права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов и т.п.

Литература

1. Грибунин В. Г., Жердин О. А., Мартынов А. П., Николаев Д. Б., Силаев А. Г., Фомченко В. М. Основы стеганографии // Под ред. д-ра техн. наук В. Г. Грибунина, г. Трехгорный, 2012.

2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с.

Методы и способы обеспечения информационной безопасности таможенных органовРеспублики Беларусь

Волосенкова Е. Д., Костюкевич В. Ю.
Научный руководитель: Ковалькова И. А.
Белорусский национальный технический университет

В современном мире развитие и применение информационных технологий занимает важное место в любой сфере деятельности. Понятие информации является чрезвычайно ёмким и широко распространённым, особенно в настоящее время, когда информатика, информационные технологии, компьютеры сопровождают человека чуть ли не с рождения.

Развиваются современные информационные технологии, а вместе с ними – преступления и нарушения в этой сфере. При этом негативные последствия от урона, нанесённого информационной безопасности отдельных субъектов, могут иметь международный масштаб. Национальное законодательство совершенствуется, чтобы предотвратить такие информационные угрозы. Новые нормы разрабатываются, а старые корректируются с учётом требований времени.

В свою очередь таможенная деятельность неразделимо связана с возникновениеми развитием информационных технологий. В настоящее время развитие информационных систем в таможенных службах государств, входящих в Таможенный союз, находится на высоком уровне. В Республике Беларусь внедрение информационных систем, информационных технологий закреплено Таможенным кодексом Республики Беларусь.

Информационные технологии приобрели глобальный трансграничный характер. Это способствует развитию всех сфер деятельности человека, общества и государства.

Одновременно с развитием технологий всё большее значение приобретает защита от пропорционально растущего числа киберугроз. Поэтому всё более актуальными и основополагающими становятся вопросы, связанные с обеспечением информационной безопасности.

Государственный таможенный комитет Республики Беларусь в целях совершенствования таможенного дела разрабатываети использует информационные системы и информационные технологии, в том числе основанные на электронных способах обмена информацией, а также средства их обеспечения на основе технических, нормативных и правовых актов.

Основополагающими нормативными актами, конкретизирующими процессы правового информирования в области таможенного законодательства ЕАЭС и национального законодательства о таможенном регулировании, являются:

- Таможенный кодекс Таможенного союза.
- Закон Республики Беларусь от 10.11.2008 №455-З «Об информации, информатизации и защите информации».
- Закон Республики Беларусь от 19.07.2010 №170-З «О государственных секретах» (далее – Закон о госсекретах).
- Закон Республики Беларусь от 10.01.2014 №129-З «О таможенном регулировании в Республике Беларусь».
- Указ Президента Республики Беларусь от 16.12.2002 №609 «О национальном правовом Интернет-портале Республики Беларусь и о внесении изменений и дополнения в Указ Президента Республики Беларусь от 30.10.1998 г. №524».
- Указ Президента Республики Беларусь от 06.02.2009 №65 «О совершенствовании работы государственных органов, иных государственных организаций со средствами массовой информации».

Государство прилагает много усилий, чтобы защищать наше кибернетическое пространство и информационные системы. Роль нормативной базы деятельности в сфере защиты информации играет закон Республики Беларусь от 10.11.2008 №455-З «Об информации, информатизации и защите информации». Он определяет порядок государственного регулирования и управления в сфере защиты информации, а также классификацию информации.

Существует общедоступная информация и ограниченная для распространения и(или) предоставления. Ограниченная для распространения информация включает информацию о частной жизни физического лица; информацию, составляющую коммерческую, профессиональную, банковскую и иную охраняемую законом тайну; служебную информацию ограниченного распространения. Служебная

тайна подразумевает меры и способы её защиты, так как входит в состав категорий «государственные секреты» и «нераскрытая информация».

Согласно ст.28 Закона о госсекретах меры защиты государственных секретов подразделяются на организационные, правовые, технические и иные. Выделяют также организационные меры(создание подразделений по защите государственных секретов) и технические (сертифицированные средства защиты).

В качестве основных способов защиты информационной безопасности выделяют:

- *Ограничение доступа к информации* (идентификация и аутентификация, контроль доступа на основе использования средств криптографии, контроль действий пользователя при санкционированном доступе, блокирование доступа к информации при определённых условиях, блокирование несанкционированного доступа, контроль функционирования средств ограничения доступа)
- *Ограничение распространения информации* (ограничение количества и дальности расположения удалённых объектов, предназначенных для взаимодействия; использование выделенных каналов связи, защищённых от несанкционированного доступа)
- *Обеспечение целостности самой информации* (резервное копирование информации, обеспечение целостности информации за счёт её избыточного кодирования, контроль целостности информации, блокирование модификаций информации при определённых условиях, «откат» модификаций информации до определённого уровня, дублирование процессов обработки информации)
- *Обеспечение целостности атрибутов информации* (резервное копирование информации с необходимыми атрибутами, контроль целостности атрибутов, «откат» модификаций атрибутов определённого уровня, блокирование модификация атрибутов при определённых условиях)
- *Обеспечение работоспособности среды обработки информации и каналов связи* (противодействие удалённым деструктивным воздействиям типа «отказ в обслуживании»; противодействие, заранее известным, внутренним логическим сбоям в системе; ограничение использования ресурсов системы допущенными пользователями и процессами; противодействие компьютерным вирусам и программным закладкам; улучшение качества электропитания; ограничение физического доступа к техническим средствам обработки; использование альтернативных каналов или сетей связи).

Определение полномочий пользователя в таможенной информационной системе осуществляет ответственный администратор

системы, а контроль деятельности(аудит) уполномоченного пользователя – администратор безопасности информационных систем.

Информационные системы и информационные технологии широко используются таможенными органами в целях обеспечения выполнения возложенных на них функций, в том числе обмена информацией с государственными органами, оказания государственных услуг участникам внешнеэкономической деятельности по предоставлению информации в электронном виде.На таможнях Республики Беларусь широко применяются следующие системные обеспечения: АС «Декларант», АС «Мониторинг-ВПТО», АС «СЭЗ», АРМ «ПТО», АРМ «БТС: Специалист», ПМ «Таможенный перевозчик». Следовательно, выполнение описанных способов и мер защиты информации позволит повысить уровень защищённости информации, циркулирующей в таможенных подразделениях до требуемого уровня безопасности.

Безопасное использование электронной почты(e-mail), выбор почтового клиента. Защита от спама

Маринич А. А.
Научный руководитель: КовальковаИ.А.
Белорусский национальный технический университет

Электронная почта (***E-mail***)– система, которая делает возможным передачу сообщений через глобальные и локальные сети компьютеров, в том числе через Интернет.

Электронная почта является важнейшим средством коммуникации, распределения информации, она решает одну из важнейших на настоящий момент задач – формирует единое информационное пространство, которая упрощает обмен информацией между людьми, подразделениями одной компании и различными организациями.Работа электронной почты, не зависит от разницы в часовых поясах, поэтому можно вести переписку по электронной почте с адресатом, который находится на другом конце света.

Для создания и получения сообщений электронной почты применяются специальные почтовые программы.*Почтовые клиенты* – это программы, с помощью которых пользователь может принимать и отправлять почту. Таких программ существует достаточно много, но принцип работы у всех одинаковый. Из множества программ электронной почты, работающих под управлением Windows, можно выделить:

- OutlookExpress;
- офисное приложение Microsoft Outlook;
- компоненты электронной почты в составе программ-браузеров;