Санкт-Петербургский Политехнический университет Петра Великого

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

**РЕФЕРАТ**

Дисциплина: **Защита информации**

Тема: Закон защиты информации

Выполнил студент гр. 43501/1 Чан Ван Кует

Проверил Новопашенный А. Г

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2016г.

Санкт-Петербург

2016

**Глава I**

**ОБЩИЕ ПОЛОЖЕНИЯ**

**Статья 1. Сфера деятельности**

Этот закон предусматривает для безопасной эксплуатации информации, включая обеспечение информацией о мерах предосторожности в сети; Защита личной информации в сети Интернет; криптография и защита информации; Стандарты управления, технические регламенты и информация о безопасности; научные исследования и разработки и бизнес в области информационной безопасности; развитие человеческих ресурсов, информационная безопасность; Государственное управление информационной безопасности; права и обязанности организаций и физических лиц, занимающихся информационной безопасностью.

**Статья 2**. **Субъекты применения**

Настоящий Закон применяется к организациям и физическим лицам, так и вне страны, непосредственно участвующих в или связанным с деятельностью информационной безопасности во Вьетнаме.

**Статья 3**. **Применение законов**

1. Там, где есть расхождения между положениями настоящего Закона с положениями других законов о деятельности информационной безопасности во Вьетнаме применяются положения настоящего Закона.

2. Если положения настоящего Закона, кроме положений международных договоров, к которым Социалистическая Республика Вьетнам является Договаривающейся Стороной применяются положения этого договора.

**Статья 4**. **Определения**

**В настоящем Законе используются следующие термины трактуются следующим образом:**

1. Информационная безопасность является защита информации и информационных систем предотвращения доступа, использования, разглашения, разрушение, изменение или несанкционированного уничтожения, с тем чтобы обеспечить целостность, конфиденциальность и доступность информации.

2. Информационная система представляет собой совокупность оборудования, программного обеспечения и базы данных настроен для достижения цели создания, поставки, передачи, сбора, обработки, хранения и обмена информацией ,

3. Информационная система является важным информационные системы на национальном уровне играют роль, а это означает политическую, экономическую и социальную значимость, когда уничтожили бы серьезно повлиять обороны и безопасности страна, социальный порядок и безопасность и общественный интерес.

4. Важные министерства информационной системы на уровне, местные информационные системы играют роль, значение для развития и управления министерств, отраслей и местностей, когда разрушены вызовет мешать работе министерств, отраслей, местностей, общественного порядка и безопасность и общественный интерес.

5. Нарушение информационной безопасности является актом доступа, использование, раскрытие, нарушить, изменить, исказить функцию, несанкционированного уничтожения информации и информационных систем.

6. Риск потери информационной безопасности являются факторами внутри или снаружи, способные влиять на состояние информационной безопасности.

7. Оценка риска для безопасности полетов представляет собой информацию идентификации, анализа информации риска для безопасности полетов и прогнозирования возможной степени охвата и потенциальный ущерб воздействия, когда произошел инцидент полицию подробную информацию.

8. Риск Управление информационной безопасностью является реализация информации по оценке риска безопасности, определить необходимость защиты информации и информационных систем и прикладных решений по предупреждению, пресечению и минимизации ущерба при информация инцидент безопасности.

9. Сеть общий термин, используемый для обозначения фиксированной телекоммуникационной сети, мобильный, Интернет и компьютерных сетей.

10. вредоносное ПО это программа обладает способностью вызывать аномальные деятельности для всех или части информационной системы или сделать копию, модификацию кражи информации, хранящейся в системе сообщение.

11. Электронный адрес является адресом, используемым для передачи и приема информации по сети.

12. Личная информация информация, которая может быть четко определены личности, личную идентичность конкретного человека.

13. Предметом личной информации, что люди определяются из индивидуальных сведений.

14. Обращение с личной информацией является реализация одного или нескольких действий по сбору, редактировать, эксплуатации, хранения, предоставления, акцию, распространять личную информацию в Интернете с целью коммерческой, бизнес.

15. шифрования гражданской Пароль используется для защиты информации, не связанную с государственной тайной, служащий для гражданских операциях, экономики и торговли.

16. Сведения о безопасности продукта является оборудование, программное обеспечение, информационная безопасность.

17. Информация по технике безопасности услуг и информационных систем для организаций и частных лиц.

18. Электронные доказательства свидетельства хранится в электронном виде в компьютере или в аппаратных средствах.

19. Оружие технологической информации, меры и методы информации предполагается использовать в информации конфликтов.

