



Правовая база

Противодействие преступлениям в сфере компьютерной информации.

Аннотация:

Нормативная правовая регламентация деятельности Национальной полиции Республики Никарагуа в части борьбы с преступностью в сфере компьютерной информации, осуществляется в рамках политической Конституции Республики Никарагуа и отдельных положений закона № 872, закона 735, закона 406, уголовно-процессуального кодекса (закон 406), закона 1042, Указа Президента № 5. 24-2020, административного соглашения 01-2021, наставления по обнаружению, фиксации, изъятию и хранению вещественных доказательств.

Переводы указанных нормативных правовых актов могут быть использованы при реализации дополнительных профессиональных программ – программ повышения квалификации «Противодействие преступлениям в сфере компьютерной информации.».

1. КОНСТИТУЦИЯ РЕСПУБЛИКИ НИКАРАГУА
2. Закон № 872. ЗАКОН ОБ ОРГАНИЗАЦИИ, ФУНКЦИЯХ, СЛУЖБЕ И СПЕЦИАЛЬНОМ РЕЖИМЕ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ ПОЛИЦИИ.
3. ЗАКОН 735. О ПРЕДОТВРАЩЕНИИ, РАССЛЕДОВАНИИ И УГОЛОВНОМ ПРЕСЛЕДОВАНИИ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ, И РАСПОРЯЖЕНИИ АРЕСТОВАННЫМ, КОНФИСКОВАННЫМ И БРОШЕННЫМ ИМУЩЕСТВОМ, И ПОПРАВКИ К ДАННОМУ ЗАКОНУ
4. ЗАКОН 406 «УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ КОДЕКС РЕСПУБЛИКИ НИКАРАГУА»
5. ЗАКОН 1042. СПЕЦИАЛЬНЫЙ ЗАКОН О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ
6. УКАЗ ПРЕЗИДЕНТА № 5. 24-2020. УТВЕРЖДЕНИЕ «НАЦИОНАЛЬНОЙ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ 2020-2025»
7. АДМИНИСТРАТИВНОЕ СОГЛАШЕНИЕ 01-2021 – «ПРАВИЛА ХРАНЕНИЯ ДАННЫХ И ИНФОРМАЦИИ»
8. НАСТАВЛЕНИЕ ПО ОБНАРУЖЕНИЮ, ФИКСАЦИИ, ИЗЪЯТИЮ И ХРАНЕНИЮ ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ, Г. МАНАГУА, 2012 ГОД

1. КОНСТИТУЦИЯ РЕСПУБЛИКИ НИКАРАГУА

Статья 97. Национальная полиция - это вооружённая организация гражданского типа, отвечающая за соблюдение правопорядка в стране, организованная по принципу превентивности, инициативности и общинности, в которой активную роль играют граждане, семьи и общины.

Она призвана обеспечивать внутренний порядок, безопасность людей и их имущества, предотвращение, пресечение и расследование преступлений и другие установленные законом задачи.

Национальная полиция профессиональна, находится вне политики, не принадлежит ни одной партии, исполнительна и не является совещательным органом. Национальная полиция действует в строгом соответствии с Конституцией, чьи нормы соблюдает и выполняет. Она

подчиняется гражданской власти, осуществляемой президентом Республики, который является Верховным Главнокомандующим Национальной Полиции.

В рамках своих полномочий Национальная полиция оказывает помощь судебным и иным органам, которые в этом нуждаются, в выполнении ими своих функций в соответствии с законом.

Внутренняя организация национальной полиции основывается на единой иерархии и дисциплине ее руководства и личного состава.

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

Статья 1 Характер. вооружённая профессиональная организация гражданского типа, которая находится вне политики, не принадлежит ни одной партии, исполнительна и не является совещательным органом. Она является единственным и неделимым органом в стране, отвечающим за всю полицейскую деятельность. Действует в строгом соответствии с Конституцией Республики Никарагуа, нормы которой она чтит и соблюдает. Полиция подчиняется гражданской власти, осуществляемой президентом Республики, который является Верховным Главнокомандующим Национальной Полиции. Внутренняя организация национальной полиции основывается на единой иерархии и дисциплине ее руководства и личного состава.

Положения настоящего Закона вносят вклад в Национальную политику по предупреждению правонарушений и обеспечению безопасности граждан и людей.

