении работы по борьбе с мошенничеством в телекоммуникационных сетях в соответствии с положениями настоящего Закона.

глава Управление
телекоммун

Статья 9 Операторы телекоммуникационного бизнеса должны полностью внедрить систему регистрации реальной идентификационной информации телефонных пользователей в соответствии с законом.

Базовые телекоммуникационные предприятия и предприятия по перепродаже мобильной связи должны взять на себя ответственность за управление внедрением системы реальных имен телефонных пользователей для агентов, а также указать в соглашении ответственность за регистрацию реальных имен агентов и соответствующие меры по устранению неисполнения обязательств.

Статья 10: Количество выданных телефонных карт не должно превышать пределов, установленных соответствующими национальными правилами. В случае выявления отклонений в обращении с карточками оператор телекоммуникационных услуг имеет право усилить проверку количества карточек. Проверить или отказать в использовании карты. Конкретные методы идентификации должны быть разработаны телекоммуникационным ведомством при Государственном совете. Компетентный отдел телекоммуникаций при Государственном совете организует создание механизма проверки количества карт, открытых пользователями телефонов и механизм обмена информацией о рисках, а также предоставлять пользователям удобные каналы для запроса информации о телефонных картах на их имя.

Статья XI операторов телекоммуникационного бизнеса для мониторинга выявления аномальных мошенничества пользователей телефонных карт должны быть повторно проверены, в соответствии с уровнем риска, чтобы принять дифференцированные, соответствующие меры проверки. Не в соответствии с положениями проверки или проверки не удалось, операторы телекоммуникационного бизнеса могут ограничить или приостановить функцию телефонной карты.

Статья XII Операторы телекоммуникационного бизнеса должны создать систему оценки рисков пользователей карт Интернета вещей, если оценка не пройдена, не должны продаваться карты Интернета вещей; строгая регистрация идентификационной информации пользователей карт Интернета вещей; принять эффективные технические меры для ограничения открытия функций карт Интернета вещей, использования сценариев и применимого оборудования.

Пользователь устройства приобретает IoT-карту у оператора телекоммуникационных услуг, а затем отправляет содержащуюся на IoT-карту информацию о ее оборудовании другим пользователям, идентификационные данные пользователей должны быть проверены и зарегистрированы, а объем продаж, запасы и информация о реальном имени пользователя должны быть переданы оператору телекоммуникационного бизнеса, которому принадлежит номер. Операторы телекоммуникационного бизнеса должны создать механизм мониторинга и раннего предупреждения об использовании карт IoT. Для запасов

В случае нештатного использования ситуации, обслуживание должно быть приостановлено, проведена повторная проверка личности и использования сцены или приняты другие оговоренные в договоре меры по избавлению.

Статья XIII Операторы телекоммуникационного бизнеса должны регулировать передачу реального номера звонящего и аренду телекоммуникационной линии, блокировку и перехват изменения телефонного номера и проверку отслеживаемости.

Операторы телекоммуникационных услуг должны строго регулировать передачу идентификационных номеров абонентов бюро по вводу/выводу международных услуг связи, правдиво и точно указывать пользователям страну или регион, к которому относится идентификационный номер абонента, а также выявлять и перехватывать ложные и нерегулярные вызовы внутри и между сетями.

Статья 14 Ни одно подразделение или частное лицо не может незаконно производить, торговать, предоставлять или использовать следующее оборудование или программное обеспечение:

- (i) Телефонные карты вставляются в оборудование в массовом порядке;
- (ii) Оборудование и программное обеспечение с функцией изменения номера вызывающего абонента, виртуального набора номера, а также незаконного доступа к телекоммуникационным сетям общего пользования посредством интернет-телефонии;
- (c) Пакетная система автоматического переключения учетных записей и сетевых адресов, пакетный прием платформ, обеспечивающих SMS-верификацию и голосовую верификацию;
- (d) другое оборудование и программное обеспечение, используемое для совершения мошенничества в телекоммуникационных сетях и других преступлений. Операторы телекоммуникационного бизнеса, поставщики услуг Интернета должны принимать технические меры и

При выявлении и блокировании доступа к сети незаконного оборудования и программного обеспечения, указанного в предыдущем пункте, сообщать об этом в органы общественной безопасности и соответствующие отраслевые органы.