20. Конфликт противоречивую информацию между двумя или несколькими организациями в стране и за рубежом в сети с целью причинения вреда информационных систем, программ и информационных ресурсов, а также существенные критические структуры и структуры друга; повреждая политической системы, экономики и общества; выполнить психологическую кампанию против отечественных и зарубежных организаций, о политической нестабильности, социальной; вынуждает организации принимать решения полезной для других организаций.

**Статья 5. Принципы пруденциального информации**

1. Организации и физические лица несут ответственность за обеспечение информацией о мерах предосторожности в Интернете. деятельность информационной безопасности организаций и частных лиц, чтобы способствовать развитию политической, экономической, социальной и культурной, в соответствии с положениями закона.

2. Организации и физические лица, участвующие в деятельности в Интернет не должны нарушать информационную безопасность организаций и отдельных лиц; Если индикаторы нарушения инцидентов информационной безопасности или небезопасных информации, организаций и физических лиц несут ответственность за своевременное уведомление соответствующим органам.

3. Организации и лица, ответственные за обеспечение информационной безопасности для управления информации и информационных систем под их юрисдикцией; под управлением, проверок, испытаний и выполнения требований по обеспечению информационной безопасности государственных учреждений, имеющих соответствующие полномочия.

4. Организации и физические лица, осуществляющие в области информационной безопасности должны координировать с учреждениями государственного управления и с компетентными организациями и частными лицами в обеспечении информацией о мерах предосторожности в Интернете.

Статья 6 государственной политики в области информационной безопасности

1. концентрировать ресурсы для укрепления пруденциального информации, особенно информационной безопасности для критических информационных систем на национальном уровне.

2. Приоритетность обучение, развитие людских ресурсов, информационной безопасности, разработанной для удовлетворения требованиям политики, экономики, общества и культуры, и способствовать обеспечению национальной обороны и безопасности.

3. приоритетов и поощрять исследования и разработки, поддержки экспорта, расширение рынка для продуктов, услуг, механизмы поддержки применяются технические меры, технологии информационной безопасности в стране изготовление, поставка; создать благоприятные условия для импорта продукции, современные технологии, которые не могут иметь производственные мощности, предложение.

4. Для обеспечения здоровой конкурентной среды в деятельности информационной безопасности, поощряет и создает благоприятные условия для организаций и частных лиц во всех экономических секторах во Вьетнаме и за рубежом, чтобы инвестировать, исследования и разработки продуктов и оказания услуг в области информационной безопасности.

**Статья 7. Международное сотрудничество в области информационной безопасности**

1. Принципы международного сотрудничества в области информационной безопасности:

а) уважать независимость, суверенитет и территориальную целостность стран, невмешательства в их внутренние дела, равенства и взаимной выгоды.

б) В соответствии с международным правом и положениями закона Вьетнама, в целях содействия экономическому развитию - экономическому развитию страны и обеспечения национальной безопасности.

2. Содержание международного сотрудничества по информационной безопасности:

а) укрепление международного сотрудничества в области научных исследований и применения науки, техники и технологии информационной безопасности;

б) Расширение сотрудничества, координации расследования и спасательные инцидентов, профилактике и Эксплуатация ВНИМАНИЕ нарушения безопасности на сетевой информации; профилактика и контроль киберпреступности, воспользовавшись сети для проведения террористических актов;

с) укрепление сотрудничества и обмена, используя информацию о происхождении, знаков и предотвратить атаки на сеть, предупреждения рисков и информацию, связанные с агентствами, иностранные организации с целью правоприменительной деятельности мер по обеспечению информацией о мерах предосторожности в сети;

d) провести международное сотрудничество по информационной безопасности.

**Статья 8. Запрещенные действия**

1. Предотвращение несанкционированного передачу информации в сети Интернет; несанкционированное вмешательство, вреда, удалять, изменять, ремонт, фальсификации информации в Интернете.

2. Воспрепятствование незаконно, влияющие на нормальное функционирование информационных систем или несанкционированного обструкции, влияет законный доступ к информационной системе пользователя.

3. Атакующий, отключить несанкционированный нейтрализовать меры безопасности для информационной системы; пользуясь лазейками и слабых информационных систем сознательно пройти меры контроля доступа, атак, угон несанкционированных информационных систем.

4. Распределить спам, текстовое сообщение спам, вредоносное, установить информационные системы подлог, мошенничество.

5. Воспользовавшись сети для распространения информации, мнение, осуществление актов, наносящих ущерб национальной безопасности и порядка, социального обеспечения, национальных интересов в Интернете; подрыв национальной блок единства; пропаганда агрессивной войны, терроризма; ненавижу, конфликты между странами, этнических, религиозных и ксенофобских.

