Республика Никарагуа
НАЦИОНАЛЬНАЯ ПОЛИЦИЯ

ВМЕСТЕ С СООБЩЕСТВОМ ЗА ВАШУ БЕЗОПАСНОСТЬ

ПРАВОВАЯ БАЗА

СОВРЕМЕННЫЕ ФОРМЫ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДЕНЕЖНЫХ СРЕДСТВ, СОВЕРШЕННОЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ И КРИПТОВАЛЮТ.

Аннотация:

Нормативная правовая регламентация деятельности Национальной полиции Республики Никарагуа в части борьбы с преступностью в сфере противодействия легализации денежных средств осуществляется в рамках политической Конституции Республики Никарагуа и отдельных положений закона № 872, закона 735, закона 977, исполнительным постановлением №15-2018, закона 976, постановления 14-2018, национальной стратегии и плану действий по противодействию отмыванию денежных средств на 2021-2025 годы, уголовно-процессуального кодекса (закон 406), закона № 641, закона № 1042 «Специальный закон о киберпреступлениях», Указа Президента 24-2020, который утверждает национальную стратегию кибербезопасности на 2020-2025 годы, административного соглашения 01 -2021 – правила сохранения данных и информации, руководства по обнаружению, фиксации, изъятию и хранению вещественных доказательств.

Переводы указанных нормативных правовых актов могут быть использованы при реализации дополнительных профессиональных программ – программ повышения квалификации «Современные формы и методы противодействия легализации (отмыванию) денежных средств, совершенной с использованием электронных платежных систем и криптовалют».

1. ПОЛИТИЧЕСКАЯ КОНСТИТУЦИЯ НИКАРАГУА.

2. ЗАКОН № 872. ЗАКОН ОБ ОРГАНИЗАЦИИ, ФУНКЦИЯХ, КАРЬЕРЕ И СПЕЦИАЛЬНОМ РЕЖИМЕ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ ПОЛИЦИИ.

3. ЗАКОН 735. ЗАКОН О ПРЕДУПРЕЖДЕНИИ, РАССЛЕДОВАНИИ И СУДЕБНОМ ПРЕСЛЕДОВАНИИ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ, И УПРАВЛЕНИИ

ИЗЪЯТЫМИ, КОНФИСКОВАННЫМИ И БРОШЕННЫМИ АКТИВАМИ И ПОПРАВКИ К НЕМУ.

4. ЗАКОН 977. ЗАКОН О БОРЬБЕ С ОТМЫВАНИЕМ ДЕНЕЖНЫХ СРЕДСТВ, ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА И ФИНАНСИРОВАНИЯ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ, С РЕФОРМАМИ

5. ИСПОЛНИТЕЛЬНОЕ ПОСТАНОВЛЕНИЕ № 15-2018. ПОЛОЖЕНИЕ ЗАКОНА №. 977, ЗАКОН О БОРЬБЕ С ОТМЫВАНИЕМ ДЕНЕЖНЫХ СРЕДСТВ, ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА И ФИНАНСИРОВАНИЕМ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ.

6. ЗАКОН 976. ЗАКОН О ПОДРАЗДЕЛЕНИИ ФИНАНСОВОГО АНАЛИЗА

7. ПОСТАНОВЛЕНИЕ 14-2018. РЕГУЛИРОВАНИЕ ЗАКОНА 976. ЗАКОН О ПОДРАЗДЕЛЕНИИ ФИНАНСОВОГО АНАЛИЗА.

8. ИСПОЛНИТЕЛЬНЫЙ ОТЧЕТ - НАЦИОНАЛЬНАЯ СТРАТЕГИЯ И ПЛАН ДЕЙСТВИЙ ПО ПРОТИВОДЕЙСТВИЮ ОТМЫВАНИЮ ДЕНЕГ НА 2021-2025 гг.

9. ЗАКОН 406. УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ КОДЕКС НИКАРАГУА.

10. ЗАКОН № 1042. СПЕЦИАЛЬНЫЙ ЗАКОН О КИБЕРПРЕСТУПЛЕНИЯХ.

11. УКАЗ ПРЕЗИДЕНТА №. 24-2020. УТВЕРЖДЕНИЕ «НАЦИОНАЛЬНОЙ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ НА 2020-2025 ГГ.».

12. АДМИНИСТРАТИВНОЕ СОГЛАШЕНИЕ 01-2021 – ПРАВИЛА СОХРАНЕНИЯ ДАННЫХ И ИНФОРМАЦИИ.

13. РУКОВОДСТВО ПО ОБНАРУЖЕНИЮ, ФИКСАЦИИ, ИЗЪЯТИЮ И ХРАНЕНИЮ ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ – 2012 Г.

1. ПОЛИТИЧЕСКАЯ КОНСТИТУЦИЯ НИКАРАГУА.

Статья 97. Национальная полиция является вооруженным органом гражданского характера, отвечает за всю полицейскую деятельность и организована по превентивной, активной и общественной модели при ведущем участии жителей, семьи и общества.

Её задачей является обеспечение внутреннего порядка, безопасности людей и их имущества, предотвращение, преследование и расследование преступлений и прочее, предусмотренное законом.

Национальная полиция является профессиональной, аполитичной, беспристрастной и беспристрастной. Национальная полиция будет управляться в строгом соответствии с Политической конституцией, которую она будет уважать и соблюдать. Он будет подчиняться гражданской власти, которую будет осуществлять Президент Республики в качестве Верховного Главнокомандующего.
Национальный.

В рамках своих функций Национальная полиция будет оказывать помощь судебным органам, а также лицам, которым она требуется в соответствии с законом для выполнения своих функций.

Внутренняя организация Национальной Полиции основана на уникальной иерархии и дисциплине ее командиров и личного состава.

2. ЗАКОН № 872. ЗАКОН ОБ ОРГАНИЗАЦИИ, ФУНКЦИЯХ, КАРЬЕРЕ И СПЕЦИАЛЬНОМ РЕЖИМЕ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ ПОЛИЦИИ.

Статья 1. Характер. Национальная полиция является вооруженным органом гражданского, профессионального, аполитичного, внепартийного, исполнительного и независимого характера. Это единая полиция в стране, она неделима и отвечает за всю деятельность полиции.

Полиция действует в строгом соответствии с Политической конституцией, которую она уважает и соблюдает. Полиция подчиняется гражданской власти, осуществляемую Президентом Республики, в качестве Верховного Начальника Национальный полиции.

Национальная полиция руководится на основе строжайшей дисциплины своих сотрудников, обязанных соблюдать закон. Её внутренняя организация основана на единой иерархии и дисциплине руководителей и сотрудников.

Положения настоящего Закона дополняют Национальную политику по Предотвращению и Гражданской и Общественной безопасности.

Статья 7. Функции. Для выполнения своей конституционной миссии, Национальная полиция исполняет функции в следующих областях:

2) в области расследований, правовой помощи и полицейской разведки. Функции и полномочия Национальной полиции направленны на преследование и расследование преступлений в целом, организованной преступности, терроризма, незаконного оборота наркотиков и связанных с ними преступлений, а именно:

а) расследовать любое действие, которое может представлять собой преступление или проступок, предотвращать дальнейшие последствия совершенных действий, выявлять и арестовывать предполагаемых преступников и участников, проводить обыски и накладывать арест на имущество; собирать полезные элементы расследования и другую информацию, необходимую для раскрытия преступления.

б) осуществлять профилактику, расследование и пресечение уголовных правонарушений, связанных с насилием по признаку пола, а также оказывать, в координации с соответствующими органами, учреждениями и секторами общества, специализированную помощь выжившим пострадавшим, в соответствии с законами в этой материи.

в) расследовать преступления публичного (общественного) характера в зависимости от конкретного случая, когда речь идет о вопиющем преступлении или имеется обвинение лица, уполномоченного требовать принятия необходимых мер; в этих случаях он должен действовать в силу занимаемой должности, остановить совершение преступления, оказать помощь жертве; провести срочные следственные действия и арестовать предполагаемых виновных.

г) противодействовать организованной преступности, терроризму, незаконному обороту наркотиков, преступлениям с использованием наркотических средств, психотропных и других контролируемых веществ и связанных с ними преступлений, а также общей преступной деятельности в целях их предупреждения, выявления, расследования и нейтрализации.

д) собирать, получать и анализировать любые данные, представляющие интерес для защиты жизни, безопасности и целостности людей и их имущества, общественной и гражданской безопасности, а также сохранения внутреннего общественного порядка.

е) подготавливать и внедрять планы и мероприятия по противодействию организованной преступности, терроризма, преступлений, связанных с наркотиками, психотропными средствами и другими контролируемыми веществами, их прекурсорами и связанными с ними преступлениями, а также общеуголовной преступной деятельности, в том числе антинаркотические операции, агентурные операции и специальные следственные действия.

ж) расследование для раскрытия и проверки предполагаемых преступных деяний будет проводиться в соответствии с правилами, приемами и научными методами такой деятельности, за исключением ограничений, установленных Политической конституцией, ратифицированными международными договорами и конвенциями, и

законом. Результат их расследования будет представлен в виде отчета Министерству государственного управления или компетентному судебному органу.

з) организовывать и обновлять архивную службу полиции, получая, заказывая, классифицируя и храня всю информацию и документацию, связанную с расследованием преступлений и правонарушений, задержанных, огнестрельного оружия, разрешений и лицензий, и других административных операций, которые производятся в Национальной Полиции.

и) выдавать справки о несудимости и судимости тем, кто их запрашивает, и производить аннулирование в установленном порядке.

к) исполнять и гарантировать исполнение решений, исходящих от судебных органов и других лиц, должным образом уполномоченных по закону, в соответствии с соответствующим правовым порядком.