Статья 7 Функции. Для выполнения своих задач, установленных Конституцией, Национальная полиция выполняет свои функции в следующих областях:

2) в расследовании преступлений, оказании помощи судебным органам и оперативно-розыскной деятельности. Данные функции и полномочия Национальной Полиции, направленные на преследование и расследование преступлений в целом, организованной преступности, терроризма, наркоторговли и связанных с ними преступлений, включают в себя следующие виды деятельности:

a) расследование любого деяния, которое может представлять собой преступление или правонарушение, недопущение негативных последствий после совершения подобных деяний, выявление и задержание предполагаемых преступников и участников, вхождение в жилище и изъятие имущества; сбор материалов, представляющих интерес для следствия и другой информации, необходимой для раскрытия преступления.

b) Предотвращение, пресечение и расследование уголовно наказуемых деяний насильственного характера, а также оказание специализированной помощи лицам, пострадавшим в результате таковых деяний, в координации с соответствующими органами, учреждениями и секторами общества, руководствуясь соответствующим законодательством.

c) расследование общественно опасных преступлений, в зависимости от конкретной инстанции, в случаях, когда виновное лицо задержано на месте преступления или имеется заявление лица, имеющего соответствующие полномочия; в подобных случаях обязанностью сотрудника полиции является пресечение совершающегося преступления, оказание помощи потерпевшему лицу, обеспечение безотлагательных следственных действий и задержание предполагаемых исполнителей преступления.

d) борьба с организованной преступностью, терроризмом, незаконным оборотом наркотиков, психотропными и другими контролируруемыми веществами, и связанными с ними преступлениями, а также с общей преступной деятельностью с целью её предупреждения, выявления, расследования и пресечения.

е) сбор, получение и анализ любых данных, имеющих отношение к защите жизни, обеспечению безопасности и неприкосновенности людей и их имущества, а также к поддержанию внутреннего общественного и социального порядка.

ф) разработка и совершенствование планов и операций по борьбе с преступлениями, связанными с организованной преступностью, терроризмом, незаконным оборотом наркотиков, психотропными и другими контролируруемыми веществами, их прекурсорами и связанными с ними преступлениями, а также общей преступной деятельностью, включая операции по борьбе с наркопреступностью, тайные операции и специальные процессуальные действия.

г) Расследование в целях обнаружения и проверки предполагаемых преступных деяний проводится в соответствии с научными и логическими нормами, приемами и методами, характерными для такой деятельности, за исключением ограничений, установленных Политической конституцией, ратифицированными международными договорами, конвенциями и законом. Результаты расследования представляются в прокуратуру или компетентный судебный орган в виде рапорта.

h) организация и обновление полицейской архивной службы, получение, сортировка, классификация и хранение всей информации и документации, относящейся к расследованию преступлений и правонарушений, лиц, содержащихся под стражей, огнестрельного оружия, разрешений и лицензий, и других административных процедур, осуществляемых национальной полицией.

i) выдача справок о судимости, лицам их запросившим, а также их аннуляция в соответствии с установленными процедурами.

j) Выполнение и обеспечение соблюдения постановлений судебных и иных органов, наделенных надлежащими правовыми полномочиями, согласно соответствующим правовым процедурам.

k) Вызов на собеседование любого лица, которое может предоставить информацию, представляющую интерес для расследования в рамках, предусмотренных Законом.

l) Выполнение поручений или действий в рамках международного сотрудничества при расследовании уголовных дел. Подобные запросы поступают в соответствии с установленными процедурами и по каналам, предусмотренными международными договорами или соглашениями и законодательством страны.

m) Развивать партнерские отношения, взаимное сотрудничество с партнерами из других стран или с региональными или международными правоохранительными органами в целях усиления борьбы с транснациональной организованной преступностью.

Статья 9. Руководство НП. В соответствии с Конституцией Республики Никарагуа и настоящим Законом, в Национальной Полиции соблюдается иерархия, которая основывается на строгой дисциплине, соблюдаемой руководителями и личным составом. Для эффективного выполнения своих задач и функций руководство НП организовано следующим образом:

- 1) Верховное командование
- 2) Руководство Национальной Полиции
- 3) Руководство главных управлений и вспомогательных органов
- 4) Руководство управлений Полиции

Статья 10. Верховное командование. Верховное командование Национальной полицией осуществляет Президент Республики в качестве Верховного Главнокомандующего, который наделен следующими полномочиями:

Статья 11. Руководство Национальной Полиции. Управление на национальном уровне осуществляется Директором или Генеральным Директором, который осуществляет единоличное руководство этим учреждением в соответствии с Конституцией Республики Никарагуа,

настоящим Законом и внутренним законодательством, и подчиняется только Верховному Главнокомандующему Республики.