Глава III финансовое управление

Статья 15 Банковские финансовые учреждения, небанковские платежные учреждения для клиентов открывают банковские счета, платежные счета и предоставляют платежные и расчетные услуги, а также с клиентами в период существования деловых отношений, должны создать систему должной осмотрительности клиентов, в соответствии с законом идентифицировать бенефициарного владельца, принять соответствующие меры по управлению рисками, чтобы предотвратить использование банковских счетов, платежных счетов и т.д. для мошеннических действий в телекоммуникационной сети.

Статья 16 Открытие банковских счетов и платежных счетов не должно превышать количество ограничений, установленных соответствующими государственными нормативными актами.

Банковские финансовые учреждения и небанковские платежные организации имеют право усилить проверку или отказать в открытии счета тем, у кого выявлены нестандартные ситуации с открытием счета.

Народный банк Китая и органы банковского надзора и управления Госсовета организовали соответствующие клиринговые агентства для создания механизма проверки количества открытых счетов между учреждениями и механизма обмена информацией о рисках, а также для предоставления клиентам удобных каналов для получения информации о банковских и платежных счетах на их имя. Банковские финансовые учреждения, небанковские платежные учреждения должны предоставлять информацию об открытии счетов и соответствующих рисках в соответствии с государственными нормативными актами. Соответствующая информация не может быть использована в иных целях, кроме борьбы с мошенничеством в телекоммуникационных сетях.

Статья 17 Банковские финансовые учреждения и небанковские платежные учреждения должны создать механизм предотвращения рисков и контроля за нештатными ситуациями при открытии счетов предприятий. Соответствующие департаменты финансов, телекоммуникаций, надзора за рынком, налогообложения и другие соответствующие департаменты должны создать систему обмена информацией и запросов об открытии счетов предприятий и предоставлять услуги по проверке сети.

Регистрационный орган субъектов рынка должен в соответствии с законом регистрировать выполнение идентификационной информации предприятий в их настоящих именах.

Обязанности по проверке; надзор и проверка вопросов регистрации в соответствии с правилами, а также возможных фальсификаций. Регистрация, связанная с мошенничеством, аномалиями в фокусе надзора и инспекции предприятий, отмена регистрации в соответствии с законом, в соответствии с положениями предыдущего пункта, своевременный обмен информацией; для банковских финансовых учреждений, небанковских платежных учреждений проведение должной осмотрительности клиентов и идентификации бенефициарного владельца облегчение в соответствии с законом.

Статья 18 Банковские финансовые учреждения, небанковские платежные учреждения должны усилить мониторинг банковских счетов, платежных счетов и платежно-расчетных услуг, а также создать и усовершенствовать механизм мониторинга аномальных счетов и подозрительных операций в соответствии с особенностями мошеннической деятельности телекоммуникационной сети.

Народный банк Китая координирует создание единой системы мониторинга противодействия отмыванию денег для межбанковских финансовых учреждений и небанковских платежных организаций и совместно с департаментом общественной безопасности Госсовета усовершенствовал систему отчетности о подозрительных операциях по борьбе с отмыванием денег, которая соответствует особенностям преступлений, связанных с движением средств от мошенничества в телекоммуникационных сетях.

В отношении аномальных счетов и подозрительных операций, выявленных в ходе мониторинга, банковские финансовые учреждения и небанковские платежные учреждения должны, с учетом ситуации риска, принять необходимые превентивные меры, такие как проверка операции, повторная проверка личности, задержка платежа и расчетов, ограничение или приостановка соответствующей деятельности. Банковские финансовые учреждения, небанковские платежные учреждения в соответствии с положениями первого пункта должны проводить ненормальные При мониторинге счетов и подозрительных операций может собираться необходимая информация о транзакциях, такая как адрес интернет-протокола аномального клиента, адрес сетевой карты, информация о терминалах приема платежей и информация о местонахождении оборудования. Указанная информация не может быть использована в целях, отличных от борьбы с мошенничеством в телекоммуникационных сетях, без разрешения клиента.