л) вызывать любое лицо, которое может предоставить информацию, представляющую интерес для проводимого расследования, с целью его опроса или получения его показаний в порядке и с гарантиями, установленными законом.

м) соблюдать протоколы или процессуальные действия международной следственной помощи по запрошенным уголовным делам, согласно установленному порядку и по каналам, предусмотренным международными договорами или соглашениями и законодательством страны.

н) развивать отношения сотрудничества, взаимодействия с учреждениями-партнерами из других стран или с региональными, или международными полицейскими органами, в целях усиления борьбы с транснациональной организованной преступностью.

Статья 9. Руководство учреждения. В соответствии с Политической Конституцией Республики Никарагуа и настоящим Законом, Национальная Полиция является иерархическим учреждением, руководство которого основано на строгой дисциплине своих командиров и личного состава. Для эффективного выполнения своих миссий и функций, состав руководства организован таким образом:

1) Верховное Управление

2) Национальное Управление

3) Управление Специализированных Национальных Отделов и Вспомогательных органов

4) Управление Полицейских Отделов

Статья 10. Верховное Управление.

Верховное Управление Национальной Полиции находится в ведении Президента Республики, в качестве Верховного Главнокомандующего, и имеет следующие полномочия:

1) распоряжаться силами и средствами Национальной полиции в соответствии с Политической конституцией и Законом.

2) назначать Генерального директора Национальной полиции из числа членов Национального штаба.

3) назначать заместителей директора и заместителей генерального директора, а также генерального инспектора.

4) присваивать степени Первого комиссара или генеральных комиссаров и комиссаров.

5) издавать приказ об отставке Первого комиссара, Генеральных комиссаров и комиссаров.

6) снимать с должности Генерального директора Национальной Полиции по следующим причинам:
а) неповиновение приказам Президента Республики в его качестве Верховного Главнокомандующего Национальной Полиции при осуществлении им своих полномочий.
б) быть осужденным вступившим в законную силу приговором за тяжкое или особо тяжкое преступление.
в) физическая или умственная недееспособность в соответствии с законом.

7) увольнять заместителей Генерального директора, Инспектора и Генерального инспектора по представлению Генерального управления по следующим основаниям:
а) неповиновение приказам Генерального директора при осуществлении своих полномочий.
б) быть осужденным за тяжкое или особо тяжкое преступление вступившим в законную силу приговором.
в) физическая или умственная недееспособность в соответствии с законом.

8) санкционировать запросы о временном отсутствии Генерального директора Национальной полиции.

9) награждать и назначать по предложению Генерального директора награды служащим Национальной полиции, находящимся на действительной службе, бывшим служащим Национальной полиции посмертно, национальным или иностранным деятелям, внесшим свой вклад в обеспечение безопасности и развития граждан, укрепление института полиции.

10) получать и утверждать проект годового бюджета Национальной полиции для его включения в проект закона о годовом общем бюджете Республики в соответствии с

Законом № 550 «Закон о финансовом управлении и бюджетном режиме», опубликованным в официальном периодическом издании La Гасета, № 167 от 29 августа 2005 г.

11) утверждать государственную политику и руководящие принципы в области безопасности граждан и человека, а также судебного преследования, предотвращения и расследования организованной преступности, терроризма, незаконного оборота наркотиков и общеуголовных преступлений.

12) призывать отставных офицеров Национальной Полиции для выполнения конкретных задач в исключительных случаях, которые будут восстановлены в должности по контракту.

13) обеспечивать Национальную Полицию необходимыми условиями и ресурсами для выполнения ее задач и конституционных функций, а также для развития и укрепления превентивной, активной и общественной модели полиции; и другие, указанные законом.

14) издавать приказ Совета министров об осуществлении никарагуанской армии в поддержку Национальной Полиции, когда стабильности Республики угрожают большие внутренние беспорядки, бедствия или стихийные бедствия.

15) получать годовой отчет Национальной полиции на общенациональном собрании начальников полиции.

Статья 11. Национальное Управление.

Национальным Управлением руководит Генеральный директор, который направляет, администрирует и осуществляет единоличное командование в учреждении, в соответствии с положениями Политической конституции Республики Никарагуа, настоящим Законом и внутренними правилами, под командой Верховного Управления.

Он осуществляет свои полномочия непосредственно или через заместителей Генерального директора и Генерального инспектора, которые помогают ему в этих целях, а также выполняют функции консультативно-совещательного органа при Генеральном директоре.

Национальная штаб-квартира состоит из Главных управлений и Генеральной инспекции.

Генеральными управлениями являются следующие:

1) Предотвращение преступлений и гражданская безопасность

2) Следствие и полицейская разведка

3) Безопасность и защита личности

4) Делегация Манагуа

5) Администрация и управление

При Главном управлении полиции находится Генеральный секретариат, действующий, как координационный и вспомогательный орган.

Статья 16 Управления Национальной Полиции.

Управления Национальной Полиции - это важные полицейские органы, предназначенные для противодействия преступной деятельности, чтобы гарантировать гражданскую и общественную безопасность на всей территории страны; они обладают руководящими полномочиями в своих конкретных областях на основании правовых и нормативных положений; они готовят и представляют на утверждение инструкции и положения, а также планируют, консультируют, контролируют, анализируют, оценивают и дают рекомендации высшему полицейскому органу по совершенствованию соответствующих процессов и осуществляют, при необходимости, оперативную деятельность в пределах своей компетентности. Они могут присутствовать на уровне территориальных отделений, и в этом случае они осуществляют функциональное подчинение.

Статья 17 Функции Специализированных национальных отделов. Основные функции Специализированных Национальных отделов описаны ниже:

1) Полицейская разведка: это специализированный отдел, отвечающий за обнаружение, предотвращение, расследование и устранение угроз и рисков, связанных с организованной преступностью, терроризмом и другими, связанными с ними преступлениями, которые могут повлиять на жизнь и безопасность людей, их имущество, семьи и общество.

2) Экономические расследования: это специализированный отдел, отвечающий за расследование преступлений против социально-экономического порядка, преступлений против государственной казны, подделки валюты, ценных бумаг и фискальных видов, преступлений против национального культурного наследия, общественного здравоохранения, природных ресурсов и окружающей среды, а также все те, которые имеют экономическое или наследственное влияние на государство; ведёт расследование и анализ заключительных технических отчетов, представленных Группой финансового анализа, для чего этот отдел получает, собирает, анализирует и распространяет информацию, связанную с этими преступлениями.

3) Антинаркотики: это основной специализированный отдел на национальном уровне для расследования и противодействия незаконному обороту наркотиков, преступлениям, связанным с наркотическими веществами, психотропными

средствами, другими контролируемыми веществами, их прекурсорами и другими преступлениями организованной преступности, связанными с этой деятельностью. Для чего отдел получает, собирает, систематизирует, анализирует и распространяет информацию, связанную с этими преступлениями. Это орган, отвечающий за обмен информацией с аналогичными партнерскими агентствами из других стран и международных организаций.

4) Следственное управление: это специализированный отдел, отвечающий за проведение, будь то по собственной инициативе, по заявлению или по распоряжению прокурора, расследования и документирования любого факта, который может представлять собой преступление или проступок; для выявления и задержания подозреваемых в преступлении и сбора элементов полезных для расследования, вещественных доказательств и улик; подготовку соответствующего полицейского отчета и представления его компетентным органам, с соблюдением установленных требований по содержанию и срокам, как это предусмотрено законодательством.

17) Полицейская контрразведка: Это специализированный отдел, отвечающий за разработку стратегий, планов и оперативных действий по защите операций полиции, информации, документации, ее объектов и персонала, а также противодействие угрозам со стороны организованной преступности и других преступных формирований внутри страны.

19) Институт криминалистики и судебной экспертизы: это специальность, задача и функции которой заключаются в участии в техническом осмотре мест, где предположительно было совершено преступное деяние, сборе и обработке уголовных доказательств, проведении экспертиз с помощью научных методов, методик и техник и подготовке соответствующих отчетов в поддержку следственной функции полиции, судебных органов и других органов, которые требуют этого в соответствии с законом.

3. ЗАКОН 735. О ПРЕДУПРЕЖДЕНИИ, РАССЛЕДОВАНИИ И УГОЛОВНОМУ ПРЕСЛЕДОВАНИЮ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ И УПРАВЛЕНИИ ИЗЪЯТЫМ И ОСТАВЛЕННЫМ ИМУЩЕСТВОМ.

Регулирует функции государства по предупреждению, выявлению, расследованию, уголовному преследованию и судебному производству по преступлениям, связанным с организованной преступностью, а также по управлению и распоряжению имуществом, предметами, товарами, оборудованием или другими инструментами, используемыми или предназначенными для использования при совершении преступлений, связанных с организованной преступностью.

Статья 2. Определения. Для целей настоящего Закона принимаются следующие определения:

* Внедренный сотрудник: Должностное лицо Национальной полиции или Армии Никарагуа, прошедшее специальную подготовку, по согласованию с главным подразделением Учреждения, которому оно принадлежит, скрывающее свою

личность и внедряющееся в преступные организации, имитируя своё участие в ней или интерес в совершении расследуемого преступления с целью выявления исполнителей или соучастников, осуществляемых преступных действий, их форм работы, организационной структуры, планов действий, контактов, средств и результатов преступной деятельности, а также выявления доказательств, которые могут быть представлены при уголовном процессе.

* Агент-разоблачитель: должностное лицо полиции, которое с разрешения Генерального Директора Национальной Полиции имитирует заинтересованность в передаче, покупке, приобретении или транспортировке для себя или третьих лиц денег, товаров, людей, услуг, оружия, веществ, перечисленных в списке, или таблице, прилагаемые к настоящему Закону; или заинтересованность в любой другой организованной преступной деятельности, демонстрируя проявление противоправного поведения или деяния, или изъятия незаконных веществ или товаров и идентификации или поимки виновных или участников.