Статья 16. Главные управления Полиции. «Главные управления» - основные полицейские органы, занимающиеся борьбой с преступностью в целях обеспечения безопасности граждан и людей на всей территории страны; действуют согласно своим полномочиям в конкретных областях, основываясь на законодательных и нормативных положениях; разрабатывают и представляют на утверждение руководства и директивы, а также планируют, консультируют, контролируют, анализируют, оценивают и рекомендуют высшему органу полиции меры совершенствования соответствующих процессов и осуществляют оперативную деятельность, относящуюся к их компетенции. Они могут присутствовать и в территориальных управлениях. В таких случаях они находятся в функциональном подчинении у последних.

17 Функции главных управлений:

1) Оперативная служба полиции. Данное управление отвечает за выявление, предупреждение, расследование и нейтрализацию угроз и рисков, связанных с организованной преступностью, терроризмом и другими подобными преступлениями, которые подвергают опасности жизнь и здоровье людей, их имущество, угрожают семье и обществу.

2) Управление по борьбе с экономическими преступлениями отвечает за расследование преступлений против социально-экономического порядка, преступления против государственных финансов, подделка валюты, ценных бумаг и налоговых видов, преступления против культурного наследия нации, преступления против здоровья населения, преступления против природных ресурсов и окружающей среды, а также все преступления, имеющие экономические или имущественные последствия для государства; исследование и анализ заключительных технических отчетов, представляемых Группой финансового анализа. Для этого он получает, собирает, анализирует и распространяет информацию, связанную с этими преступлениями.

3) Управление по борьбе с незаконным оборотом наркотиков - ведущее управление в расследовании и пресечении незаконного оборота наркотиков, преступлений, связанных с наркотическими средствами, психотропными веществами, другими контролируемыми веществами, их прекурсорами и других преступлений организованной преступности, связанных с этой деятельностью. Для этого полиция получает, собирает, систематизирует, анализирует и распространяет информацию, связанную с этими преступлениями. Это подразделение отвечает за обмен информацией с зарубежными партнерами и международными учреждениями

4) Следственное управление: это специальность, которая по собственной инициативе, по жалобе или по распоряжению прокурора, проводит расследование и документирует любое деяние, которое может представлять собой преступление или правонарушение; выявлять и задерживать лиц, подозреваемых в совершении преступлений, а также собирать полезные следственные материалы, доказательства и улики, составлять соответствующие полицейские отчеты и направлять их в установленные законом сроки компетентным органам, как это предусмотрено соответствующими законами.

5) Безопасность и защита личности. Данное управление, отвечает за разработку и осуществление системы превентивных мер и оперативных процедур для всестороннего обеспечения безопасности жизни и физической неприкосновенности президента Республики и его семьи, Вице-президента Республики, председателей органов государственной власти и других лиц, как в общественной, так и в личной жизни.

17) Полицейская контрразведка. Управление, отвечающее за разработку стратегий, планов и оперативных действий по защите полицейских операций, информации, документации, объектов и персонала, а также противодействию угрозам организованной преступности и другим преступным проявлениям внутри страны.

19) Институт криминалистики и судебной экспертизы участвует в техническом осмотре мест, где предположительно было совершено преступное деяние, собирает и обрабатывает доказательств по уголовному делу, проводит экспертизы, используя научные методы и процедуры, готовит соответствующие доклады для обеспечения следственной деятельности полиции по запросу судебных и других органов в соответствии с Законом

3. ЗАКОН 735. О ПРЕДОТВРАЩЕНИИ, РАССЛЕДОВАНИИ И УГОЛОВНОМ ПРЭСЛЕДОВАНИИ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ, И РАСПОРЯЖЕНИИ АРЕСТОВАННЫМ, КОНФИСКОВАННЫМ И БРОШЕННЫМ ИМУЩЕСТВОМ, И ПОПРАВКИ К ДАННОМУ ЗАКОНУ

Настоящий закон направлен на регулирование функций 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, охватываемых настоящим Законом.