6. Воспользовавшись сети для распространения незаконные документы, изображения, звуки или другую информацию, направленную на разжигание насилия, непристойности, развратного, преступности, социальных зол, суеверия, диверсионной декоративные традиции и обычаи народа; клеветническим, порнографических сообщений, нарушающих законные права и интересы организаций и частных лиц.

**Глава II**

**ИНФОРМАЦИЯ ПО БЕЗОПАСНОСТИ ОНЛАЙН**

**Раздел 1**

**Системы информационной безопасности**

**Статья 9 Классификация информационных систем**

1. Информационные системы классифицируются по степени важности, включают:

а) критические информационные системы на национальном уровне;

б) на системном уровне важная информация министерства и населенные пункты;

с) системы другой важной информацией.

2. Правительство подробно критерии, процедура классификации и обнародует список важных информационных систем на национальном уровне.

**Статья 10 информативность системы защиты**

1. принимать постановления по подтверждению информационной безопасности при проектировании, строительстве, управлении, эксплуатации, использования, обновления, отмены информационную систему.

2. Применить методы и приемы управления в соответствии со стандартами и техническими регламентами на информации о безопасности, чтобы предотвратить и контролировать риск, информационная безопасность устранения неполадок.

3. Проверка и контроль за соблюдением положений и оценки эффективности мер и методов управления применяются.

4. Управление рисками информационной безопасности.

**Статья 11. Мониторинг безопасности информационной системы**

Мониторинг безопасности информационной системы 1. Мониторинг является выявление нарушения информации о безопасности полетов или потенциально вызвать проблемы небезопасного информацию для информационных систем.

2. Информационная система мониторинга безопасности, включая:

а) Наблюдение за потоком информации, посылаемой, полученные по сети;

б) деятельность по мониторингу в компьютере, устройства обработки информации есть подключение к сети.

3. Организации, управляющие критически важных информационных систем несут ответственность за осуществление информационной информацию хранения мониторинга системы мониторинга безопасности и по мере необходимости.

4. Телекоммуникационные предприятия, предприятия, обеспечивающие информационных технологий услуг несут ответственность за полное осуществление требований государственных органов, уполномоченных когда предложено координировать информационную систему надзора за безопасностью.

5. Министерство информации и коммуникаций несет ответственность за управление мониторинга безопасности информационной системы организаций и предприятий по всей стране, контроль организации информационной безопасности в Интернете.

**Статья 12. Ответственность за обеспечение защиты важных информационных систем на национальном**

1. Ответственность управляющих организаций:

а) полностью осуществить информации о содержимом защита системы, предусмотренной в статье 10 настоящего Закона;

б) системы управления строительная техника, мониторинга безопасности информационной системы;

с) обеспечить наличие информационных систем;

d) периодически оценивать риск, риск информационной безопасности;

е) создать специализированные отделы по обеспечению безопасности информации и участие в инцидентах информационной безопасности спасательных сетевых как это предусмотрено;

е) Для реализации режима отчетности, как это предписано.

2. Обязанности учреждений государственного управления

а) Министерство информации и коммуникаций, в сотрудничестве с соответствующими министерствами оценка, информация инспекции безопасности, проверять и контролировать соблюдение положений закона о системе защиты сообщение.

б) Министерство обороны должно согласовывать с Министерством информации и связи и Министерство, соответствующих рейтинговых агентств, тестирования информационной безопасности, инспекции, проверки соблюдения законодательства об охране защита информационных систем для информационных систем, управляемых Министерством обороны.

с) Министерство общественной безопасности координируют с Министерством информационных технологий и связи и Министерством, соответствующие организации оценки, информация проверка безопасности, проверки и надзор за соблюдением положений Закона о защите защита информационных систем для информационных систем, управляемых Министерством общественной безопасности.

**Статья 13. Ответственность за обеспечение защиты важных информационных систем в соответствии с министерствами, филиалов и пунктов**

1. Ответственность управляющих организаций:

а) полностью осуществить информации о содержимом защита системы, предусмотренной в статье 10 настоящего Закона;

б) обеспечить наличие информационных систем;

в) проводить периодическую оценку риска, риск информационной безопасности;

д) организовать специализированный отдел, чтобы обеспечить безопасность информации и участие в инцидентах информационной безопасности спасательных сетевых как это предусмотрено;

е) Для реализации режима отчетности, как это предписано.

2. Министры, руководители учреждений на уровне министров, правительственных учреждений, председатель народных комитетов провинций и городов в прямом подчинении центрального правительства должны подробно обязанности и меры по защите критически важных информационных систем министерств, отраслей и местностей под руководством Министерства информации и коммуникаций.