* Контролируемая поставка: специальное оперативно-розыскное мероприятие, проводимое на национальной территории или за ее пределами, которое включает в себя перехват и контроль над количеством, качеством и объемом предполагаемо незаконных партий денежных средств или ценных бумаг, оружия, контролируемых веществ, прекурсоров или средств, которые служили или могли служить для совершения любого из преступлений, связанных с настоящим Законом, с ведома и под контролем компетентных органов в целях их изъятия и выявления или разоблачения лиц, причастных к их совершению, получения информации о планах, предотвращения незаконного использования вышеупомянутых объектов, предупреждения и установления любого факта совершения таких преступлений.

* Наблюдаемая поставка: специальное оперативно-розыскное мероприятие, проводимое по запросу одного или нескольких государств на основе международных документов, цель которого заключается в разрешении ввоза в страну, пересечении её территории и вывоза за её пределы предполагаемо незаконных партий денежных средств или ценных бумаг, оружия, контролируемых веществ, прекурсоров или средств, которые служили или могли служить для совершения любого из преступлений, указанных в настоящем Законе, и осуществляемое с ведома и под контролем соответствующих компетентных органов в целях выявления причастных лиц или сбора доказательств.

* Информатор (осведомитель): лицо, которое предоставляет специализированным органам Национальной полиции или разведки армии Никарагуа, данные или сведения о подготовке или совершении преступления, или о тех, кто участвовал или будет участвовать в нем.

* Защита свидетелей, экспертов и других участников судопроизводства: Совокупность мер, действий и процессов, направленных на защиту жизни, личной

неприкосновенности, свободы или имущества свидетеля, экспертов и других участников судопроизводства или семьи защищаемой стороны.

Статья 62. Перехват сообщений. При расследовании преступлений, предусмотренных настоящим Законом, при наличии мотивированного ходатайства Генерального прокурора Республики или Генерального директора Национальной полиции, окружные судьи по уголовным делам вправе давать им разрешение на воспрепятствование, прерывание, перехват или запись сообщений, электронной переписки; других радио-электрических и информационных средств связи; стационарных, мобильных, беспроводных, цифровых или любых других, исключительно для целей уголовного расследования и в соответствии с нормами, установленными Уголовно-процессуальным кодексом.

В тех же случаях судья вправе распорядиться о сборе и записи сообщений и изображений между лицами, присутствующими на месте.

Прослушивание может быть предписано и осуществлено до или в ходе уголовного процесса. В последнем случае решение хранится в тайне вводится в процесс только в соответствии с положениями уголовно-процессуального кодекса, касающимися прослушивания телефонных переговоров.

Прослушивание разрешается на срок до шести месяцев, за исключением дел по особо тяжким преступлениям или при расследовании сложных дел; в таких случаях судья по обоснованному решению вправе продлить указанный срок на шесть месяцев. В случае отказа в разрешении на прослушивание, ходатайствующая сторона должна быть немедленно уведомлена об этом; данное решение может быть обжаловано.

Перехват любых сообщений между обвиняемым и его защитником запрещен.

Статья 67. Лица, подлежащие защите. В контексте настоящего Закона, под лицами, подлежащими защите, понимаются потерпевшие, свидетели, эксперты и другие субъекты, участвующие в расследовании и уголовном судопроизводстве, а также их родственники или иные лица, находящиеся в ситуации риска или опасности, из-за их прямого или косвенного вмешательства в расследовании преступления, предусмотренных настоящим Законом.

Статья 68. Ситуация риска или опасности. Под ситуацией риска или опасности понимается обоснованное существование угрозы жизни или ущерба здоровью, личной неприкосновенности, свободе и безопасности лиц, указанных в предыдущей статье. Ситуация риска или опасности для человека будет определяться совместно, Министерством государственного управления и Национальной полицией, при поддержке никарагуанской армии. Личность свидетеля может быть раскрыта перед судьей только на специальном слушании, для чего нет необходимости указывать имя, личную информацию и адрес в документе обмена доказательствами.

Статья 69. Расходы на охрану. Расходы на применение мер защиты в целях охраны жизни, личной неприкосновенности, свободы и безопасности людей, упомянутых в настоящей главе, будут финансироваться Министерством финансов и государственного кредита за счет средств, поступающих от Отдела управления изъятых, конфискованных или покинутых активов, без ущерба для помощи от государственных или частных, внутренних или внешних пожертвований.

Прокуратура совместно с Национальной полицией подготовит годовой бюджет для применения и реализации программы по охране.

Статья 82. Специальные средства расследования. Под специальными оперативно-розыскными мероприятиями понимаются негласные операции, обеспечивающие конфиденциальность расследования и участвующих в них лиц, заключающиеся в непринятии мер по предотвращению возможности совершения преступления и в участии внедренных сотрудников и агентов-разоблачителей или информаторов, которые могут временно изменять свою личность и использовать фиктивные документы, удостоверяющие личность, с целью сбора доказательственной информации о совершении наказуемых деяний, указанных в настоящем Законе.

В качестве внедренных агентов могут действовать только специально подготовленные действующие сотрудники Национальной полиции или Армии Никарагуа.

Исключительные специальные операции по фиктивному приобретению или продаже имущества, инструментов или товаров, связанных с преступлениями, указанными в настоящем законе, осуществляются группой специально подготовленных агентов для проведения негласных операций от учреждений, уполномоченных настоящим Законом.

Национальная Полиция или армия Никарагуа, в зависимости от обстоятельств, обязаны контролировать деятельность указанных агентов, обеспечивать их защиту и надлежащее вознаграждение, а также при необходимости привлекать их к ответственности.

Статья 83. О контролируемой поставке и наблюдаемой поставке. В случае необходимости для расследования преступлений, указанных в настоящем Законе, Генеральный прокурор Республики обязан согласовать использование специальных методов расследования – наблюдаемой поставки и контролируемой поставки, в зависимости от ситуации. После получения разрешения, данные мероприятия должны проводиться под контролем высшего должностного лица Национальной полиции.

Статья 84. Разрешение на проведение наблюдаемой поставки. Для проведения наблюдаемой поставки органы власти обратившейся страны обязаны направить запрос Генеральному прокурору Республики, с тем чтобы Национальная полиция провела наблюдаемую поставку, разрешив ввоз, оборот, пересечение и вывоз за

пределы национальной территории незаконных партий денежных средств или ценных бумаг, оружия, контролируемых веществ, прекурсоров или средств, которые служили или могли служить для совершения любого из преступлений, указанных в настоящем Законе. В этих целях обратившаяся сторона должна в кратчайшие сроки предоставить соответствующую информацию о действиях, которые необходимо осуществить.

С согласия заинтересованных сторон, незаконные партии, согласованные к наблюдаемой поставке, могут быть перехвачены или оставлены нетронутыми, либо содержащиеся в них наркотические средства или психотропные вещества могут быть заменены полностью или частично.

Статья 85. Разрешение на контролируемую покупку. В случае контролируемых покупок, Генеральный директор Национальной полиции обращается к Генеральному прокурору Республики, и тот дает разрешение на использование этого специального метода расследования, в случае наличия обоснованных признаков, что было или будет совершено преступление, связанное с настоящим Законом, и выполняется одно или несколько из следующих условий:

а) Когда расследование дела представляется невозможным или чрезвычайно трудным.

б) Когда особая значимость дела требует вмешательства оперативного работника под прикрытием, так как другие меры оказались безрезультатны.

в) Когда возникает необходимость симулированной покупки или продажи предметов, веществ, товаров, ценностей или продуктов, являющихся средствами преступления или составляющими доходы преступления.

Статья 86. Цель негласных операций. Правомерными считаются негласные операции, которые при выполнении вышеуказанных требований, имеют своей целью:

а) проверить факт совершения преступлений, указанных в настоящем Законе, с целью получения изобличающих обвиняемого или других соучастников преступления доказательств, а также фактов, приведшим к негласной операции или другим деяниям, выявленным в ходе расследования;

б) выявить организаторов и других соучастников таких преступлений.

с) осуществить изъятие, иммобилизацию, конфискацию или другие превентивные меры;

в) не допустить совершения преступлений, охватываемых настоящим Законом, или достижения преступного результата;

г) получить и обеспечить средства доказывания.

Статья 87. Изменение личности. В случаях, когда негласная операция требует изменения личности внедренного сотрудника, разрешается полное или частичное изменение личности действующего сотрудника или должностного лица. Генеральный директор Национальной полиции или Главнокомандующий Армией Никарагуа, в зависимости от обстоятельств, координирует деятельность по внесению изменений в базы данных, регистры, книги, публичные архивы исключительно в целях, указанных в настоящем Законе.

Статья 88. Обязанности внедренного агента.
Лицо, выполняющее функции внедренного агента, обязано:

а) всесторонне, своевременно и достоверно сообщать своему руководству всю информацию, полученную в результате внедрения;

б) сохранять конфиденциальность полученной информации, не допуская ее попадания к третьим лицам;

в) хранить и передавать в полном объеме для конфискации денежные средства, ценности или имущество, полученные от преступной группы, при условии, что это не препятствует расследованию;

г) воздерживаться от совершения преступлений или правонарушений сверх своих функций.

Статья 89. Защита внедренного агента в судебном процессе. В случаях, когда в уголовном процессе требуется представить результаты негласного расследования, они включаются в заключение вышестоящего руководителя внедренного агента, который обязан обозначить его псевдонимом либо измененным именем, если это применимо. Кроме того, по возможности, внедренный агент вправе давать показания в суде с помощью системы, не позволяющей обвиняемому или обвиняемым узнать личность агента.