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

* Внедренный агент: 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: сотрудник полиции, который с одобрения Генерального директора Национальной полиции симулирует заинтересованность в передаче, покупке, приобретении или перевозке для себя или третьих лиц деньги, товары, людей, услуг, оружия, веществ, включенные в перечень или таблицу, прилагаемые к настоящему Закону, или заинтересованные в любой другой организованной преступной деятельности с целью достижения проявлений незаконного поведения или действия или изъятия незаконных веществ или товаров и выявления или поимки преступников 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.

* Конфидент: лицо, предоставляющее специализированным органам Национальной полиции или разведке Армии Никарагуа данные или сведения о подготовке или совершении преступления либо о тех, кто участвовал или будет участвовать в нем.

* Защита свидетелей, экспертов и других субъектов процесса: комплекс мер, действий и процедур, направленных на защиту жизни, личной неприкосновенности, свободы или имущества свидетеля, эксперта и других субъектов процесса или семьи охраняемого субъекта.

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 радиоэлектрических 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, подлежащих защите. Для целей настоящего Закона под лицами, подлежащими защите, понимаются жертвы, свидетели, эксперты и другие субъекты, участвующие в расследовании и уголовном процессе, а также члены их семей или другие лица, которым угрожает опасность или в связи с их прямым или косвенным участием в расследовании преступлений, упомянутых в настоящем Законе, или в силу их семейных отношений с лицом, участвующим в этих преступлениях.

Статья 68 Ситуация риска или опасности. Под риском или опасностью понимается разумное существование угрозы или ущерба жизни, личной неприкосновенности, свободе и безопасности лиц, упомянутых в предыдущей статье. Степень риска или опасности для какого-либо лица определяется совместно прокуратурой и национальной полицией при поддержке никарагуанской армии. Личность свидетеля может быть раскрыта судье только на специальном слушании, для чего не требуется указывать имя, личные данные и адрес в письме об обмене информацией содержащей доказательства.

Статья 69 Расходы на защиту. Расходы на осуществление мер защиты в целях охраны жизни, личной неприкосновенности, свобода и безопасность лиц, упомянутых в настоящей главе, будут финансироваться министерством финансов и государственного кредита, с использованием ресурсов, полученных от Группы управления и распоряжения имуществом, предметами, товарами, оборудованием или другими инструментами, используемыми или предназначенными для использования при совершении преступлений, охватываемых настоящим Законом.

Прокуратура совместно с Национальной полицией составляет годовой бюджет расходов на осуществление и осуществление данной программы.

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 агентов 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 проведение контролируемой поставки. Для проведения контролируемой поставки Генеральный директор Национальной полиции обращается с ходатайством о ее проведении к Генеральному прокурору Республики, который выносит постановление о разрешении на использование специального метода расследования – контролируемой поставки при наличии достаточных оснований полагать, что имело место совершение преступления, указанного в настоящем Законе, или начало его совершения, только при наличии одного или нескольких обстоятельств:

- a) расследование дела представляется невозможным или крайне сложным;
- b) особая значимость деяния требует вмешательства специалиста по негласным операциям ввиду безрезультатности прочих принятых мер;

с) необходимость в фиктивном приобретении или продаже предметов, вещей, ценностей или товаров, которые являются средствами преступления или выгодой в результате его совершения.

Статья 86. Цель негласных операций. Законными 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;

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

е) 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;

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

д) 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, совершенные 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 регламентом настоящего Закона.

4. ЗАКОН 406 «УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ КОДЕКС РЕСПУБЛИКИ НИКАРАГУА»

Статья 213. Перехват телефонных разговоров. Перехват телефонной или другой телекоммуникационной связи осуществляется в следующих случаях:

1. терроризм;
2. похищение с целью вымогательства;
3. торговля органами и людьми с целью передачи их в сексуальное рабство;
4. преступления, связанные с наркотиками, психотропными и другими контролируруемыми веществами;
5. Легализации капиталов или отмывание денежных средств и активов;
6. Международная торговля похищенным оружием, взрывчатыми веществами и транспортными средствами.