**Раздел 2**

**Защита информации ОНЛАЙН**

**Статья 14 Классификация и защиты информации**

1. Организации и физические лица, владеющие информацией для проведения секретной информации от степени важности информации и объектов имеют доступ к соответствующим гарантиям.

2. Информация, подлежащая приоритет для защиты включают в себя:

а) Экстренное оповещение национальной обороны и безопасности;

б) Информация для экстренных случаев служит предотвращение стихийных бедствий, поиска и спасения, спасение, пожара или других стихийных бедствий;

в) информации о чрезвычайных ситуациях Аварийные службы и профилактики заболеваний;

d) прочие сведения, установленные законом о чрезвычайном положении.

3. Организации и физические лица устанавливают меры по управлению и методы для обеспечения того, чтобы информация всегда доступна для тех, кто прав доступа.

4. Организации и физические лица осуществлять защитные меры для каждого типа информации, чтобы обеспечить эту информацию не может быть раскрыта или использована незаконно, в том числе:

а) Принять меры по ограничению доступа для предотвращения объект не допускается;

б) регистрации информации журнала пользователь.

**Статья 15. Управление информацией передаются по сети**

1. Представление информации в сети необходимо убедиться, что:

а) Не подделка источником информации;

б) Соблюдение положений настоящего Закона и других положений соответствующих законов.

2. Организации и физические лица не допускается, чтобы отправить коммерческую информацию на электронный адрес получателя, если получатель не были согласованы, запросы, или получить информацию опроверг, если ввести предполагается получить информацию в соответствии с законом.

3. Предприятия, обеспечивающие телекоммуникационные услуги, поставщику услуг корпоративных приложений и корпоративных телекоммуникаций поставщика услуг внедрения информационных технологий несут ответственность за отправку информации:

а) соблюдать положения закона о сохранении информации, защиты личной информации, информации о клиентах;

б) Применение мер пресечения, лечения после получения уведомления из организаций и физических лиц по поводу информации домогательства, нарушение положений закона;

с) обеспечить технические условия, необходимые для профессиональных и государственных органов компетентными для выполнения задач государственного управления информацией о безопасности полетов при запросе.

4. Правительство предоставляет подробную информацию об управлении передаются по сети.

**Статья 16. Сетевые проблемы Спасательные**

1. Спасательная операция является проблемой сеть для обработки, решить эту проблему в результате чего небезопасный информации в Интернете.

2. Проблемы Сеть спасения сделаны в соответствии со следующими принципами:

а) Быстро, точно, своевременно и эффективно;

б) соблюдение положений законодательства по вопросам сетевых координации спасательных;

с) координация между организациями, местными предприятиями, на международном уровне.

3. Министерствам и ведомствам на уровне министров, правительственных учреждений, народных комитетов провинций и городов непосредственно под центральным правительством, телекоммуникационных компаний и организаций, управляющих критически важных информационных систем должны установить или назначить спасательные подразделения специализированных компьютерных краш согласовывать с Министерством информации и коммуникаций.

4. Министерство информации и коммуникаций несет ответственность за координацию спасательных инцидентами общенациональных сетей и содержащие подробную информацию о вопросах сетевых координации спасательных.

**Статья 17. Вариант аварийного реагирования на чрезвычайные ситуации небезопасно национальной информационной**

1. Emergency Response Team, чтобы обеспечить безопасность национальной информации работу спасателей в ситуациях стихийных бедствий или чрезвычайных ситуаций спасательной по просьбе правительства обеспечить безопасность Другая важная информация партии и Государственный.

2. Команда Оперативного Реагирования обеспечил национальную информацию, выполняет следующих принципов:

а) осуществление обеспечивает информацию реагированию в чрезвычайных ситуациях децентрализованных стран, отвечающих;

б) сделать пятно, быстро, строго конфиденциальна, в тесной координации;

с) Применение науки и техники, чтобы обеспечить эффективность и целесообразность.

3. Система аварийного спасения планирует обеспечить безопасность национальной информации включают:

а) План аварийного реагирования для обеспечения безопасности национальной информации;

б) план информации в чрезвычайных ситуациях для обеспечения безопасности министерств и ведомств на уровне министров, учреждений, подключенных к правительству, центральных органов партии;

в) План аварийного реагирования для обеспечения безопасности локальной информации;

d) План аварийного реагирования для обеспечения безопасности бизнеса телекоммуникаций.