Статья 90. Ответственность внедренного агента. Действия внедренного агента, а также сама операция должны осуществляться в целях, изложенных в настоящем Законе. Внедренный агент несет личную ответственность за действия, которые представляют собой любое преступление, совершенное в результате превышения своих функций.

Внедренный агент, участвующий в незаконной деятельности, освобождается от уголовной или гражданской ответственности за действия, которые он должен совершить или которые он не смог предотвратить, при условии, что они являются необходимым условием для успешного осуществления расследования и

обеспечивают надлежащую соразмерность цели расследования. Для подтверждения действительности данного условия достаточно соответствующего сообщения Генерального директора Национальной полиции или Главнокомандующего Армией Никарагуа, в зависимости от обстоятельств, Генерального прокурора Республики.

В отношении информатора, действуют положения Уголовно-процессуального Кодекса о прекращении уголовного преследования в связи с активным сотрудничеством или о заключении соглашения с условиями, если в отношении него не было возбуждено уголовное дело, в исключительных случаях вознаграждение за его сотрудничество может быть предоставлено только наличными денежными средствами, как это предусмотрено Положением настоящего Закона.

4. ЗАКОН 977. ЗАКОН О ПРОТИВОДЕЙСТВИИ ОТМЫВАНИЮ (ДЕНЕЖНЫХ) СРЕДСТВ, ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА И ФИНАНСИРОВАНИЮ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ, С ЕГО РЕФОРМАМИ

Статья 1. Основной объект закона

Объектом настоящего Закона является защита национальной экономики и целостности финансовой системы от рисков, связанных с отмыванием активов, финансированием терроризма и финансированием распространения оружия массового уничтожения. В дальнейшем эта деятельность будет упоминаться как «ОА/ФТ/ФРОМП».

Статья 2. Специальный объект

1. Создать механизмы, основанные на риск-ориентированном подходе, для продвижения и укрепления мер по предотвращению, расследованию, судебному преследованию и наказанию за ОА/ФТ/ФРОМП.

2. Осуществлять финансовые меры, принятые Советом Безопасности ООН и другими международными организациями, членом которых является Никарагуа, в отношении ОА/ФТ.

3. Укреплять национальное законодательство в соответствии со сферой действия международных конвенций и основных международных стандартов по борьбе с ОА/ФТ/ФРОМП.

4. Снизить экономический и оперативный потенциал национальных или транснациональных преступных организаций

Статья 5 Национальная система ОА/ФТ/ФРОМП. «Национальная система по борьбе с отмыванием денег и финансированием терроризма и распространением оружия массового уничтожения» или «Национальная система по ОА/ФТ/ФРОМП» представляет собой скоординированный набор компетентных органов в этом вопросе, обязанных субъектов и установленных политик. в законах, правилах и положениях, которые способствуют защите целостности финансовой системы и экономики Никарагуа. Компетентные органы и Обязанные субъекты являются операторами Системы и могут быть организованы в подсистемы.

Статья 6 Национальный совет по ОА/ФТ/ФРОМП. Создается Национальный совет по ОА/ФТ/ФРОМП, именуемый в дальнейшем «Совет». Совет будет состоять из постоянных представителей и назначенных технических посредников от следующих учреждений:
а. Министерство финансов и государственного кредита.
б. Генеральный прокурор республики.
в. Общественная служба.
г. Национальная Полиция.
д. Надзор за банками и другими финансовыми учреждениями.Группа финансового анализа.
е. Национальная комиссия по микрофинансированию.
ё. Министерство внутренних дел.
ж. Никарагуанская армия.

Координацию Совета осуществляет лицо, назначенное Президентом Республики, а его Технический Секретариат подчиняется Директору Финмониторинга. Точно так же он может созывать учреждения, необходимые для выполнения его функций.

Совет готовит и утверждает правила, которые периодически пересматриваются для проведения необходимых реформ.

5. ИСПОЛНИТЕЛЬНЫЙ ПОСТАНОВЛЕНИЕ № 15-2018. ПОЛОЖЕНИЕ ЗАКОНА №. 977, ЗАКОН О БОРЬБЕ С ОТМЫВАНИЕМ ДЕНЕЖНЫХ СРЕДСТВ, ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА И РАСПРОСТРАНЕНИЕМ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ

Статья 1. Объект. Целью настоящего постановления является установление нормативных положений для применения Закона № 977 «Закон о борьбе с отмыванием денег, финансированием терроризма и финансированием распространения оружия массового поражения», опубликованного в La Gaceta, Official Gazette No. № 138 от 20 июля 2018 г., а также создание условий для предотвращения, выявления и сообщения о деятельности по ОА/ФТ/ФРОМП и предикатным преступлениям; обязанности Субъектов, Обязанных указанным законом; и выборочная финансовая санкция на блокирование средств или других активов, вытекающая из резолюций Совета Безопасности Организации Объединенных Наций по противодействию ОА/ФТ/ФРОМП.

6. ЗАКОН 976. ЗАКОН ОБ УПРАВЛЕНИИ ФИНАНСОВОГО АНАЛИЗА И ЕГО ПОПРАВКИ.

Статья 1 Объект. Целью настоящего Закона является регулирование организации, полномочий и деятельности группы финансового анализа в соответствии с Законом № 793, «Закон о финансовом анализе», опубликованным в La Gaceta, Official Gazette No. 117 от 22 июня 2012 г., который в дальнейшем будет именоваться «УФА».

Для всех юридических целей следует понимать, что правосубъектность УФА существует без решения о преемственности с начала действия Закона № 793.

7. ПОСТАНОВЛЕНИЕ 14-2018. РЕГУЛИРОВАНИЕ ЗАКОНА 976. ЗАКОН ОБ УПРАВЛЕНИИ ФИНАНСОВОГО АНАЛИЗА.

Статья 1. Объект. Целью настоящего Указа является установление нормативных положений для применения Закона № 976, «Закон о подразделениях финансового анализа», опубликованный в La Gaceta, Official Gazette № 138 от 20 июля 2018 года.

Статья 2. Сфера применения . Положения настоящего Положения применяются к Группе финансового анализа (ГФА), а также к органам и Обязанным субъектам, перечисленным в Законе № 976 «Закон о Группе финансового анализа».

8. ИСПОЛНИТЕЛЬНЫЙ ОТЧЕТ - НАЦИОНАЛЬНАЯ СТРАТЕГИЯ И ПЛАН ДЕЙСТВИЙ ПО ПРОТИВОДЕЙСТВИЮ ОТМЫВАНИЮ ДЕНЕГ (ПОД/ФТ/ПФТ)

Национальная стратегия ОА/ФТ/ФРОМП. Инструмент, в котором определяются общие направления действий в этой области, определяя области, на которые должно быть оказано влияние, и преследуемые общие цели. Таким образом, это документ, в котором на основе информации, собранной в ходе проведенных оценок рисков, излагаются общие принципы, которым необходимо следовать для борьбы с этими преступлениями, с учетом направлений смягчения последствий, которыми будут руководствоваться действия, которые предлагаются.

Национальный план по ОА/ФТ/ФРОМП состоит из набора конкретных мер, определенных для достижения целей, изложенных в Национальной стратегии, классифицированных и упорядоченных таким образом, чтобы они были интегрированы и скоординированы при планировании.

Действия предусматривают, по крайней мере, описание их содержания, сроки и ожидаемое время, определяемые приписанным им приоритетом, целями, преследуемыми каждым из них, ответственными лицами и участниками их

реализации. Группировка всей этой информации составит основу Национального плана по ОА/ФТ/ФРОМП.

9. ЗАКОН 406 УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ КОДЕКС НИКАРАГУА.

Статья 213.- Телефонные вмешательства. Перехват телефонных переговоров или других видов телекоммуникаций будет осуществляться в случае:
1. Терроризма;
2. Похищения с целью вымогательства;
3. Торговли органами и людьми в сексуальных целях;
4. Преступлений, связанных с наркотиками, психотропными и другими контролируемыми веществами;
5. Отмывания денег или активов;
6. Международного оборота оружия, взрывчатых веществ и угнанных автомобилей.

Запрещается прослушивание общения между подсудимым и его защитником.

Перехват телекоммуникаций осуществляется только по прямому и обоснованному запросу Генерального прокурора Республики или Генерального директора Национальной полиции, которые должны заявить, что они оценили предысторию и что вмешательство, по их мнению, оправдано, и также укажет продолжительность, на которую запрашивается разрешение, а также людей, которые будут иметь доступ к коммуникациям.

Судья определяет происхождение меры, мотивированным постановлением, и указывает дату, когда прослушивание должно быть прекращено. Прослушивание не может длиться более тридцати дней, его срок может быть продлен не больше 1раза.

К процессу будут привлечены только записи тех разговоров или их часть, которые по требованию прокурора будут сочтены полезными для установления истины. Однако ответчик может потребовать включения других разговоров или других частей, которые были исключены, если он сочтет это целесообразным для своей защиты. Судья дает приказ на уничтожение частей, не относящихся к процессу.

Все лица, имеющие доступ к разговорам, должны соблюдать конфиденциальность их содержания. Государственные служащие, нарушающие это положение, могут быть уволены со своих должностей и не освобождаются от соответствующей гражданской и уголовной ответственности.

Статья 214. - Перехват письменных, телеграфных и электронных сообщений. Перехват письменных, телеграфных и электронных сообщений будет осуществляться в случае преступлений, указанных в предыдущей статье, по запросу компетентного судьи с четким указанием причин, которые его оправдывают, и информации, которая, как ожидается, будет обнаружена. в них. . Судебное постановление, которым

санкционировано данное положение, должно быть надлежащим образом мотивировано.