Запрещается перехват любого общения обвиняемого с его защитником.

Перехват телекоммуникаций осуществляется только по конкретному и обоснованному запросу Генерального прокурора Республики или Генерального директора Национальной полиции, которые должны обосновать причины такого вмешательства, и указывают также продолжительность, на которую запрашивается мера, а также людей, которые получают доступ к коммуникациям.

Судья устанавливает происхождение такой меры на основании обоснованного решения и прямо указывает дату прекращения перехвата, который не может длиться более тридцати дней. Данная мера может быть продлена только один раз и на такой же срок.

В процесс включаются только записи таких бесед или их часть, которые согласно запросу прокурора, считаются пригодными для установления истины. Однако обвиняемый может ходатайствовать о включении других переговоров или других сторон, которые были исключены, если он сочтет это целесообразным для своей защиты. Судья выносит постановление об уничтожении тех частей, которые не имеют отношения к процессу.

Все лица, имеющие доступ к перехваченной связи, должны держать в тайне ее содержимое, за исключением случаев, когда их необходимо использовать в процессе. Государственные служащие, нарушающие это положение, могут быть отстранены от должности без освобождения от соответствующей гражданской и уголовной ответственности.

Статья 214. Перехват письменных, телеграфных и электронных сообщений. Перехват письменных, телеграфных и электронных сообщений, в случаях расследования преступлений, упомянутых в предыдущей статье, осуществляется по разрешению компетентного судьи, при этом в ходатайстве указываются четкие основания и информация, которую ожидается получить. Решение суда, санкционирующее это положение, должно быть должным образом мотивировано.

Разрешение на начало оперативной работы по перехвату коммуникаций выдается судьей, а материалы, связанные с преступлением, включаются в материалы расследования.

5. ЗАКОН 1042. СПЕЦИАЛЬНЫЙ ЗАКОН О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

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 Ненадлежащий доступ к компьютерным системам
- * Статья 5 Ненадлежащий доступ к программному обеспечению или данным
- * Статья 6 Перехват сообщений и передачи между системами информационно-коммуникационных технологий
- * Статья 7 Неправомерное использование внешних коммуникаций с помощью информационно-коммуникационных технологий
- * Статья 8 Вмешательство компьютерной системы или данных
- * Статья 9 Изменение, повреждение целостности и доступности данных
- * Статья 10 Повреждение компьютерных систем
- * Статья 11 Владение оборудованием или предоставление услуг для нарушения компьютерной безопасности

Глава III «Компьютерные преступления»

- * Статья 12 Компьютерное мошенничество
- * Статья 13 Компьютерный шпионаж
- * Статья 14 Нарушение безопасности компьютерной системы
- * Статья 15 Кража с помощью компьютеров

Глава IV «Компьютерные преступления, связанные с содержанием данных»

- * Статья 16 Манипуляции с записями
- * Статья 17 Мошенническое манипулирование смарт-картами или аналогичными инструментами
- * Статья 18 Неправомерное получение товаров или услуг с помощью смарт-карт или аналогичных средств
- * Статья 19 Ненадлежащее предоставление товаров или услуг
- * Статья 20 Нарушение судебного режима хранения данных
- * Статья 21 Отсутствие конфиденциальности
- * Статья 22 Аннулирование и присвоение компьютерной идентичности
- * Статья 23 Несанкционированное разглашение
- * Статья 24 Использование персональных данных
- * Статья 25 Передача закрытой общественной информации
- * Статья 26 Ненадлежащее разглашение личных данных или информации
- * Статья 27 Компьютерная замена в маркетинговых актах
- * Статья 28 Об угрозах с помощью информационно-коммуникационных технологий
- * Статья 29 Провокация, пропаганда и склонение к совершению преступлений с использованием информационно-коммуникационных технологий

* Статья 30 Распространение фейковых новостей через информационно-коммуникационные технологии

Глава V «Компьютерные преступления, связанные с сексуальной свободой и неприкосновенностью»

* Статья 31 Использование детей, подростков или инвалидов, нуждающихся в особой защите, в порнографии с использованием информационно-коммуникационных технологий

* Статья 32 Коррупция лиц моложе 16 лет или инвалидов, нуждающихся в особой защите посредством использования информационно-коммуникационных технологий