4. Ответственность за обеспечение безопасности координирующую национальную информацию заинтересованных сторон:

а) Министерство информации и коммуникаций несет ответственность по руководству работой по координации реагирования на чрезвычайные ситуации, чтобы обеспечить информацию о безопасности по всей стране;

б) министерства, филиалы и населенные пункты отвечают за координацию и направление координации информации в чрезвычайных ситуациях для обеспечения безопасности при министерствах, филиалов и пунктов;

в) Телекоммуникационные предприятия придется осуществлять и координировать с Министерством информационных технологий и связи и министерства и населенных пунктов, связанных.

**Статья 18. Для обнаружения, предотвращения и обрабатывать вредоносного**

1. Организации, управляющие важных информационных систем техников развернутых операционных систем для обнаружения, предотвращения и оперативно решать вредоносных программ.

2. Организации, предоставляющие услуги электронной почты, передачи, хранения онлайн информационной системы должны обнаружить и отфильтровать вредоносные программы в информации, посылаемой, полученную или хранимую на своих информационных систем и несет ответственность за отчетность перед компетентным органом в соответствии с законом.

3. Предприятия, обеспечивающие услуги Интернет есть меры для предотвращения распространения вредоносных программ по требованию властей.

4. Министерство информации и коммуникаций должно, в сотрудничестве с Министерством обороны, Министерством общественной безопасности и Министерством, соответствующие отраслевые организации по выявлению, предупреждению и обрабатывать вредоносное ПО сети.

**Статья 19: Для обеспечения ресурсов безопасности Интернет**

1. Организации и физические лица, использующие должен ресурсы Интернет:

а) Немедленно уведомить Национальный регистратор доменных Вьетнам ".vn" или когда власти обнаружили их захвате доменного имени оборудования;

б) Применение мер и методов управления для предотвращения потери информации о безопасности полетов, полученной из доменного имени, ваш адрес в Интернете;

с) обеспечить адекватную информацию и координировать с учреждениями по управлению государственными компетентными при запросе;

d) Управление и обслуживание за собой право использовать свое доменное имя и нести ответственность за использование доменных имен в нарушение своего дела.

2. Регистрация доменного имени ".vn" доменное имя реестров международном во Вьетнаме осуществлять полный архив информации, относящейся к разрешению доменных имен для наших клиентов в минимальные сроки 05 лет и отчеты, координировать свои действия с органами государственного управления компетентными при запросе.

3. Регистрация доменных имен ".vn" в стране, чтобы использовать сервер доменных имен, используемые код страны доменное имя Вьетнама ".vn" для предоставления услуг разрешения имен доменов.

4. Организации, использующие интернет-адреса и номера автономных систем должны нести ответственность за внедрение и использование маршрутизации интернет-адресов, номера автономных систем, как это предписано Министерства информации и коммуникаций.

5. Организации и предприятия, обеспечивающие управление Интернет-услуги, чтобы принять меры по выявлению и предотвращению распространения информации, вредоносных программ, спама от интернет-адресов, находящихся под их управлением и предложения.

6. Агентство по управлению ресурсами несет ответственность за обеспечение безопасности информации в Интернет для разрешения доменных имен хост-системы и национальной инспекции и мониторинга информационной безопасности разрешения имен система регистрация доменных имен под своей области управления.

**Статья 20. Обязанности организаций и физических лиц в области защиты информации в сети**

1. Организации и физические лица, использующие онлайновые услуги, обязаны незамедлительно сообщать в предприятия или поставщика услуг специализированного отдела компьютерного сбоя спасения при обнаружении диверсий, неисправность техники компьютерное и сетевое.

2. Организации и физические лица, осуществляющие безопасности информации надлежит:

а) Не повредить информацию в сети и неблагоприятно влиять на работу политики, экономики, культуры и общества;

б) представить требования к управлению, инспекции, тестированию и внедрению государственных органов, уполномоченных по защите информации о безопасности в Интернете.

**Раздел 3**

**Предотвращения конфликтов информации в Интернете**

**Статья 21 Принципы информации по предотвращению конфликтов онлайн**

1. Сотрудничество для информации по предотвращению конфликтов в целях поддержания мира и национальной безопасности и способствовать политической стабильности, экономического и культурного - социальная.

2. Не будет построен или одобрен план имеет потенциал, чтобы увеличить риск противоречивую информацию там, напряженность в отношениях между странами или запуск сетевых атак.

Разрешение 3. Конфликт основную информацию в Интернете с помощью мер переговоров, посредничества, примирения, арбитража, суда или другими мирными средствами.

**Статья 22. Содержание информации по предотвращению конфликтов на сайте**

1. Во избежание повреждения информация, полученная из своих информационных систем; определить сотрудничество ресурсов, отталкиваются, исправлению кибератаки осуществляется через информационную систему внешней и внутренней учреждений.