Открытие сообщения будет осуществляться судьей, и содержание, связанное с преступлением, будет включено в расследование.

10. ЗАКОН № 1042. СПЕЦИАЛЬНЫЙ ЗАКОН О КИБЕРПРЕСТУПЛЕНИЯХ.

Статья 1. Объект регулирования
Целью настоящего Закона является предупреждение, расследование, уголовное преследование и применение мер наказания за преступления, совершенные посредством информационно-коммуникационных технологий в отношении физических или юридических лиц; а также обеспечение комплексной защиты систем, использующих указанные технологии, их содержимого и любой из их частей, в соответствии с положениями, предусмотренными настоящим Законом.
Статья 2. Сфера применения
Настоящий Закон направлен на обеспечение общественного порядка и применяется в отношении лиц, совершивших преступления, предусмотренные настоящим Законом, на территории Никарагуа или за ее пределами.
Статья 3. Определения
Для целей настоящего Закона вводятся следующие понятия:
1. Доступ к информационным системам – вход в указанные системы, включая удаленный доступ.
2. Доступ к информации, содержащейся на устройстве, которое позволяет хранить данные – чтение, копирование, извлечение, изменение или удаление информации, содержащейся на указанном устройстве.

4. Киберпреступления – характерные противоправные, уголовно наказуемые, длящиеся или единичные действия или бездействия, совершенные в отношении физических и / или юридических лиц с использованием в качестве метода, средства или цели компьютерных данных или систем, информационно-коммуникационных технологий, в целях нанесения ущерба личным юридическим, имущественным или информационным благам потерпевшего.

6. Данные, связанные с трафиком – все данные, связанные с сообщением, осуществляемым посредством любых технологических средств, создаваемые последними и указывающие источник, пункт назначения, маршрут, время,

дату и тип использованных услуги или протокола, размер и продолжительность сообщения.

11. Предоставление компьютерных данных и файлов – передача информации, документов или данных в электронном формате, которые хранятся у физических лиц, в государственных или частных учреждениях.

12. Цифровая идентифицирующая информация - информация, данные или любая другая характеристика, которая индивидуализирует, отождествляет или отличает одно лицо от другого либо одного пользователя от другого в рамках компьютерной системы.

13. Изъятие и хранение компьютерных систем или устройств хранения данных – физическое завладение и обеспечение их хранения компетентными органами.

14. Перехват – действие по захвату или прерыванию компьютерных данных, содержащихся или передаваемых посредством информационно-коммуникационных технологий до момента их поступления к месту назначения.

15. Вмешательство – создание препятствий, помех или преград посредством информационно-коммуникационных технологий в государственных или частных компьютерных системах.

16. Прослушивание переговоров посредством информационно-коммуникационных технологий – захват, прослушивание или запись содержания указанных переговоров в реальном времени без их прерывания, а также без прерывания данных трафика.

21. Требование немедленного сохранения данных, которыми владеют третьи лица – возложение на физических или юридических лиц обязанности по полному сохранению цифровой информации, которой они владеют или имеют полномочия по распоряжению таковой.

22. Опечатывание, пломбирование и запрет использования компьютерных систем или устройств хранения данных – блокирование или невозможность их использования с сохранением полноты их содержания.

23. Компьютерная система – любое обособленное устройство, подключенное или связанное с другими устройствами через каналы связи или технологию, которая заменит их в будущем, функция которого или функция любой из частей которого заключается в автоматической обработке данных при работе компьютерной программы.

25. Информационно-коммуникационные технологии – совокупность средств связи и информационных приложений, которые позволяют перехватывать, производить, воспроизводить, передавать, хранить,

обрабатывать и предоставлять информацию в форме изображений, голоса и текстов, кодов или данных, содержащихся в сигналах акустического, оптического или электромагнитного характера и других, посредством сетевых протоколов, а также протоколов передачи и приема данных.

Глава II.
Преступления, связанные с целостностью компьютерных систем

Статья 4. Неправомерный доступ к компьютерным системам

Лицо, которое намеренно и без разрешения либо с превышением пределов имеющегося у него разрешения, получает доступ, перехватывает или использует частично или полностью компьютерную систему, использующую информационно-коммуникационные технологии, наказывается лишением свободы от одного года до трех лет и штрафными днями в количестве от 200 до 500.

Статья 5. Неправомерный доступ к компьютерным программам или данным

Лицо, которое сознательно и намеренно использует какое-либо устройство информационно-коммуникационных технологий, прямо или косвенно, частично или полностью получает доступ к любой программе или данным, хранящимся на нем, с целью их присвоения или совершения другого преступления посредством их использования, наказывается лишением свободы от двух до четырех лет и штрафными днями в количестве от 300 до 500.

Нижние и верхние пределы наказаний за указанные в статьях 4 и 5 действия увеличиваются на одну треть в случае их совершения в коммерческих целях или в отношении:

1. Государственных учреждений или учреждений, находящихся в их ведении.
2. Государственных, частных или смешанных учреждений, предоставляющих общественные услуги.
3. Банки, микрофинансовые учреждения, учреждения по хранению депозитов, финансовые группы, страховые компании и другие финансовые и биржевые учреждения, находящиеся под надзором и / или регулируемые в Никарагуа.

Статья 6. Перехват сообщений и связи между системами информационно-коммуникационных технологий

Лицо, незаконно перехватывающее любой вид письменного сообщения, которое не адресовано ему, или передачу данных в, из либо внутри компьютерной системы, а также любого технологического средства, не имеющего общего доступа, используя при этом информационно-коммуникационные технологии; а равно электромагнитные излучения, передающие данные из компьютерной системы, наказывается лишением свободы от одного года до трех лет и штрафными днями в количестве от 200 до 500.

Статья 7. Неправомерный перехват чужих сообщений посредством информационно-коммуникационных технологий
Лицо, неправомерно использующее информационно-коммуникационные технологии или любое другое средство и посредством этого записывающее или перехватывающее слова или разговоры третьих лиц, будь то видео, изображения, коды, аудио или тексты, не предназначенные для общего доступа, а равно прослушивающее частные сообщения, не адресованные ему, наказывается лишением свободы от одного года до трех лет и штрафными днями в количестве от 100 до 300.

Статья 8. Вмешательство в работу компьютерных систем или данных
Лицо, намеренно и любыми способами, на временной или постоянной основе вмешивающееся или нарушающее работу компьютерной системы или данных, содержащихся в ней, наказывается лишением свободы от трех до пяти лет и штрафными днями в количестве от 200 до 400.
Вышеуказанные действия, наносящие ущерб государственным компьютерным системам или системам, предназначенным для предоставления услуг в сферах здравоохранения, связи, финансов, энергетики, водоснабжения, транспортных средств, портов и аэропортов, общественной безопасности, системы социального обеспечения, образования и в любой другой, являющейся одной из их подсистем, а также государственной обороны или других государственных служб, наказываются лишением свободы от четырех до шести лет и штрафными днями в количестве от 300 до 500.

Статья 9. Изменение, нарушение целостности и доступности данных
Лицо, нарушающее безопасность компьютерной системы, тем самым уничтожая, изменяя, дублируя, приводя в непригодное состояние или повреждая информацию, данные или процессы, касающиеся их целостности, доступности и конфиденциальности на любой из стадий: получения, обработки, передачи или хранения, наказывается лишением свободы от четырех до шести лет и штрафными днями в количестве от 300 до 500.

Статья 10. Повреждение компьютерных систем
Лицо, уничтожающее, повреждающее, видоизменяющее, запускающее программу или осуществляющее какое-либо действие, которое изменяет функционирование или выводит из строя частично или полностью компьютерную систему, использующую информационно-коммуникационные технологии или какой-либо физический или логический её элемент, наказывается лишением свободы на срок от трех до пяти лет и штрафными днями в количестве от 300 до 500.

Если вышеуказанное преступление совершено по неосторожности, назначается наказание в виде штрафных дней в количестве от 200 до 500.

Если преступление, предусмотренное данной статьей, касается какой-либо из частей компьютерной системы, использующих информационно-коммуникационные технологии и предназначенных для предоставления государственных или финансовых услуг или содержащих персональные данные, конфиденциальные персональные данные, государственную секретную информацию, а также техническую или относящуюся к физическим или юридическим лицам информацию, назначается наказание в виде лишения свободы от четырех до шести лет и штрафных дней в количестве от 300 до 600.
Если действие, предусмотренное в предыдущем абзаце, совершено по неосторожности, назначается наказание в виде штрафных дней в количестве от 300 до 600.

Статья 11. Владение оборудованием или предоставление услуг в целях нарушения информационной безопасности

Лицо, владеющее, производящее, предоставляющее, адаптирующее, ввозящее, продающее оборудование, устройства, компьютерные программы, пароли или коды доступа в целях создания уязвимости, неправомерного нарушения информационной безопасности любой компьютерной системы, а равно предлагающее или предоставляющее услуги, предназначенные для совершения любого из преступлений, предусмотренных настоящим Законом, наказывается лишением свободы на срок от четырех до шести лет и штрафными днями в количестве от 300 до 600.

Глава III
О компьютерных преступлениях

Статья 12. Компьютерное мошенничество

Лицо, которое в результате неправомерного использования информационно-коммуникационных технологий, с помощью каких-либо манипуляций с компьютерными системами или любой из их частей, компьютерными данными или содержащейся в них информацией, внедряет ложную или мошенническую информацию, в результате чего получает выгоду для себя или третьих лиц в ущерб другим лицам, наказывается лишением свободы от трех до шести лет и штрафными днями в количестве от 300 до 600.