* Статья 33 Притеснения с помощью информационно-коммуникационных технологий

* Статья 34 Сексуальные домогательства с использованием информационно-коммуникационных технологий

* Статья 35 Общие отягчающие условия

Глава VI Процедура, обеспечительные и процессуальные меры

* Статья 36 Исследование, получение и сохранение данных

* Статья 37 Сохранение данных

* Статья 38 Меры страхования

* Статья 39 Ходатайство о разрешении суда

* Статья 40 Объективная компетенция

* Статья 41 Ответственность судебного хранителя компьютерных систем

* Статья 42 Конфиденциальность процесса расследования

6. УКАЗ ПРЕЗИДЕНТА № 5. 24-2020. УТВЕРЖДЕНИЕ «НАЦИОНАЛЬНОЙ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ 2020-2025»

Введение. Внедрение ИКТ в сочетании с подключением к Интернету и широкополосной связи на глобальном уровне способствовало социально-экономическому развитию стран. Их использование положительно сказалось на глобальной конкурентоспособности за счет повышения эффективности и производительности.

Однако существуют риски и киберугрозы, связанные с использованием ИКТ (информационно-коммуникационных технологий), которые требуют от стран разработки организационных структур, стратегий, правовых рамок и передового оборонного потенциала для борьбы с ними.

Вышеизложенное требует разработки национальной стратегии кибербезопасности для управления рисками и сведения к минимуму этих новых угроз, а также правил приобретения и эксплуатации технологий с учетом национальных и международных условий кибербезопасности.

В Национальной стратегии кибербезопасности (НСБ) излагается позиция Никарагуа в отношении новой концепции кибербезопасности, которая способствует ее усилиям по содействию безопасному и надежному киберпространству на территории Никарагуа в рамках Национальной политики безопасности.

История. В международном контексте перед лицом уязвимости международного сообщества в использовании киберпространства Организация Объединенных Наций и Организация американских государств приняли резолюции, направленные на создание " «Глобальная культура кибербезопасности и защита важнейших информационных инфраструктур» и принятие "Комплексной межамериканской стратегии кибербезопасности: Многоаспектный и multidисциплинарный подход к созданию культуры кибербезопасности ".

В латиноамериканском регионе страны, в том числе Никарагуа, приступили к разработке стратегий кибербезопасности для обеспечения защиты прав граждан, государства и общества в целом на использование ИКТ, приняв и сославшись на резолюции вышеупомянутых организаций.

Кроме того, осуществление государственной политики и условия экономической стабильности в Никарагуа привели к увеличению инвестиций, в частности в развитие телекоммуникационного сектора, что свидетельствует о значительных достижениях в области доступа к информационно-коммуникационным технологиям и их использования; кроме того, расширение технологической инфраструктуры широкополосной связи, что существенно сказывается на экономическом и социальном развитии страны.

В рамках государственной политики Никарагуа Национальная программа развития человеческого потенциала на 2018-2021 годы содержит основные направления суверенной безопасности и развития телекоммуникаций, на которых основывается разработка Национальной стратегии кибербезопасности, что позволяет продолжать осуществление планов и программ, обеспечивающих, чтобы Никарагуа оставалась самой безопасной страной в регионе Центральной Америки.

В этой связи, несмотря на достигнутый прогресс в области кибербезопасности, к числу областей, требующих дальнейшего укрепления путем разработки национальной стратегии кибербезопасности, относятся: организационная структура, нормативная база; технологическая инфраструктура; человеческий талант технического персонала; и прежде всего возможности граждан в безопасном и ответственном использовании ИКТ.

Руководящие принципы

1. Защита прав граждан в киберпространстве.
2. Управление рисками и устойчивость
3. Защита и защита киберпространства
4. Развитие национальных и международных партнерств и партнерств.