Статья 19 Банковские финансовые учреждения, небанковские платежные учреждения должны, согласно соответствующим положениям государства, полно и точно передавать имя торговца, непосредственно предоставляющего товары или услуги, имя получающего и оплачивающего клиента, номера счетов и другую информацию о сделке, чтобы обеспечить достоверность и полноту информации о сделке и согласованность всего процесса платежа.

Статья 20 Департамент общественной безопасности Государственного совета совместно с соответствующими ведомствами будет Система мгновенного запроса, экстренной остановки платежа, быстрого замораживания, своевременного разморозивания в электронном виде, а также кибермошенничество, а также разъяснения соответствующих условий, процедур и мер по оказанию помощи.

Если органы общественной безопасности принимают решение о принятии таких мер в соответствии с законом, банковские финансовые учреждения и небанковские платежные учреждения должны сотрудничать.

Глава IV Управление Интернетом

Статья 21 Операторы телекоммуникационного бизнеса, поставщики интернет-услуг предоставляют пользователям следующие услуги, при подписании соглашения с пользователем или для подтверждения предоставления услуг, пользователь должен по закону предоставить реальную идентификационную информацию, если пользователь не предоставляет реальную идентификационную информацию, услуги не предоставляются:

- (i) Предоставление услуг доступа в Интернет;
- (ii) Предоставление услуг по трансляции сетевых адресов, таких как веб-прокси;
- (iii) Предоставление услуг регистрации доменных имен в Интернете, хостинга серверов, аренды помещений, облачных услуг и услуг по распространению контента;
- (d) Предоставление услуг по публикации информации и программного обеспечения, или предоставление услуг по обмену мгновенными сообщениями, онлайн-торговле, онлайн-играм, публикации прямых веб-трансляций, а также рекламы и продвижения.

Статья 22 Интернет-провайдеры для мониторинга выявления аномальных счетов, связанных с мошенничеством, должны быть повторно проверены, в соответствии с соответствующими государственными правилами, чтобы принять функцию ограничения, приостановления услуг и других мер по ликвидации.

Интернет-провайдеры обязаны по требованию органов общественной безопасности и телекоммуникационных органов.

Соответствующие учетные записи в Интернете, зарегистрированные в связи с телефонными картами, виртуальными в денежном отношении телефонные карты, подлежат проверке, и в соответствии с ситуацией риска принимаются меры по ликвидации, в том числе ограничение функций, приостановка использования, закрытие учетной записи, запрет на повторную регистрацию и т. д.

Статья 23 Создание мобильных интернет-приложений должно осуществляться в соответствии с соответствующими государственными нормами и правилами в компетентном департаменте телекоммуникаций для получения лицензии или проведения процедур учета.

Лица, предоставляющие услуги по упаковке и распространению приложений, должны регистрировать и проверять реальную идентификационную информацию разработчика и оператора приложения, а также проверять функции и использование приложения.

Общественная безопасность, телекоммуникации, письмо сети и другие ведомства и операторы телекоммуникационного бизнеса, интернет-провайдеры должны укрепить платформу распространения за пределами способа загрузки и распространения приложений, связанных с мошенничеством, сосредоточиться на мониторинге, своевременном удалении.

Статья 24 Предоставление услуг по разрешению доменных имен, передаче доменных имен, преобразованию ссылок URL, должно быть в соответствии с соответствующими положениями государства, проверка регистрации доменных имен, информации о разрешении и подлинности адреса Интернет-протокола, точности, спецификации передачи доменных имен, запись и сохранение соответствующих услуг, предоставляемых в журнале информации для поддержки реализации разрешения передачи, преобразования записей отслеживания. Статья 25 Ни одно подразделение или физическое лицо не должно осуществлять мошенничество с телекоммуникационными сетями для других.

Оказывать поддержку или помощь в борьбе с мошенничеством следующим образом:

- (i) Продажа или предоставление личной информации;
- (ii) Оказание помощи другим лицам в отмывании денег, в частности, посредством операций с виртуальной валютой;
- (c) другие действия по оказанию поддержки или помощи в мошеннической деятельности в телекоммуникационной сети. Операторы телекоммуникационного бизнеса, поставщики интернет-услуг должны, согласно соответствующим государственным нормативным актам.