Статья 13. Компьютерный шпионаж

Лицо, незаконно овладевшее конфиденциальными персональными данными или государственной секретной информацией, содержащейся в системе, использующей информационно-коммуникационные технологии, или в любой ее части, наказывается лишением свободы от пяти до восьми лет и штрафными днями в количестве от 300 до 600.
Если какое-либо из вышеуказанных действий совершается с целью извлечения выгоды для себя или третьих лиц, и в случае угрозы безопасности суверенитета государства, надежности функционирования подверженных

опасности учреждений, или если в результате указанных действий нанесён ущерб физическим или юридическим лицам ввиду разглашения информации, отнесенной согласно закону к государственной секретной, назначается наказание в виде лишения свободы от шести до десяти лет и штрафных дней в количестве от 300 до 600.

Статья 14. Нарушение безопасности компьютерной системы

Лицо, без наличия соответствующего разрешения нарушающее безопасность какой-либо компьютерной системы с ограниченным или защищенным доступом, наказывается лишением свободы от двух до пяти лет и штрафными днями в количестве от 300 до 600.

Такое же наказание назначается лицу, которое подстрекает третье лицо выполнить на недобровольной основе действия, указанные в предыдущем абзаце.

Статья 15. Кража с помощью компьютерных средств

Лицо, которое посредством информационно-коммуникационных технологий присваивает материальные или нематериальные блага или ценности имущественного характера, лишая их собственника, держателя или владельца, с целью получения экономической выгоды для себя или другого лица, в случае если стоимость похищенного превышает два минимальных месячных размера оплаты труда в промышленном секторе3, наказывается лишением свободы от двух до пяти лет и штрафными днями в количестве от 300 до 600.

Глава IV

Компьютерные преступления, связанные с содержимым данных

Статья 16. Манипуляции с записями

Лицо, которое, злоупотребляя своими полномочиями в рамках управления технологическими общедоступными или частными платформами, отключает, изменяет, скрывает, уничтожает или приводит в негодность полностью или частично информацию любого типа, данные, содержащиеся в журнале доступа или использования их элементов, наказывается лишением свободы от пяти до восьми лет и штрафными днями в количестве от 300 до 600.

Если вышеуказанные действия способствуют совершению другого преступления третьим лицом, нижний и верхний пределы наказания увеличиваются на одну треть.

Статья 17. Мошеннические манипуляции со смарт-картами или аналогичными инструментами

Лицо, которое намеренно и без наличия соответствующего разрешения, каким-либо образом создает, перехватывает, записывает, копирует, изменяет, дублирует, клонирует или удаляет компьютерные данные, содержащиеся на смарт-карте или на любом другом инструменте, предназначенном для тех же

целей; для включения, изменения данных о пользователях, учетных записей, журналов, несанкционированных операций, наказывается лишением свободы от пяти до восьми лет и штрафными днями в количестве от 300 до 600.

Статья 18. Незаконное получение благ или услуг с помощью смарт-карт или аналогичных средств

Лицо, без наличия соответствующего разрешения и с помощью информационно-коммуникационных технологий использующее чужую смарт-карту или инструмент, предназначенный для тех же целей, для получения любого вида благ или услуг либо для обеспечения их оплаты без принятия на себя обязательства по соразмерной оплате полученных благ или услуг, наказывается лишением свободы от пяти до восьми лет и штрафными днями в количестве от 300 до 600.

Статья 19. Неправомерное предоставление благ или услуг

Лицо, знающее, что срок действия смарт-карты или инструмента, предназначенного для тех же целей, истек или они аннулированы, либо ненадлежащим способом получены, удержаны, фальсифицированы или изменены; предоставляет их кому-либо в качестве денег, товаров, услуг или любой другой вещи, имеющей экономическую ценность, наказывается лишением свободы от пяти до восьми лет штрафными днями в количестве от 300 до 600.

Статья 20. Нарушение судебной охраны данных

Лицо, знающее, что компьютерная система или любая из ее частей находится под охраной суда, пользуется ими, манипулирует записями или их содержимым, срывает (повреждает) пломбы или печати, наказывается лишением свободы от одного года до четырех лет.

Если действие, указанное в предыдущем абзаце, совершено лицом, ответственным за судебную охрану, либо с его помощью или с его разрешения, назначается наказание от двух до пяти лет лишения свободы.

Статья 21. Разглашение конфиденциальной информации

Лицо, разгласившее конфиденциальную информацию, ставшую ему известной в связи с участием в процессе расследования, сбора, перехвата или прослушивания данных компьютерной системы или ее частей, наказывается штрафными днями в количестве от 100 до 300.

Статья 22. Искажение и присвоение цифровой идентифицирующей информации

Лицо, исказившее или завладевшее цифровой идентифицирующей информацией физического или юридического лица посредством информационно-коммуникационных технологий, наказывается лишением свободы от трех до пяти лет и штрафными днями в количестве от 200 до 500.

Если действия, указанные в предыдущем абзаце, сопряжены с нанесением ущерба, вымогательством, обманом, оскорблениями или угрозами другому лицу с целью причинения вреда или получения выгоды для себя или третьих лиц, назначается наказание в виде лишения свободы от пяти до восьми лет и штрафных дней в количестве от 300 до 600.

Статья 23. Несанкционированное разглашение

Лицо, без наличия разрешения разглашающее код, пароль или любые другие средства доступа к программе, информации или данным, хранящимся на технологическом оборудовании или устройстве, с целью извлечения выгоды для себя или третьих лиц либо совершения преступления, наказывается лишением свободы от пяти до восьми лет и штрафными днями в количестве от 200 до 500.

Статья 24. Использование персональных данных

Лицо, которое без наличия разрешения, использует персональные данные посредством информационно-коммуникационных технологий, нарушая при этом системы конфиденциальности и безопасности данных, добавляя или изменяя данные в ущерб третьим лицам, наказывается лишением свободы от четырех до шести лет и штрафными днями в количестве от 200 до 500.

Нижний и верхний пределы наказания, предусмотренного в предыдущем абзаце, увеличиваются на одну треть в отношении лица, предоставившего или раскрывшего другому лицу информацию, зарегистрированную в архиве или в банке персональных данных, которая должна храниться в тайне.

Статья 25. Передача государственной секретной информации

Лицо, без разрешения либо с превышением пределов имеющегося у него разрешения передающее информацию, отнесенную согласно закону, к государственной секретной, посредством использования которой посягающее на компьютерную систему или данные, либо ставящее под угрозу суверенную безопасность государства, используя при этом информационно-коммуникационные технологии любого вида, наказывается лишением свободы от пяти до восьми лет и штрафными днями в количестве от 200 до 500.

Статья 26. Неправомерное раскрытие данных или информации персонального характера

Лицо, которое без согласия владельца информации частного и персонального характера, раскрывает, распространяет или передает полностью или частично указанную информацию или данные, будь то изображения, видео, тексты, аудио или прочие, полученные посредством информационно-коммуникационных технологий, наказывается лишением свободы от трех до шести лет и штрафными днями в количестве от 200 до 500.

Если одно из вышеуказанных действий совершено в корыстных целях, с целью облегчить совершение другого преступления или сопряжено с распространением материалов откровенно сексуального характера в ущерб третьим лицам, назначается наказание в виде лишения свободы от четырех до восьми лет и штрафных дней в количестве от 200 до 500.

Если одно из действий, предусмотренных настоящей статьей, совершено в отношении конфиденциальных персональных данных, назначается максимальное наказание, указанное в предыдущем абзаце, с возможностью увеличения его верхнего предела до одной трети.

Статья 27. Выдача себя за другое лицо в коммерческих сделках

Лицо, без разрешения, от имени третьего лица и с использованием информационных и коммуникационных технологий продающее товары или услуги, выдавая себя за авторизованного производителя, поставщика или дистрибьютора, наказывается лишением свободы от трех до пяти лет и штрафными днями в количестве от 200 до 500.

Наказание за действия, указанные в предыдущем абзаце, составляет от четырех до шести лет лишения свободы, в случае если объектом продажи являются лекарственные препараты, пищевые добавки или продукты питания, напитки или любые продукты, предназначенные для потребления человеком.

Статья 28. Об угрозах, осуществляемых посредством информационно-коммуникационных технологий

Лицо, которое угрожает другому посредством использования информационно-коммуникационных технологий с:

1. Причинением ему, его семье или другим связанным с ним лицам злодеяния, образующего состав преступления и кажущегося по своей природе правдоподобным, наказывается лишением свободы от одного года до трех лет.

2. Выдвижением обвинений в отношении чести или престижа, нарушением или разглашением тайн в ущерб ему, его семье, другим связанным с ним лицам либо организации, которую он представляет или в делах которой он заинтересован, наказывается лишением свободы от двух до четырех лет.

Если угроза осуществляется от имени реальных или предполагаемых организаций или групп, назначается наказание в виде лишения свободы от трех до пяти лет.

Если угроза причинения злодеяния, образующего состав преступления, направлена на запугивание жителей какой-либо группы населения, этнической, культурной или религиозной, коллективной социальной или любой другой группы лиц, и имела место реальная возможность быть подвергнутыми указанным угрозам, назначается наказание в виде лишения свободы от четырех до шести лет.

Статья 29. Провокация, оправдание и подстрекательство к совершению преступлений посредством информационно-коммуникационных технологий

Лицо, которое посредством информационно-коммуникационных технологий подстрекает, побуждает, провоцирует или способствует совершению преступлений, поощряет совершение преступлений либо восхваляет его исполнителя или соучастников либо поручает им

совершение преступления, наказывается лишением свободы от трех до пяти лет и штрафными днями в количестве от 200 до 500.