Национальная стратегия кибербезопасности

- * Структура и сфера охвата Стратегии
- * Общая цель.
- * Конкретные цели

Стратегические оси:

1. Стратегический компонент 1: Укрепление организационной структуры.
2. Стратегическая направленность 2: укрепление правовых рамок
3. Стратегическое направление 3 «Образование, подготовка кадров и профессиональная подготовка».
4. Стратегическая направленность 4: Укрепление технологий
5. Стратегическое направление 5: Безопасность и устойчивость важнейших услуг и инфраструктуры на национальном уровне

7. АДМИНИСТРАТИВНОЕ СОГЛАШЕНИЕ 01-2021 – «ПРАВИЛА ХРАНЕНИЯ ДАННЫХ И ИНФОРМАЦИИ»

Он устанавливает обязанность операторов, уполномоченных телекоммуникационными и почтовыми службами(TELCOR) сохранять данные и информацию, полученные или обработанные в контексте предоставления телекоммуникационных услуг, в целях предупреждения, расследования, судебного преследования и наказания за совершение преступлений, предусмотренных Законом № 1042 «Специальный закон о киберпреступлениях».

Статья 2. Операторы связи, уполномоченные TELCOR, будь то физические или юридические лица, обязаны предоставлять услуги телефонной связи и фиксированного и мобильного Интернета, а также общественные ретрансляторы и магистральные (усеченных) каналов связи в следующих формах:

- a) Стационарная телефонная связь
- b) Сотовая телефонная связь
- c) Доступ к Интернету
- d) Передача данных
- e) Маркетинг телекоммуникационных услуг
- f) Служба доставки
- g) Коммерциализация службы спутниковой связи
- h) Коммерциализация спутниковой телефонии
- i) Наземные станции телепортации
- j) Наземные станции VSAT (очень маленькие и недорогие наземные станции спутниковой связи, напрямую подключенные к пользователям)
- k) Общинные ретрансляторы и магистральные каналы.

Статья 3. Обязательство сохранять данные и информацию

Субъекты, на которых распространяется действие настоящих Правил, должны сохранять следующие данные и информацию:

- a) данные, необходимые для отслеживания и идентификации происхождения сообщения:
 - 1) для стационарной и мобильной телефонии:
 - i) номер телефона, по которому поступил звонок
 - ii) полное имя, номер удостоверения личности и адрес пользователя услуги, когда исходный номер находится в одной сети.
 - 2) Что касается доступа в Интернет, электронной почты в Интернете и Интернет-телефонии (VoIP):
 - i) идентификация пользователя и/или назначенного объекта;
 - a) идентификация пользователя и/или средства и номер телефона, присвоенные любой связи, имеющей доступ к сети телефонной связи общего пользования;
 - 3) Имя и адрес пользователя услуги и/или средства, которому в момент связи был присвоен адрес Интернет-протокола (IP), идентификатор пользователя или номер телефона.
 - iv) информация протокола связи, используемая в номере сервиса и порта связи.
 - Б) данные, необходимые для идентификации места назначения сообщения:
 - 1) для стационарной и мобильной телефонии:
 - i) номер или набранные номера (целевой номер телефона или номера) и, в случае других услуг, таких, как переадресация или передача звонка, номер или номера, на которые передаются звонки; и
 - ii) полные имена, номера удостоверений личности и адреса пользователей услуг, когда номера назначения находятся в одной сети.
 - 2) Что касается электронной почты и Интернет-телефонии (VoIP):
 - i) идентификация пользователя или номера телефона получателя или получателей телефонного звонка по Интернету;
 - ii) полные имена, номера удостоверений личности и адреса пользователей услуг и идентификация пользователя получателя сообщения.
 - iii) информация о протоколе связи, используемом в номере сервиса и порта связи.
 - с) данные, необходимые для определения даты, времени и продолжительности сообщения:
 - 1) в отношении стационарной и мобильной телефонной связи: дата и время начала и окончания связи;

2) Что касается доступа в Интернет, электронной почты в Интернете и Интернет-телефонии (VoIP):

i) дату и время подключения и отключения службы доступа к Интернету на основе заданного часового пояса, а также динамический или статический адрес Интернет-протокола (IP), присвоенный поставщиком услуг, а также идентификацию зарегистрированного пользователя;

ii) дата и время подключения и отключения службы электронной почты Интернета или службы телефонии Интернета в зависимости от заданного часового пояса.

d) данные, необходимые для определения типа связи:

1) в отношении стационарной и мобильной телефонной связи: используемая телефонная служба; и

2) Что касается электронной почты в Интернете и телефонной связи в Интернете, то использовались услуги Интернета.

e) данные, необходимые для идентификации оборудования связи пользователей или того, что считается оборудованием связи:

1) в отношении фиксированной телефонной связи: телефонные номера страны происхождения и страны назначения;

2) в отношении мобильной телефонной связи (голосовая связь и передача данных):

i) номера телефонов страны происхождения и назначения;

ii) международная идентификация мобильного абонента (IMSI) вызывающей стороны;

3) Международная идентификация мобильного оборудования (IMEI) стороной осуществляющей вызов;

iv) MAC (Media Access Control) адрес компьютера.