Следующие операции используются для поддержки и помощи при мошенничестве, и на них распространяется обязанность разумной осторожности по отслеживанию, выявлению и пресечению таких действий:

(i) Предоставление доступа в Интернет, размещение серверов, хранение данных в сети и передача данных,
Аренда линий, разрешение доменных имен и другие услуги по предоставлению сетевых ресурсов;

(ii) Предоставление услуг по продвижению сети, таких как распространение или поиск информации, реклама и продвижение, привлечение и продвижение;

(c) Предоставление услуг по производству и обслуживанию сетевых технологий и продуктов, таких как приложения и веб-сайты;

(iv) Предоставление платежных и расчетных услуг.

Статья 26 Органы общественной безопасности для рассмотрения дел о мошенничестве в телекоммуникационных сетях в соответствии с законом для получения доказательств, интернет-провайдеры должны своевременно оказывать техническую поддержку и помощь.

Интернет-провайдеры в соответствии с положениями настоящего Закона о соответствующей информации, связанной с мошенничеством, деятельность по мониторингу, найденные мошенничества, связанные с подсказками, информация о рисках должны, в соответствии с соответствующими положениями государства, в соответствии с типом риска, связанного с мошенничеством, масштабы ситуации переданы общественной безопасности, финансов, телекоммуникаций, чистого письма и других ведомств. Соответствующие департаменты должны создать и усовершенствовать механизм обратной связи, а также своевременно информировать передающее подразделение о соответствующей ситуации.

Глава V Комплексные меры

Статья 27 Органы общественной безопасности должны создавать и совершенствовать механизм борьбы с мошенничеством в телекоммуникационных сетях и регулирования его деятельности, укреплять создание специализированных групп и экспертов, а все полицейские силы и органы общественной безопасности по всему миру должны тесно сотрудничать в целях эффективного наказания мошеннических действий в телекоммуникационных сетях в соответствии с законом.

Органы общественной безопасности, получившие сообщение о мошеннической деятельности в телекоммуникационной сети или обнаружившие мошенническую деятельность в телекоммуникационной сети, подают заявление в соответствии с положениями Уголовно-процессуального закона Китайской Народной Республики

Обнаруже

ние. Статья 28 Департаменты финансов, телекоммуникаций и Интернет-информации, в соответствии со своими обязанностями, осуществляют надзор и инспекцию выполнения положений настоящего Закона банковскими финансовыми учреждениями, небанковскими платежными учреждениями, операторами телекоммуникационного бизнеса и поставщиками Интернет-услуг. Соответствующие надзорные и инспекционные мероприятия осуществляются в соответствии с законом.

Статья 29 Обработчик личной информации должен в соответствии с Законом Китайской Народной Республики о защите личной информации и другими законами регулировать работу с личной информацией, укреплять защиту личной информации и создавать превентивный механизм против использования личной информации для мошенничества в телекоммуникационных сетях.

Департаменты и подразделения, выполняющие обязанности по защите персональной информации, осуществляют ключевую защиту логистической информации, информации о сделках, информации о кредитах, медицинской информации, информации о сватовстве и другой информации, которая может быть использована при мошенничестве в телекоммуникационных сетях. Органы общественной безопасности, занимающиеся делами о мошенничестве в телекоммуникационных сетях, должны одновременно расследовать источник личной информации, использованной в преступлении, и привлекать к ответственности соответствующих лиц и подразделения в соответствии с законом.

Статья 30 Операторы телекоммуникационного бизнеса, банковские финансовые учреждения, небанковские платежные учреждения, поставщики интернет-услуг должны проводить антiteleкоммуникационную сетевую пропаганду для практиков и пользователей, в соответствующей деловой деятельности, чтобы предотвратить телекоммуникационное сетевое мошенничество, побуждающее к появлению новых средств телекоммуникационного сетевого мошенничества в области телекоммуникационного сетевого мошенничества, своевременно делать пользователю напоминания о незаконной торговле, аренде, кредитовании моей карты, счета, номера счета и т.д. Используется для мошенничества в телекоммуникационных сетях, чтобы предупредить о юридической ответственности.