Статья 30. Распространение ложных новостей посредством информационно-коммуникационных технологий

Лицо, которое с использованием информационно-коммуникационных технологий публикует или распространяет ложную и / или искаженную информацию, которая вызывает тревогу, страх, беспокойство у населения, группы населения или его части, отдельного лица или его семьи, наказывается лишением свободы от двух до четырех лет и штрафными днями в количестве от 300 до 500.

Если публикация или распространение ложной и / или искаженной информации наносит ущерб чести, престижу или репутации лица либо его семьи, назначается наказание в виде лишения свободы от одного года до трех лет и штрафных дней в количестве от 300 до 500.

Если публикация или распространение ложной и / или искаженной информации подстрекает к ненависти и насилию, ставит под угрозу экономическую стабильность, общественный порядок, общественное

здоровье или суверенную безопасность, назначается наказание в виде лишения свободы от трех до пяти лет и штрафных дней в количестве от 500 до 800.

Глава V
Компьютерные преступления, связанные с сексуальной свободой и неприкосновенностью

Статья 31. Привлечение малолетних, несовершеннолетних или лиц с ограниченными возможностями, нуждающихся в опеке, к участию в порнографии посредством использования информационно-коммуникационных технологий

Лицо, которое посредством использования информационно-коммуникационных технологий подстрекает, способствует, продвигает, использует, злоупотребляет или эксплуатирует в сексуальных или эротических целях малолетних, несовершеннолетних или лиц с ограниченными возможностями, нуждающихся в опеке, заставляя их присутствовать или участвовать в публичном или частном сексуальном поведении, представлении или половом акте, наказывается лишением свободы от пяти до восьми лет и штрафными днями в количестве от 300 до 600.
Ни в одном из случаев, указанных в предыдущих абзацах, не имеет значения, имел ли место факт согласия потерпевшего.

Статья 32. Совращение лиц, не достигших 16 лет, или лиц с ограниченными возможностями, нуждающихся в опеке, посредством использования информационно-коммуникационных технологий

Лицо, достигшее 18 лет, которое делает явные или неявные предложения лицам, не достигшим 16 лет, или лицам с ограниченными возможностями, нуждающимся в опеке, о проведении встреч сексуального или эротического характера, либо для изготовления порнографических материалов посредством использования информационно-коммуникационных технологий для себя или третьих лиц, наказывается лишением свободы от одного года до трех лет.

Статья 33. Домогательство посредством использования информационно-коммуникационных технологий

Лицо, которое пытает, издевается, унижает, оскорбляет, клевещет либо иным образом влияет на психологическую или эмоциональную стабильность человека, подвергая тем самым опасности его жизнь или физическую неприкосновенность, посредством использования информационно-коммуникационных технологий, наказывается лишением свободы от двух до четырех лет.

В случае если потерпевшим является малолетний, несовершеннолетний или лицо с ограниченными возможностями, нуждающееся в опеке, назначается наказание в виде лишения свободы от четырех до шести лет.

Статья 34. Сексуальное домогательство посредством использования информационно-коммуникационных технологий

Совершеннолетнее лицо, которое отправляет сообщения, фразы, фотографии, видео или совершает другие недвусмысленные действия сексуального характера или содержания другому лицу без его согласия посредством использования информационно-коммуникационных технологий, наказывается лишением свободы от двух до четырех лет.

В случае если потерпевшим является лицо, не достигшее 16 лет, и вне зависимости от факта его согласия или несогласия, либо лицо с ограниченными возможностями, нуждающееся в опеке, назначается наказание в виде лишения свободы от четырех до шести лет.

Статья 35. Общие отягчающие обстоятельства

За совершение преступлений, указанных в статьях 31, 32, 33 и 34, назначается наказание по его верхним пределам с возможностью увеличения до одной трети максимально установленных, и лишением права заниматься своей профессиональной деятельностью в течение срока наказания, если любое из указанных действий совершено:

1. Родственниками по восходящей или нисходящей линиям, братьями и сестрами, супругами, сожителями и родственниками четвертой степени кровного родства или второй степени некровного родства4;
2. Высшим должностным лицом, должностным лицом и государственным служащим;
3. Лицом, ответственным за уход, опеку или наблюдение за потерпевшим
4. Любым лицом, пользующимся превосходством, возникшим в результате доверительных, образовательных, рабочих или любых других отношений.

Глава VI

Порядок, меры пересечения и процессуальные меры

Статья 36. Исследование, получение и сохранение данных

При исследовании, получении и сохранении данных, содержащихся в информационной системе или ее частях, данных трафика, соединения, доступа или любой другой полезной информации, применяются положения настоящего Закона.

Статья 37. Сохранение данных

Национальная полиция или прокуратура в рамках своей компетенции действуют с оперативностью, необходимой для сохранения данных, содержащихся в информационной системе или ее частях, либо в данных

трафика системы, в основном, в случаях, когда они подвергнуты угрозе исчезновения или модификации.

Статья 38. Обеспечительные меры

Не затрагивая любых обеспечительных мер, могущих способствовать эффективному преследованию по делам преступлениях, подпадающих под действие настоящего Закона, могут быть запрошены следующие особые меры:

1. Изъятие и хранение компьютерных систем или устройств хранения данных.
2. Пломбирование, опечатывание и запрет на использование компьютерных систем или устройств хранения данных.
3. Требование немедленного сохранения данных, находящихся у третьих лиц.
4. Копирование данных.

Статья 39. Запрос о судебном разрешении

На этапе расследования для получения и сохранения информации, содержащейся в компьютерных системах или любых их частях, требуется разрешение любого судьи районного суда по рассмотрению уголовных дел, полученное в ответ на мотивированное ходатайство Национальной полиции или прокуратуры. Сразу после начала процесса любая из сторон вправе запросить разрешение у судьи по делу.

В этих целях судья вправе:

1. Обязать физическое или юридическое лицо немедленно предоставить информацию, содержащуюся в компьютерной системе или в любой из ее частей;
2. Обязать физическое или юридическое лицо сохранять и поддерживать целостность компьютерной системы или любой из ее частей, сохранить данные трафика, соединения, доступа или любую другую информацию, которая находится в его распоряжении или под его контролем и которая может быть полезной для расследования на срок до девяноста (90) дней. Такое распоряжение может быть продлено единожды и на такой же срок;
3. Распорядиться о доступе к указанной компьютерной системе или к любой из ее частей;
4. Обязать поставщика услуг предоставить информацию о данных, относящихся к пользователю, которые он может иметь в распоряжении или под своим контролем;
5. Произвести выемку или обеспечить сохранность полностью или частично компьютерной системы или любой из ее частей;
6. Сделать и сохранить копию содержимого компьютерной системы или любой из ее частей;
7. Распорядиться о поддержании целостности содержимого информационной системы или любой из ее частей;
8. Сделать недоступным либо перенести содержимое компьютерной системы или любой из ее частей, к которому был осуществлен доступ в процессе расследования;

9. Обязать лицо, осведомленное о работе компьютерной системы или любой из ее частей или о мерах защиты данных в указанной системе, предоставить необходимую информацию для проведения соответствующего расследования;

несовершеннолетних, а также лиц с ограниченными возможностями, нуждающихся в опеке, исследуются и рассматриваются в суде первой инстанции, специализирующемся на преступлениях насильственного характера.

Статья 41. Ответственность по судебной охране компьютерных систем

Лицо, которому было доверено хранение компьютерной системы или любой из ее частей, а также их содержимого, сохраняет их конфиденциальность и целостность, не позволяя третьим лицам, не относящимся к компетентным органам, иметь доступ и знать о них.

Лицо, ответственное за охрану, не вправе использовать содержащуюся под охраной компьютерную систему или любую из ее частей в целях, не связанных с процессом расследования.

Статья 42. Конфиденциальность процесса расследования

Лица, участвующие в процессе исследования, сбора, прослушивания, перехвата данных компьютерной системы или ее частей, хранят конфиденциальность всей информации, о которой им стало известно в отношении проведенных компетентным органом процессуальных действий.

11. УКАЗ ПРЕЗИДЕНТА №. 24-2020. УТВЕРЖДЕНИЕ «НАЦИОНАЛЬНОЙ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ НА 2020-2025 ГГ.»

Вступление. Внедрение ИКТ, информационных и коммуникационных технологий, а также обеспечение связи посредством использования Интернета и широкополосной связи на глобальном уровне способствовало социально-экономическому развитию стран. Его использование положительно повлияло на глобальную конкурентоспособность за счет повышения эффективности и производительности.

Однако существуют кибернетические риски и угрозы, связанные с использованием ИКТ (информационных и коммуникационных технологий), которые требуют от стран разработки организационных структур, стратегий, правовых рамок и передовых средств защиты для борьбы с ними.

Вышеизложенное делает необходимым наличие Национальной стратегии кибербезопасности для управления и минимизации рисков перед лицом этого нового типа угроз, а также правил приобретения и эксплуатации технологий с учетом национального и международного контекста с точки зрения кибер-безопасности.

Национальная стратегия кибербезопасности устанавливает позицию Никарагуа в отношении новой концепции кибербезопасности до ее усилий по содействию развитию безопасного и надежного киберпространства на территории Никарагуа в рамках Политики национальной безопасности.

В международном контексте, учитывая выявленную международным сообществом уязвимость в использовании киберпространства, Организация Объединенных Наций и Организация американских государств приняли резолюции, направленные на создание «Всемирной культуры кибербезопасности и защиты основных информационных инфраструктур». и принятие «Комплексной межамериканской стратегии кибербезопасности: многоаспектный и междисциплинарный подход к созданию культуры кибербезопасности» соответственно.