2. Предотвращение действия отечественных организаций и иностранных целью саботажа полностью или частично целостности сети.

3. За исключением использования информационных технологий для вмешательства во внутренние дела зарубежных и отечественных институтов.

4. За исключением организацию или организаций по содействию осуществлению незаконного активности в сети местных и международных организаций; исключить клевету, организованной пропаганды унизительное, враждебную вмешиваться или вмешиваться во внутренние дела иностранных и отечественных учреждений.

**Статья 23. Права и обязанности информации по предотвращению конфликтов онлайн**

1. Организации и физические лица, участвующие в деятельности в Интернет с правами и обязанностями в полной мере реализовать содержание информации предотвращение конфликтов сети, указанной в статье 22 настоящего Закона.

2. Организации и частные лица имеют право и обязаны бороться с распространением ложной информации с целью вмешательства во внутренние дела отечественных и зарубежных организаций или поставить под угрозу национальную безопасность.

3. Организации и физические лица имеют право и обязаны предотвращать распространение оружия информации с целью противоречивой информации.

4. Правительство предоставляет подробные правила об информации, предотвращения конфликтов на сайте.

**Статья 24. Предотвращение террористической деятельности в Интернете**

1. Прекратите использование сети для террористических целей, в том числе:

а) предотвращать использование сетей в террористических целях; Интернет источники отключение характер терроризма;

б) Установить и расширить обмен информацией по сигналам, факторов, методов и с использованием Интернета в террористических целях, задачах и деятельности террористических организаций в сети, обмена знаниями Практический опыт и контроль Интернет источники, находить и контролировать содержание веб-сайта имеет природу терроризма;

в) Судебные органы должны исследовать, предотвращения и пресечения террористической деятельности в сети и ликвидации последствий терроризма; обрабатывать личную, организационную вдохновителя, организовывать и проводить террористических актов;

d) Судебная имеет право запрашивать экспертизы электронных доказательств для целей расследования, судебного процесса.

2. Правительство предоставляет подробные правила по предотвращению террористической деятельности в сети.

**Статья 25. Предотвращение нарушений законодательства деятельности онлайн**

1. Организации и частные лица не должны использоваться, манипулировать, распространяя информацию в Интернете источник для незаконных целей; незаконное распространение информации;

2. Организации и физические лица не должны нарушать конфиденциальность, и вредные для целостности или доступности информации;

3. Организации и физические лица, отвечающие за подготовку или стать соучастниками или разжигание уголовное дело и социальный вред к сети.

4. Компетентный орган разрешено использовать технические меры и операции для сбора, хранения и защиты информации для обработки расследовании правонарушений.

**Глава III**

**Защита персональной информации**

**Статья 26 Принципы защиты личной информации**

1. Защита личной информации соответствует положениям настоящего Закона и положений субъектов, связанных с юридическими.

2. Обработка персональных данных в целях обеспечения обороны и безопасности, общественного порядка и безопасность, а также служить индивидуальные потребности просто не входит в сферу регулирования настоящего Закона.

**Статья 27. Обязанности организаций обработки личной информации**

Если не указано иначе используются для расчета тарифов, выставление счетов, ваучер, предлагают продукты и услуги в соответствии с договором, в целях предотвращения актов уклонение договорное обязательство или закон предусматривает иное, обработку организации личная информация имеет следующие обязанности:

1. Разработка и гласности принципы, политику и правила по обращению и защите личной информации их организации.

2. Для сбора и использования личной информации:

а) Уведомление держателям личной информации, известной о форме, объеме и цели сбора и использования личной информации проконсультироваться предмет личной информации до сбора информации ; не установленные механизмы выбора по умолчанию согласен субъекта персональных данных;

б) использовать личную информацию для целей, указанных перед гусеничном только.

3. Не предоставлять долю, распространять личные данные собираются или контролируемый доступ к третьим лицам, кроме как с согласия субъекта индивидуальной информации.

4. После получения действительный предложения просьбой обновить, изменить, отменить вашу личную информацию владельцев личную информацию или прекратить действующий запрос личную информацию, предоставленную третьими лицами, :

а) Сделать запрос и доложить к предмету личной информации в кратчайшие сроки; или предоставлять личную информацию может любой доступ, обновление, изменение, отмена ваша личная информация хранится под своих подданных;

б) В случае временного нереализованных требований в соответствии с требованиями компетентных органов или из-за ремонтных затрат, понесенных или вызванного техническими факторами, других факторов, которые могут связываться принять надлежащие меры меры по защите личной информации о предмете и доложить к предмету личной информации там.