Новости, радио, телевидение, культура, информационные службы Интернета и другие подразделения должны быть нацелены на сообщество, чтобы проводить пропаганду и обучение против мошенничества в телекоммуникационных сетях.

Любое подразделение или частное лицо имеет право сообщить о мошеннических действиях в телекоммуникационной сети, соответствующие отделы должны своевременно принять меры в соответствии с законом, предоставить эффективную информацию информатору в соответствии с положениями о награде и защите

Сестр

инско Статья 31 Ни одно подразделение или физическое лицо не может незаконно выдавать, продавать, сдавать в аренду или предоставлять во временное пользование телефонные карты, карты Интернета вещей, телекоммуникационные линии, SMS-порты, банковские счета, платежные счета, Интернет-счета и т.д. или оказывать помощь в проверке реального имени, а также выдавать себя за другое лицо или фиктивные агентские отношения для открытия указанных карт, счетов, счетов и т.д.

В отношении подразделений, физических лиц и соответствующих организаций, совершивших деяния, указанные в предыдущем пункте, как установлено органами общественной безопасности на муниципальном уровне округа или выше, а также получивших уголовное наказание за мошенничество в телекоммуникационных сетях или связанные с ним преступления, может быть внесено в кредитное досье в соответствии с соответствующими государственными правилами, и могут быть приняты меры по ограничению функций их соответствующих карт, счетов, номеров счетов и прекращению внебиржевого бизнеса, приостановке нового бизнеса и ограничению доступа в Интернет. Любой, кто не согласен с вышеуказанными определениями и мерами, может подать жалобу, и соответствующие ведомства должны создать и усовершенствовать каналы подачи жалоб, системы восстановления и помощи в получении кредитов. Конкретные меры должны быть предписаны департаментом общественной безопасности Государственного совета совместно с соответствующими компетентными органами.

Статья 32 Государство поддерживает операторов телекоммуникационного бизнеса, банковские финансовые учреждения, небанковские платежные учреждения и интернет-провайдеров в исследовании и разработке технологий противодействия мошенничеству в телекоммуникационных сетях, которые используются для мониторинга и выявления динамического блокирования и устранения аномальной информации и деятельности, связанной с мошенничеством. Департамент общественной безопасности Государственного совета, департамент финансового управления, ответственный департамент телекоммуникаций и Государственная сеть связи

Департаменты и другие ведомства должны отвечать за разработку мер противодействия в этой области промышленности, способствовать обмену информацией и данными об образцах, связанных с мошенничеством в телекоммуникационных сетях, усилить перекрестную проверку информации о пользователях, вовлеченных в мошенничество, и создать механизм мониторинга и выявления, динамического блокирования и утилизации аномальной информации и деятельности, связанной с мошенничеством.

В соответствии с положениями статьи 11, статьи 12, статьи 18, статьи 22 и предыдущего параграфа настоящего Закона, если в отношении аномалий, связанных с мошенничеством, принимаются какие-либо ограничения, приостановление обслуживания или другие меры по ликвидации, должны быть сообщены причины

Обнаруже
ликвидации, каналы возмещения ущерба и информация, которую необходимо
представить, а также должны быть уведомлены ликвидированные стороны о принятых
мерах.

Заявитель может подать апелляцию в департамент или организацию, принявшую решение ~~дипломатическим путем~~. ~~Принятие решений~~ департаменты и подразделения, которые были назначены, должны создать и усовершенствовать каналы подачи жалоб, принимать жалобы и своевременно проверять их, а в случае успешной проверки немедленно отменять соответствующие меры.

Статья 33 Государство поощряет создание государственных служб сетевой аутентификации личности и поддерживает их добровольное использование частными лицами и предприятиями, а операторы телекоммуникационного бизнеса, банковские финансовые учреждения, небанковские платежные учреждения и поставщики интернет-услуг могут повторно проверять личность пользователей с помощью национальных государственных служб сетевой аутентификации личности на предмет наличия аномалий, связанных с мошенничеством, в телефонных картах, банковских счетах, платежных счетах и счетах в интернете.