3) Что касается доступа в Интернет, электронной почты в Интернете и телефонной связи в Интернете:

i) первоначальный номер телефона в случае доступа по номеру; и

ii) цифровой абонентской линии (DSL) или другого идентификатора терминала автора сообщения.

3) MAC (Media Access Control) адрес компьютера.

f) данные, необходимые для определения местонахождения оборудования мобильной связи:

1) метка местонахождения (идентификатор ячейки) в начале и конце сообщения; и

2) данные, позволяющие определить географическое местоположение ячейки путем указания на метку местоположения в течение периода, в котором хранятся передаваемые данные.

g) данные должны храниться и предоставляться операторами, предоставляющими услуги ретранслятора и магистральной связи.

1) Частота операций, порученных пользователю

2) Пользовательский регистр тонов

3) Идентификационные номера, присвоенные пользователю

4) Регистр групп, используемых в магистральной связи

5) Серийные номера оборудования, поставляемого пользователям

6) данные, идентифицирующие ретранслятор и/или канал, по которому подключено оборудование пользователя.

7) данные, позволяющие определить географическое местонахождение мобильного оборудования с помощью идентификационного номера.

Статья 4. Общие правила сохранения данных и информации

Обязанные стороны принимают необходимые меры для обеспечения полного сохранения данных, указанных в статье 3 настоящих Правил, в той мере, в какой они генерируются или обрабатываются, в контексте предоставления соответствующих телекоммуникационных услуг.

Ни в коем случае обязанные стороны не могут использовать или использовать данные и информацию, полученные от своих пользователей, в иных целях, чем те, которые установлены в Законе № 1042 «Специальный закон о киберпреступности» и других правовых нормах.

Данные и информация, хранящиеся в соответствии с положениями настоящего Положения, могут предоставляться только национальной полиции или прокуратуре в соответствии с положениями Закона № 1042 «Специальный закон о киберпреступности» без ущерба для положений Закона № 735 «Закон о предупреждении, расследовании и судебном преследовании организованной преступности, и распоряжении арестованным, конфискованным и оставленным имуществом», его положений и других соответствующих законов.

Статья 5. - Период сохранения данных и информации

Уполномоченные лица сохраняют данные и информацию, указанные в настоящих правилах, в течение двенадцати месяцев с даты, на которую было направлено сообщение

Статья 6. Регистрация prepaid пользователей

Операторы, активирующие телефонную связь и услуги мобильного интернета в рамках prepaid режима, должны вести обновленный учет каждого пользователя, который включает по крайней мере: полное имя, гражданство и адрес пользователя, идентификационный номер и тип и код или номер назначенной линии.

Этот регистр должен обновляться и храниться по крайней мере в течение периода, указанного в статье 5 настоящих Правил, и должен незамедлительно представляться TELCOR-Ente Regulador, когда это требуется. Она также должна быть доступна для сотрудников национальной полиции и прокуратуры.

Статья 7. Меры наказания

Несоблюдение или несоблюдение положений настоящих Правил обязанными сторонами приводит к возбуждению соответствующей процедуры санкций без ущерба для других санкций, установленных в других законах.

8. НАСТАВЛЕНИЕ ПО ОБНАРУЖЕНИЮ, ФИКСАЦИИ, ИЗЪЯТИЮ И ХРАНЕНИЮ ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ, Г. МАНАГУА, 2012 ГОД

Способствует совершенствованию управления учреждениями и операторами системы уголовного правосудия; предоставляет сотрудникам средства для получения образования, информации, методов и процедур работы с доказательствами и их цепочки хранения, обеспечивает постоянное, последовательное и скоординированное совершенствование их деятельности; предоставляет услуги на требуемых качественных и эффективных уровнях в целях расширения доступа к системе уголовного правосудия.

Исполнитель:

переводчик-методист Учебного центра
(филиала) СибЮИ МВД РФ
капитан полиции

Д.С. Аксенов