5. окончательно удалить персональную информацию, хранящуюся в конце использования или хранения уже истек поставлена ​​при сборе личной информации и уведомил держателей личной информации, чтобы знать, за исключением где закон предусматривает иное.

6. Нанесите практики управления, методы, необходимые для защиты личной информации, собранной их организации, хранения; соблюдение стандартов и технических регламентов в целях обеспечения безопасности информации. При наступлении или риска возникновения технических проблем, нужно применить корректирующие меры как можно скорее.

**Статья 28. Права и обязанности владельцев личной информации**

1. Требовать организации, предприятия обработки личной информации при условии вашей личной информации от организаций, предприятий обрабатывать личную информацию, которую он собирает, архивы.

2. Требовать организаций, предприятий обработки персональной информации обновлять, изменять, отменять вашу личную информацию от организаций и предприятий, которые занимаются сбор информации, хранение или прекратить предоставление Ваша личная информация третьим лицам в случае ранее согласились.

3. Соблюдение положений законодательства о предоставлении личной информации при использовании онлайн-сервисов.

**Статья 29. Обязанности органов государственной управления в защите личной информации в сети**

1. Организовать периодический осмотр, тестирование организации, предприятия обработки личной информации.

2. Настройка онлайн-канал связи для получения обратной связи от граждан по вопросам, связанным с защитой личной информации.

3. Выдача предписания, конкретные указания о защите личной информации в Интернете.

**Глава IV**

**ПАРОЛЬ И БЕЗОПАСНОСТЬ ИНФОРМАЦИЯ**

**Статья 30. Управление шифрованием**

1. Информация Совет правительства является национальная шифрования агентство, практики управления паролями в стране.

2. Гражданский криптографической методика государственной тайны. Государственный реализуют специализированное управление для научных исследований, производства, потребления и использования гражданских криптографических продуктов.

3. Сообщение, общественные выставки криптографической изделие не гражданские власти согласились национальной криптографии.

**Статья 31. Научно-исследовательские и изготовление гражданской криптографии**

1. Агентство по управлению назначенных национальных пароли организационную миссию научных исследований для гражданского шифрования. Организации должны быть указаны технические силы и оборудования, соответствующего задаче, умение применять теории и современных криптографических методов, алгоритмов шифрования должны быть гражданский интенсивность безопасность и энергия нападения большой мощности.

2. Национальная управляющая организация эксперт криптография обследование, результаты испытаний научных исследований в соответствии с гражданским криптографических стандартов инженерных и технических правил для гражданского пароль.

3. Агентство по управлению обозначены производственные национальные пароли организации гражданского криптографии. Если не указано конкретно, любая организация или частное лицо не должны быть изготовлены гражданские криптографические продукты. Места организация должна иметь технические силы, чтобы встретиться с производства гражданской криптографических продуктов и должны иметь оборудование, технология производства и контроля качества системы обеспечения качества гражданские криптографические продукты.

4. Тип продукта, тип продукции продукции агентства по управлению гражданской пароль должен быть одобрен криптографические страны, не производить гражданских криптографию выходит за рамки утвержденного. Продукты гражданской шифрования должны быть проведены осмотр, тестирование на соответствие.

**Статья 32. Потребление гражданского криптографии**

1. Органы управления национальной организации шифр лицензионные продукты потребляются гражданского пароль. Нелицензированные когда ни одна организация или частное лицо не имеет права потреблять продукты гражданского пароль.

2. Организация гражданского потребления криптографии зарегистрировать имя, адрес и код организации и частных лиц, непосредственно используя гражданские криптографические продукты, и намерены использовать шифрование для документирования гражданский трек.

3. Организации и физические лица не имеют права потреблять продукты неизвестного происхождения криптографии; импорт и экспорт шифрования продуктов, которые будут гражданские власти утвердили национальную криптографию.

**Статья 33. Использование гражданского криптографии**

1. Организации и физические лица допускаются только использовать пароль гражданские организации лицензированных предложить, не используется шифрование продукции, производимой для самоподготовки или криптографии продуктов неизвестного происхождения ,

2. Организации и физические лица, работающие за рубежом на территории Вьетнама использовали пароль устройства или методы шифрования должны быть зашифрованы властей ратификации; для дипломатических представительств и консульств за рубежом, за исключением.

3. Организации и физические лица не может присвоить гражданской продукции криптографии, которые они используют. Гражданские криптографические инцидентов продукта будут определено организацией ремонта, средства защиты. Отказаться, уничтожить гражданские криптографические продукты должны уведомить власти установили национальный шифровальный послужной список.