Статья 34 Органы общественной безопасности совместно с финансовыми, телекоммуникационными и информационными интернет-департаментами организуют банковские финансовые учреждения, небанковские платежные учреждения, телекоммуникационных операторов, интернет-провайдеров и другие системы раннего предупреждения и разубеждения, своевременно предупреждают о найденных потенциальных жертвах в соответствии с обстоятельствами, чтобы принять соответствующие меры по разубеждению. В случае мошенничества в телекоммуникационных сетях следует усилить работу по возвращению украденных товаров и возмещению убытков, усовершенствовать систему распоряжения средствами, задействованными в деле, и своевременно возвращать законное имущество жертв. Жертвам, которые столкнулись с серьезными жизненными трудностями и отвечают соответствующим национальным условиям оказания помощи, соответствующие стороны оказывают помощь в соответствии с положениями.

Статья 35 По решению или утверждению рабочего механизма Госсовета по борьбе с мошенничеством в телекоммуникационных сетях, органы общественной безопасности, финансовые, телекоммуникационные и другие ведомства, занимающиеся мошенничеством в телекоммуникационных сетях в конкретных областях серьезности, могут в соответствии с соответствующими положениями государства принять необходимые временные меры по предотвращению рисков.

Статья 36 Если лицо, направляющееся в регион с серьезной мошеннической деятельностью в телекоммуникационных сетях, подозревается в крупной мошеннической деятельности в телекоммуникационных сетях, иммиграционная служба может принять решение не разрешать ему покинуть страну.

Лица, получившие уголовное наказание за участие в мошеннических действиях с телекоммуникационными сетями, муниципальный уровень района

С учетом обстоятельств преступления и необходимости предотвращения рецидива
Они не имеют права покидать страну в течение периода от шести месяцев до трех лет
момент отбытия наказания. Он должен уведомить иммиграционные власти о его
исполнении.

Статья 37 Департамент общественной безопасности Госсовета и другие
департаменты совместно с дипломатическим ведомством укрепляют
международное правоохранительное и судебное сотрудничество, а соответствующие
страны, регионы и международные организации создают эффективный механизм
сотрудничества, посредством развития международного полицейского сотрудничества
и других средств, для повышения уровня сотрудничества в области обмена
информацией, расследования и сбора доказательств, следствия и ареста, возвращения
украденных товаров и возмещения ущерба, а также для эффективной борьбы и
пресечения мошеннической деятельности трансграничных телекоммуникационных
сетей.

Глава VI Юридическая ответственность

Статья 38 Если организация, планирование, осуществление или участие в
мошеннической деятельности в телекоммуникационной сети или оказание помощи
в мошеннической деятельности в телекоммуникационной сети является преступлением,
уголовная ответственность должна быть расследована в соответствии с законом.

Если действия, указанные в предыдущем пункте, еще не образуют состава
преступления, органы общественной безопасности назначают срок задержания не менее
десяти и не более пятнадцати дней; конфискуют незаконные доходы и налагают штраф
в размере не менее двойной и не более десятикратной суммы незаконных доходов, а при
отсутствии незаконных доходов или если незаконные доходы составляют менее 10
000 юаней, налагают штраф в размере не более 100 000 юаней.

Статья 39 Если оператор телекоммуникационного бизнеса нарушает
положения настоящего Закона при любых из следующих обстоятельств, то
соответствующее компетентное ведомство предписывает ему внести исправления, а
если обстоятельства менее серьезные, то ему делается предупреждение, выносятся
замечание или налагается штраф в размере не менее 50 000 юаней, но не более 500 000
юаней; если обстоятельства серьезные, то на него налагается штраф в размере не менее
500 000 юаней, но не более 5 000 000 юаней, и он также может получить предписание
соответствующего компетентного ведомства о приостановлении соответствующего
бизнеса, приостановлении деятельности, приостановлении деятельности для
реорганизации, отзыве соответствующего разрешения на деятельность или отозвать
лицензию на ведение бизнеса.

