**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИФНОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ**

**Кафедра радиоэлектронных средств**

**РЕФЕРАТ**

**На тему:**

**«Концепция национальной безопасности Республики Беларусь. Понятие «Безопасность государства». Принципы обеспечения безопасности государства»**

**МИНСК, 2008**

Обеспечение собственной безопасности — задача первостепенной важности для любой системы независимо от ее сложности и назначения будь то социальное образование (государство, межгосударственный блок), биологический организм или технологическая система (система обработки информации). Понятие «Безопасность» может рассматриваться отдельно для разных образований.

Одним из документов, дающим основные определения безопасности для образования «Государство», является Модельный Закон «О безопасности», который принят Межпарламентским Комитетом Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан в С.-Петербурге 15 октября 1999г. №9-9, приложение 1.А именно:

- Безопасность ГОСУДАРСТВА – состояние защищенности интересов страны от реальных и потенциальных угроз.

- ВОЕННАЯ безопасность – состояние защищенности государства от реальных и потенциальных угроз и посягательств военного характера на независимость и территориальную целостность страны.

- ЭКОЛОГИЧЕСКАЯ безопасность – состояние защищенности жизненно-важных интересов и прав личности, общества и государства от угроз, возникающих в результате антропогенных и иных воздействий на окружающую среду.

- ЭКОНОМИЧЕСКАЯ безопасность – состояние защищенности экономики государства, предприятия, благосостояния граждан от внутренних и внешних условий, процессов и факторов, ставящих под угрозу их устойчивое развитие и экономическую независимость.

- ИНФОРМАЦИОННАЯ безопасность – состояние защищенности информационных ресурсов государства, предприятия, а также прав личности и общества в информационной сфере.

- ОБЩЕСТВЕННАЯ безопасность - состояние защищенности жизни, здоровья и благополучия граждан, а также ценностей общества от возможных опасностей и угроз, способных нанести им ущерб.

- КОЛЛЕКТИВНАЯ безопасность (государств) – состояние защищенности государства от реальных и потенциальных угроз и посягательств военного характера на основе координации и обеспечения совместной деятельности государств-участников соответствующих международных договоров.

В законе также рассматривается:

- ОБЪЕКТ безопасности - права и свободы личности, материальные и духовные ценности общества, конституционный строй, независимость и территориальная целостность государства, экономическое состояние, права и свободы предприятия (организации),

- СУБЪЕКТ безопасности - как государство, осуществляющее свои полномочия через органы законодательной, исполнительной и судебной ветвей власти, граждане, предприятия (организации).

Все статьи закона являются основополагающими для построения безопасных отношений между государствами СНГ, подписавшими настоящий договор. При этом (ст.2) отмечается, что «Законодательство государства в области безопасности основывается на конституции государства и состоит из настоящего Закона и иных нормативных правовых актов государства»

В статье 3 Закона определяются семь основных принципов обеспечения безопасности государств:

соблюдение законности при осуществлении деятельности по обеспечению безопасности;

оперативное взаимное информирование и согласованность действий и сил обеспечения безопасности;

единство, взаимосвязь и сбалансированность всех видов безопасности;

приоритетность политических, экономических и информационных мер;

взаимная ответственность личности, общества и государства;

контроль реализации всей совокупности действий по защите безопасности;

соблюдение международных договоренностей в сфере безопасности.

**Экономическая безопасность государства. Формы собственности на материальные и информационные ресурсы**

#### Значительное внимание в Модельном законе «О безопасности» уделяется экономической (статья 18) безопасности.

В тексте статьи 18 закона отмечается, что экономическая безопасность обеспечивается:

А. Решениями и действиями государственных органов, организаций независимо от форм собственности, должностных лиц и граждан направленными на:

1) обеспечение экономической независимости государства;

2) недопущение экономической изоляции государства от мировой экономической системы;

3) сохранение и укрепление ресурсно-энергетической основы экономики страны;

4) обеспечение взаимовыгодного сотрудничества с отечественными и международными финансовыми институтами, приоритетность направления внутренних, внешних кредитных ресурсов и инвестиционных возможностей на восстановление и развитие отечественной экономики;

5) не превышение предельно допустимого уровня дефицита государственного бюджета и укрепление его доходной части;

6) недопущение увеличения внешнего долга против размеров, установленных законом о государственном бюджете;

Б. Государственным контролем за состоянием и использованием объектов экономики государства, находящихся в управлении или собственности иностранных организаций и организаций с иностранным участием.