**Статья 34 Безопасность, охрана гражданских криптография**

1. Научно-исследовательские, производство реализации гражданской криптографии в окружающую среду должно соответствовать требованиям безопасности.

2. Потребление, транспортировка и хранение криптографических мер пожарной безопасности должны быть приняты.

3. Организации и сотрудников, работающих в научно-исследовательской, производства и потребления, а также гражданского криптографией гражданского использования, чтобы понять и осознать гражданские методы шифрования и выполнять обязанности безопасности ,

**Статья 35. Рассмотрение, оценка и мониторинг кодов**

1. Осмотр оценивали криптографического устройства с управление паролями от ведомств, ответственных за национальную криптографической оценки и признания, либо департаментом, блока или других лиц не допускается, чтобы продолжить оценка и криптоанализа.

2. Организации, управляющие уровни шифрования регулярно или нерегулярно проверяют, оценивают ситуацию в управлении, использовать шифрование и криптографические устройства для защиты секретных информационных и коммуникационных систем информации; проводить осмотр и оценку устройств системной информации паролем секретный характер, конфиденциальной минимум двух лет; в процессе оценки, если он обнаруживает скрытую информацию безопасности графику или правила прорыв на шифрование или неудовлетворительных стандартных методов шифрования, которые рассматриваться в соответствии с законом об управлении шифрования.

**Глава V**

**УПРАВЛЕНИЕ стандартов и технических регламентов**

**ИНФОРМАЦИЯ ПО БЕЗОПАСНОСТИ**

**Статья 36 стандартов, технических регламентов информационной безопасности**

1. Стандарты безопасности информационных систем, включая международные стандарты, национальные стандарты и основные стандарты для информационных систем, аппаратных средств, программного обеспечения, управление процессами, безопасной эксплуатации Информация, опубликованная, применяется во Вьетнаме в соответствии с законом о стандартах, технических регламентах и ​​качество продуктов и услуг.

2. Система технического регулирования и информации о безопасности полетов, в том числе национальных стандартов и правил на основе информационных систем, аппаратного и программного обеспечения, процессов управления, оперативной информацией безопасности строительство, выпущенный и применяется во Вьетнаме в соответствии с законом о стандартах, технических регламентах и ​​качество продуктов и услуг.

**Статья 37. Управление стандартов, технических регламентов и информации о безопасности полетов**

1. Сертификация соответствия является сертификация устройств, программного обеспечения, информационных систем, систем управления информационной безопасности в соответствии с техническими регламентами на информации о безопасности, предоставленной министерством информации и коммуникаций выпущенный и стандарты по информационной безопасности Министерства информации и коммуникаций обязательные правила.

2. Публикация соответствия является организация, в настоящее время опубликованы на совместимость аппаратных устройств, программного обеспечения, информационных систем, систем управления стандартов информационной безопасности, технический регламент на информация о технике безопасности.

3. Министерство науки и техники для оценки и публикации национальных стандартов по информационной безопасности, после консультаций с Министерством информационных технологий и связи.

4. Министерство информации и предоставляет коммуникаций:

а) принимать национальные технические регламенты на информации о безопасности полетов, требований к управлению каталог продукции информационной безопасности, правил оценки соответствия по информационной безопасности;

б) осуществлять продуктов контроля качества и услуг для обеспечения информационной безопасности;

с) координировать с Министерством обороны издан список продуктов, необходимых информации инспекция безопасности;

d) обеспечивать подробные условия и управленческой деятельности организаций по оценке соответствия, где информация о правил безопасности.

**Статья 38. Подтверждение и объявление процедуры и оценка, информация проверка безопасности**

1. Аккредитация, оценки соответствия, соответствие информации о безопасности полетов производится в следующих случаях:

а) Периодически для информационных систем, включенных в список критических информационных систем на национальном и каталог важная информация министерств и населенных пунктов на уровне системы;

б) Перед организаций и частных лиц, включенных в список оборудования, необходимого информации управления безопасностью продукции, распространенный на рынке для выполнения сертификатов соответствия или регулирование соответствия объявление и использовать знак соответствия;

с) служить деятельность Государственное управление в области информационной безопасности.

2. Аккредитация, оценки соответствия, соответствие информационной безопасности информационных систем в списке важнейших информационных систем, обслуживающих национальную и государственную управление реализации информационной безопасности текущие рейтинговые агентства по министром информации и коммуникаций назначен.

3. Взаимное признание результатов оценки соответствия, с информацией о правил безопасности между Вьетнамом и страны или территории, должны соответствовать международным договорам, которые Социалистическая Республика Вьетнам членство; между учреждениями оценки совместимости национальной территории делается по соглашению между сторонами.