Непосредственные руководители и другие лица, несущие прямую ответственность, наказываются штрафом в размере не менее 10 000 юаней и не более 2 000 юаней. Штраф в размере не более ста тысяч долларов:

(i) Неприменение механизма внутреннего контроля против мошенничества в телекоммуникационных сетях, установленного соответствующими национальными правилами;

(ii) Невыполнение обязанности по регистрации настоящих имен телефонных карт и карт Интернета вещей;

(c) невыполнение обязанностей по мониторингу и идентификации, мониторингу и раннему предупреждению и соответствующей утилизации телефонных карт и карт "Интернета вещей";

(d) Непроведение оценки рисков пользователей IoT-карт или неспособность ограничить функцию открытия IoT-карты, использование сценариев и применимого оборудования;

(e) Непринятие мер по контролю и утилизации подмены телефонных номеров, ложных вызовов или незаконного оборудования с соответствующими функциями.

Статья 40 Если банковское финансовое учреждение или небанковское платежное учреждение нарушает положения настоящего Закона при следующих обстоятельствах, то соответствующее компетентное ведомство предписывает ему внести исправления, а если обстоятельства менее серьезные, то ему делается предупреждение, выносятся замечание или налагается штраф от 50 000 юаней до 500 000 юаней; если обстоятельства серьезные, то налагается штраф от 500 000 юаней до 5 000 000 юаней, а также соответствующее компетентное ведомство может предписать ему прекратить добавление нового бизнеса, уменьшить вид бизнеса или приостановить соответствующую деятельность, приостановить деятельность для исправления ситуации, отозвать соответствующее разрешение на деятельность или отозвать лицензию на деятельность, а также наложить штраф в размере не менее 10 000 юаней и не более 200 000 юаней на непосредственно ответственных руководителей и других непосредственно ответственных лиц:

(i) Неприменение механизма внутреннего контроля против мошенничества в телекоммуникационных сетях, установленного соответствующими национальными правилами;

(ii) Невыполнение обязательств по надлежащей проверке и соответствующих мер по управлению рисками;

(iii) неспособность осуществлять мониторинг рисков и соответствующее удаление необычных счетов и подозрительных операций обязательства;

(d) неспособность передать полную и точную информацию о сделке в соответствии с правилами.

Статья 41 Если оператор телекоммуникационного бизнеса или интернет-провайдер нарушает положения настоящего Закона при следующих обстоятельствах, то соответствующее компетентное ведомство предписывает ему внести исправления, а если обстоятельства менее серьезные, то ему делается предупреждение, выносятся замечание или налагается штраф от 50 000 юаней до 500 000 юаней; если обстоятельства серьезные, то налагается штраф от 500 000 юаней до 5 000 000 юаней, а также соответствующее компетентное ведомство может предписать ему приостановить соответствующий бизнес, приостановить и исправить свой бизнес, закрыть свой веб-сайт или приложение, отозвать соответствующее разрешение на ведение бизнеса или отозвать лицензию на ведение бизнеса, а также наложить штраф в размере не менее 10 000 юаней и не более 200 000 юаней на непосредственно ответственных руководителей и других непосредственно ответственных лиц:

(i) Неприменение механизма внутреннего контроля против мошенничества в телекоммуникационных сетях, установленного соответствующими национальными правилами;

(ii) Невыполнение обязанностей системы реального имени для сетевых услуг или невыполнение проверки зарегистрированного интернет-счета, связанного с телефонной картой, вовлеченной в дело, или мошенничество;

(C) не в соответствии с соответствующими положениями государства, проверять регистрацию доменного имени, информацию о разрешении и адрес Интернет-протокола подлинность и точность, регулировать прыжок доменного имени, или записывать и сохранять соответствующие услуги, предоставляемые информацией журнала;

(d) Невозможность регистрации и проверки реальной идентификационной информации о разработке и эксплуатации мобильного интернет-приложения оператором или невозможность проверки функций и использования приложения, предоставления услуг по упаковке и распространению приложений;

(e) невыполнение обязанности по мониторингу, выявлению и уничтожению мошеннических интернет-аккаунтов и приложений, а также другой мошеннической информации и деятельности в телекоммуникационных сетях;

(vi) отказ в предоставлении технической поддержки и помощи в расследовании и рассмотрении преступлений, связанных с мошенничеством в помощи или не передает соответствующие сведения о преступлениях и информацию о телекоммуникационных сетях, в соответствии с законом.