В. Обязательным учетом требований по обеспечению безопасности при заключении контрактов по использованию стратегических ресурсов государства.

Г. Не допущением принятия каких бы то ни было решений и совершения действий, противоречащих интересам формирования и бесперебойного функционирования рыночного пространства государства, единой и самостоятельной финансовой системы государства, единых и самостоятельных коммуникационной и энергетической систем государства.

Д. Запрещением решений и действий, препятствующих притоку инвестиций в экономику государства, провоцирующих резкое падение курса национальной валюты, истощение золотовалютных активов государства, рост объемов государственного долга, а также способствующих неконтролируемому вывозу капитала за пределы страны.

**Информационная безопасность государства. Информационные войны. Интересы личности, общества и государства в информационной сфере.**

Задачи информационной безопасности отражаются в ст.22 Закона [1]. Здесь отмечается, что информационная безопасность должна обеспечиваться следующими основными действиями и мерами:

1. В государстве создается и укрепляется система защиты информации, в том числе государственных информационных ресурсов.

2. Обязанностью государственных органов, организаций, независимо от форм собственности, должностных лиц и граждан является принятие всех необходимых мер по недопущению:

- информационной зависимости государства;

- информационной экспансии и блокады со стороны других государств;

- информационной изоляции президента, парламента, правительства и сил обеспечения безопасности государства.

3. Не допускается принятие каких бы то ни было решений и совершение действий, противоречащих национальным интересам:

- формирования и бесперебойного функционирования информационного пространства государства;

- вхождения государства в мировую систему связи и информатики.

4. Запрещается:

- в течение пяти лет выезжать на постоянное местожительство за пределы государства лицам, имевшим в силу должностного положения доступ к сведениям, составляющим государственные секреты;

- распространять на территории государства печатную продукцию, теле- и радиопередачи зарубежных средств массовой информации, содержание которых подрывает безопасность государства;

- разглашать служебную и иную информацию, связанную с интересами государства;

- иностранным физическим и юридическим лицам, а также лицам без гражданства прямо и (или) косвенно владеть, пользоваться, распоряжаться и (или) управлять более 20 процентами пакета акций (долей, паев) юридического лица представителя средств массовой информации в государстве или осуществляющего деятельность в этой сфере.

 О серьезности данной проблемы можно судить по факту того, что лозунгом текущей эпохи всеми признается лозунг «Кто владеет информацией – тот владеет миром». Существование таких структур как АНБ (Американская национальная безопасность США) и ШПС (Штаб правительственной связи Англия) и им подобным является бесспорным доказательством большой заинтересованности в информации других государств и на удовлетворение потребности в ценных сведениях тратятся большие средства.

По данным из открытых источников информации в структуре «АНБ»: в 6 раз больше сотрудников, чем в ЦРУ. Занимается электронной разведкой 4120 мощных центров прослушивания, размещенных на многочисленных военных базах в Германии, Турции, Японии и др.странах. Они имеют возможность собирать и анализировать почти повсеместно радиограммы, телефонные переговоры. Могут перехватывать идущие по радиорелейным и спутниковым каналам связи, электронные сигналы любого типа, включая излучения систем сигнализации в квартирах и противоугонных устройств автомобилей.

Известная американская разведывательная система «Эшелон» перехватывает все, что существует в электромагнитном виде и обеспечивает тотальный контроль электронных средств коммуникаций. Перехват информации осуществляется из «международных выделенных линий», каналов мобильной и радиосвязи, радиоканалов на любых частотах, спутниковой связи, глобальных компьютерных сетей. Ключевым компонентом системы «Эшелон» являются словари-компьютеры, поддерживающие обширную базу данных по определенным мишеням (имена, номера телефонов, адреса, темы). Каждое перехваченное сообщение анализируется по критериям-мишеням и, при наличии совпадения «сырой» материал автоматически направляется для обработки (в словари). При запросе система выдает список сообщений, подходящих по каждому критерию отбора для рассмотрения, анализа и пересылки.