В латиноамериканском регионе страны, включая Никарагуа, приступили к разработке стратегий кибербезопасности, чтобы гарантировать защиту прав граждан, государства и общества в целом при использовании ИКТ, приняв и взяв за основу резолюции вышеупомянутых организаций.

С другой стороны, применение государственной политики и условия экономической стабильности в Никарагуа позволили увеличить инвестиции и, в частности, развитие телекоммуникационного сектора, представляя важные достижения с точки зрения доступа и использования технологий. Информация и коммуникация; Точно так же расширение технологической инфраструктуры широкополосной связи оказывает важное влияние на экономическое и социальное развитие страны.

В рамках государственной политики Никарагуа НАЦИОНАЛЬНАЯ ПРОГРАММА ЧЕЛОВЕЧЕСКОГО РАЗВИТИЯ НА 2018–2021 ГГ. содержит оси суверенной безопасности и развития телекоммуникаций, на которых основана разработка Национальной стратегии кибербезопасности, позволяющей продолжать реализацию планов и программ, гарантирующих, что Никарагуа продолжает оставаться самой безопасной страной в регионе Центральной Америки.

В этом смысле, несмотря на достижения в области кибербезопасности, области, которые необходимо продолжать укреплять посредством создания Национальной стратегии кибербезопасности, включают: организационную структуру, нормативно-правовую базу; технологическая инфраструктура; человеческий талант технического персонала; и в первую очередь возможности граждан в области безопасного и ответственного использования ИКТ.

Основные принципы
Защита прав граждан в киберпространстве.
Управление рисками и потенциал устойчивости
Защита и оборона киберпространства
Развитие национальных и международных союзов и сотрудничества.

Национальная стратегия кибербезопасности

* Структура и содержание стратегии
* Общая цель.
* Конкретные цели

Стратегические оси:

1. Стратегическая ось 1: Институциональное укрепление.
2. Стратегическая ось 2: Укрепление правовой базы
3. Стратегическая ось 3 Образование и обучение
4. Стратегическая ось 4: Укрепление технологий
5. Стратегическая ось 5: Безопасность и отказоустойчивость критически важных служб и инфраструктур на национальном уровне

12. АДМИНИСТРАТИВНОЕ СОГЛАШЕНИЕ 01-2021 – ПРАВИЛА СОХРАНЕНИЯ ДАННЫХ И ИНФОРМАЦИИ

Устанавливает обязанность Операторов, уполномоченных TELCOR, сохранять данные и информацию, сгенерированные или обработанные в рамках предоставления телекоммуникационных услуг, в целях предотвращения, расследования, судебного преследования и наказания за совершение преступлений, установленных в Законе № 1042 «Особый Закон о киберпреступлениях».

Статья 2. Обязанные субъекты Операторы электросвязи, уполномоченные TELCOR, будь то физические или юридические лица, для предоставления фиксированной и мобильной телефонной связи, и услуг Интернета, а также общественных ретрансляторов и транкинговых каналов в следующих условиях:
Стационарная связь
Сотовая связь
Доступ в Интернет
Передача данных
Маркетинг телекоммуникационных услуг
Служба клиента

Маркетинг службы спутниковой связи
Маркетинг спутниковой связи
Наземные станции телепортов
Станции VSAT
Ретрансляторы и магистральные пункты связи.

Статья 3. Обязательство по сохранению данных и информации

Субъекты, подлежащие данному регламенту, должны сохранять следующие данные и информацию абонента, который инициирует вызов;
полное имя, номер документа, удостоверяющего личность, и адрес пользователя услуги, если исходный номер находится в той же сети.
Что касается доступа в Интернет, электронной почты в Интернете и интернет-телефонии:
идентификация пользователя;
идентификацию пользователя и/или объекта и номер телефона, присвоенный всем средствам связи, имеющим доступ к телефонной сети общего пользования;
имя и адрес пользователя услуги и/или объекта, которому во время связи был назначен адрес интернет-протокола (IP), идентификатор пользователя или номер телефона.
Информация о коммуникационном протоколе, используемом в службе, и номер коммуникационного порта.
Данные, необходимые для определения адресата сообщения:
В отношении стационарной и мобильной телефонной связи:
Набранный номер или номера (телефонный номер или номера адресата) и, в тех случаях, когда задействованы другие услуги, например вызов переадресация или переадресация, номер(а), на который переадресовываются вызовы; и
Полные имена, номера документов, удостоверяющих личность, и адреса пользователей услуг, если номера назначения находятся в одной сети.
В отношении электронной почты в Интернете и интернет-телефонии (VoIP):
идентификатор пользователя или номер телефона получателя(ей) телефонного звонка в Интернете; и
Полные имена, номера документов, удостоверяющих личность, и адреса пользователей услуг, а также идентификатор пользователя получателя сообщения.
Информация о протоколе связи, используемом в услуге, и номер порта связи.
Данные, необходимые для определения даты, времени и продолжительности связи:
По фиксированной и мобильной связи: дата и время начала и окончания связи;
2) В отношении доступа в Интернет, электронной почты в Интернете и интернет-телефонии (VoIP):

Дата и время подключения и отключения услуги доступа в Интернет с учетом определенного часового пояса, а также адрес интернет-протокола (IP), динамический или статический, назначенный Поставщиком услуг, а также идентификацию зарегистрированного пользователя; и
Дата и время подключения и отключения службы электронной почты в Интернете или службы телефонной связи в Интернете в зависимости от определенного часового пояса.
Данные, необходимые для определения типа связи:
В отношении стационарной и мобильной телефонной связи: используемая телефонная служба;
В отношении электронной почты и интернет-телефонии: используемая интернет-служба.
Данные, необходимые для идентификации коммуникационного оборудования пользователей или того, что считается коммуникационным оборудованием:
В отношении фиксированной телефонной связи: исходящий и целевой телефонные номера;
В отношении мобильной телефонии (голос и данные):
телефонные номера отправителя и получателя;
Международный идентификатор мобильного абонента (IMSI) вызывающей стороны;
Международный идентификатор мобильного оборудования (IMEI) вызывающей стороны;
MAC-адрес (управление доступом к среде) оборудования.
В отношении доступа в Интернет, электронной почты в Интернете и Интернет-телефонии:
исходный номер телефона в случае доступа путем набора номера;
цифровая абонентская линия (DSL) или другой идентифицирующий оконечный пункт отправителя сообщения.
MAC-адрес (управление доступом к среде) оборудования.
Данные, необходимые для определения местоположения оборудования мобильной связи:
Метка местоположения (идентификатор соты) в начале и конце связи; и
2данные, которые позволяют определить географическое местоположение ячейки по метке местоположения в течение периода, в течение которого хранятся данные связи.
Данные, которые должны сохраняться и предоставляться операторами, предоставляющими услуги коллективных ретрансляторов и транковых каналов.
1) Рабочая частота, назначенная пользователю
2) Реестр тонов, назначенный пользователю
3) Идентификационные номера ID, присвоенные пользователю
4) Реестр групп, используемых в магистральной связи
5) Серийные номера оборудования, поставляемого пользователям

6) Данные, идентифицирующие ретранслятор и/или канал, к которому подключено оборудование пользователя.
7) Данные, которые позволяют определить географическое положение мобильного оборудования по присвоенному идентификатору.

Статья 4. Общие правила сохранения данных и информации
Обязанные субъекты принимают необходимые меры для обеспечения полного сохранения данных, указанных в статье 3 настоящего Регламента, в той мере, в какой они создаются или обрабатываются, в рамках оказание указанных услуг связи.
Обязанные субъекты ни в коем случае не могут воспользоваться или использовать данные и информацию, созданные их пользователями, в целях, отличных от тех, которые установлены в Законе № 1042 «Специальный закон о киберпреступлениях» и других правовых нормах.
Данные и информация, сохраненные в соответствии с положениями настоящего Регламента, могут быть предоставлены только Национальной полиции или Государственному министерству в соответствии с положениями Закона № 1042 «Специальный закон о киберпреступлениях», без ущерба для установленного в Законе № 735 «Закон о предупреждении, расследовании и преследовании организованной преступности и управлении арестованными, конфискованными и брошенными активами», его положения и другие законы по этому вопросу.

Статья 5. Срок хранения данных и информации
. Обязанные субъекты должны хранить данные и информацию, указанные в настоящих правилах, в течение двенадцати месяцев, считая с даты, когда сообщение было послано.
Статья 6.- Регистрация пользователей с предоплатой
Операторы, подключающие услуги мобильной связи и Интернета в режиме предоплаты, должны вести обновленную запись о каждом пользователе, которая включает как минимум: полное имя, национальность и адрес пользователя, номер и тип документа, удостоверяющего личность, и код или номер присвоенного линия.
Эта запись должна обновляться и храниться в течение как минимум периода, указанного в статье 5 настоящего Регламента, и при необходимости должна быть немедленно предоставлена регулирующему органу TELCOR. Кроме того, он должен быть доступен для Национальной полиции и прокуратуры.

Статья 7.- Санкции
Несоблюдение или нарушение положений настоящего Регламента обязанными субъектами приведет к открытию соответствующей санкционной процедуры без ущерба для других санкций, установленных в других Законах.

13. РУКОВОДСТВО ПО ОБНАРУЖЕНИЮ, ФИКСАЦИИ, ИЗЪЯТИЮ И ХРАНЕНИЮ ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ.

Способствует управлению учреждениями системы уголовного правосудия; предоставляет должностным лицам возможность получения инструкций, информации, методов и процедур для выполнения задач по обращению с доказательствами и их хранению, гарантирует постоянное, последовательное и скоординированное совершенствование их действий при предоставлении услуг с требуемым уровнем качества и эффективности для обеспечения правосудия.

Манагуа, 28 декабря 2022 г.