рисках, как это требуется.

Статья 42 Лицо, нарушившее положения статей 14 и 25, пункт 1, настоящего Закона, конфискует свои незаконные доходы и подвергается штрафу со стороны органов общественной безопасности или соответствующих компетентных органов в размере не менее двойной, но не более десятикратной суммы незаконных доходов или, если незаконные доходы отсутствуют или если незаконные доходы составляют менее 50 000 юаней, в размере не более 500 000 юаней; если обстоятельства серьезны, оно приговаривается органами общественной безопасности к одновременному заключению под стражу на срок не более 15 дней.

Статья 43 Нарушение положений второго абзаца статьи 25 настоящего Закона должно быть предписано соответствующим компетентным ведомством внести исправления, а если обстоятельства менее серьезны, то должно быть вынесено предупреждение, уведомление о критике или наложен штраф в размере не менее 50 000 юаней, но не более 500 000 юаней; если обстоятельства серьезны, то должен быть наложен штраф в размере не менее 500 000 юаней, но не более 5 000 000 юаней, а также может быть предписано соответствующим компетентным ведомством приостановить соответствующий бизнес, приостановить бизнес для реорганизации, закрыть сайт или приложение, и наложить штраф на непосредственно ответственных лиц. руководители и другие лица, несущие прямую ответственность, должны быть оштрафованы на сумму не менее 10 000 юаней и не более 200 000 юаней.

Статья 44 Лицо, нарушившее положения пункта 1 статьи 31 настоящего Закона, конфискует свои незаконные доходы и штрафуется органами общественной безопасности в размере не менее двойной и не более десятикратной суммы незаконных доходов; при отсутствии незаконных доходов или при сумме незаконных доходов менее 20 000 юаней оно штрафуется в размере не более 200 000 юаней; при серьезных обстоятельствах данное лицо приговаривается к аресту на срок не более пятнадцати дней.

Статья 45 Если сотрудники отделов или подразделений, занимающихся борьбой с мошенничеством в телекоммуникационных сетях, злоупотребляют своими полномочиями, пренебрегают своими обязанностями или занимаются фаворитизмом, или если любое другое нарушение положений настоящего Закона является преступлением, они должны быть привлечены к уголовной ответственности в соответствии с законом.

Статья 46: Любое лицо, которое организует, планирует, осуществляет или участвует в мошеннической деятельности в телекоммуникационной сети или оказывает соответствующую помощь в мошеннической деятельности в телекоммуникационной сети, помимо ответственности в соответствии с законом.

Если лицо причиняет ущерб другому лицу не путем привлечения к уголовной или административной ответственности, оно должно нести ответственность за такой ущерб в гражданской ответственности в соответствии с положениями Гражданского кодекса соответствия с положениями Китайской Народной хартии.

Республики и других законов.

Операторы телекоммуникационного бизнеса, банковские финансовые учреждения, небанковские платежные учреждения и поставщики интернет-услуг, которые нарушают положения настоящего Закона и наносят ущерб другим лицам, несут гражданскую ответственность в соответствии с положениями Гражданского кодекса Китайской Народной Республики и других законов.

Статья 47 Народные прокуратуры, выполняя свои обязанности по борьбе с мошенничеством в телекоммуникационных сетях, могут в соответствии с законом обращаться в народные суды с исками о нарушении интересов государства и общественных интересов.

Статья 48 Если соответствующие подразделения и лица не удовлетворены административными наказаниями и административными принудительными мерами, принятыми в соответствии с настоящим Законом, они могут обратиться за административным пересмотром или подать административный иск в соответствии с законом.

Глава VII ПРИЛОЖЕНИЯ Правила

Статья 49 Если соответствующие системы управления и ответственности, участвующие в борьбе с мошенничеством в телекоммуникационных сетях, не предусмотрены настоящим Законом, применяется Закон Китайской Народной Республики о сетевой безопасности, Закон Китайской Народной Республики о защите личной информации, Закон Китайской Народной Республики о борьбе с отмыванием денег и другие соответствующие законы.

Статья 50 Настоящий Закон вступает в силу 1 декабря 2022 года.