Создаваемая США система «Magic Lantern» позволяет тайно внедрять в компьютеры подозреваемых программы слежения, засылая их через Интернет при помощи вирусов. Слежка может производиться не только за перепиской, но и за любыми данными пользователя, включая перечень посещаемых им страниц, и словами, которые он вводит в поисковые машины.

У «ШПС» примерно такие же возможности.

Теперь многим ясно, что операции с информационными ресурсами могут превращать в «Металлолом» самую совершенную боевую технику и обеспечивать разгром противника, не пролив ни одной капли крови своих солдат.

В настоящее время во всех самостоятельных странах разрабатываются средства ведения информационной войны.

Понятие информационная война представляет собой комплексное воздействие на систему государственного и военного управления противостоящей стороны, ее политическое и военное руководство, которое уже в мирное время приводило бы к принятию благоприятных решений, а в ходе войны полностью парализовало бы всю систему военного управления противника .

Основная цель информационной войны - обеспечить национальную безопасность государства за счет:

* информационного воздействия на противостоящую сторону,
* защиты собственных информационных ресурсов и систем, разведывательно-аналитического обеспечения.

Основным направлением информационного противоборства является информационно-техническое. Объекты нападения: системы связи, радиоэлектронные средства.

 При этом используются программно-электронные методы воздействия на информационные ресурсы путем радиоэлектронного подавления каналов передачи информации, внедрения элементов «информационного оружия» и вирусов (логических бомб) в системы управления войсками и оружием противоборствующих государств с целью разрушения (уничтожения), искажения, съема (перехвата) информации в процессе ее сбора, обработки и хранения, передачи и распространения.

Агрессивность внешнего мира по отношению к ценной информации в государстве предопределяет применение ответных защитных мер. Необходимость таких мер понимается во всех государствах СНГ, в том числе и в Республике Беларусь.

 Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

 Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия.

 Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития информационной инфраструктуры, для реализации конституционных прав и свобод гражданина в области получения информации и пользования ею, для обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности государства, для политической, экономической и социальной стабильности государства.

**Влияние особенностей современного этапа на безопасность создания, хранения и использования материальных и информационных ресурсов**

Проблемы экономической и информационной безопасности актуальны и остры не только на уровне органов государственного управления стран. В среде крупных собственников процесс накопления экономических и информационных ценностей сопровождается усилением активных мероприятий по переделу сфер влияния. Возникают информационные войны с ведением направленных разведывательных мероприятий и применением специальных технических средств:

между финансово-промышленными группами (ФПГ);

между властью и ФПГ;

между властью и оппозицией, которую в свою очередь поддерживают ФПГ;

между разными сегментами власти, поддерживаемыми разными ФПГ;

между отдельными собственниками и т.д.

Совершенствуется промышленный шпионаж и хищение оригинальных решений. Имеет место информационное давление на потребителей и применение компромата относительно отдельных производителей

Современная действительность изобилует примерами разного рода хищений ценностей. Злоумышленники узнают пароли и коды, проникают в охраняемые зоны, в банковские, военные или другие информационные системы, похищают или изменяют имеющуюся там информацию..

В органах государственного управления во всех государствах имеются соответствующие образования, предназначенные для защиты экономических, информационных и других интересов государств и имеющие для этого необходимые полномочия.

Для защиты конкретной собственности от вредного воздействия угроз окружающего мира и обеспечения развития своего бизнеса на уровне отдельного предприятия или организации у собственника бизнеса любой формы собственности существует необходимость в непрерывном получении:

* информации о потенциально возможных угрозах ресурсам предприятия и способах защиты от них;
* информации о существующих средствах и методах защиты материальных и информационных ресурсов.

Для этого нужны соответствующие специалисты – АДМИНИСТРАТОРЫ безопасности – люди, профессионально владеющие способами и методами построения систем защиты ресурсов от угроз и знаниями о возможностях специальных технических средств защиты и особенностях их применения.

**ЛИТЕРАТУРА**

1. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С.Барсуков. – М., 2001 – 496 с.
2. Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикста, 2005. – 544 с.
3. Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.