**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ**

**Кафедра ЭТТ**

**РЕФЕРАТ**

**На тему:**

«Защита ценных ресурсов от угроз»

**МИНСК, 2008**

Основные направления защиты ценных ресурсов объекта от угроз

Очевидно, что для успешного противостояния атакам на ценные ресурсы необходимы профессиональные действия собственников ресурсов, различных государственных структур, структурных подразделений предприятий и отдельных исполнителей. Государство выступает в качестве гаранта в деле защиты от противоправных действий «нарушителей» в отношении собственности, каждый негосударственный собственник ресурсов принимает свои меры для защиты своей собственности в рамках действующего в государстве законодательства.

Кроме Собственников ресурсов и «Нарушителей» существуют Предприятия, организации и отдельные предприниматели, оказывающие услуги в области защиты собственности. Они так же могут быть государственной и негосударственной формы собственности и действуют в рамках установленных Законодательством Норм и Правил.

Исходя из необходимости получения максимальной эффективности мер по защите ценных ресурсов и учитывая, что «БЕЗОПАСНОСТЬ ОБЪЕКТА» - это состояние защищенности его ресурсов (персонала, материальных и информационных ценностей) от комплекса внутренних и внешних угроз, можно предположить, что совокупность мер по их защите от угроз должна включать меры:

* Правовой защиты;
* Организационной защиты - за счет организации режима безопасности, адекватного существующим угрозам;
* Защиты за счет применения технических, аппаратных, программных и программно-аппаратных средств (пожарной автоматики, охраны и антитеррора, спецсредств защиты информации и персонала, средств защиты технологических процессов и систем жизнедеятельности объекта);
* Страхования рисков.

Если изобразить указанную совокупность мер графически, то, с учетом имеющихся на текущий момент сведений о применяемых для защиты ценных ресурсов мерах, основные направления действий сил защиты можно представить следующим рисунком:

**Технические средства антитеррора**

## Система правовых и организационных мер

## Страхование рисков

ОСНОВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ РЕСУРСОВ ОТ УГРОЗ

Государственное регулирование деятельности по защите ресурсов от угроз.

Государственное регулирование деятельности в области защиты ресурсов объектов от угроз осуществляется через принятие соответствующих законодательных актов, утверждение нормативно-технических документов и контроль их выполнения, а также через стандартизацию, лицензирование и сертификацию производства товаров и услуг, подготовку кадров. Основополагающие вопросы по безопасности в РБ решают Президент и Совет безопасности. Существуют Министерства и Ведомства, как например, Министерство обороны, Министерство внутренних дел, Прокуратура и суды, КГБ, ГЦБИ, МЧС (Госатомнадзор, Госпожнадзор и др.) которые всей своей деятельностью направлены на обеспечение безопасности.

Основными госорганами, определяющими деятельность в интересующем нас направлении, являются: МЧС (Госпожнадзор), МВД (Департамент охраны), ГЦБИ (Государственный центр безопасности информации при Президенте Республики Беларусь), Министерство промышленности, Министерство связи, Министерство энергетики, Министерство труда, Учреждения науки и образования.

* **МЧС (Управление Госпожнадзора)** контролирует деятельность по созданию и поддержанию режима пожарной безопасности на предприятиях Республики. Основными структурными подразделениями, определяющими политику пожарной безопасности на предприятиях Республики, являются:
* Республиканское и областные Управления Госпожнадзора
* Городские и районные отделы – ПАСО – пожарные аварийно-спасательные отряды.
* Центр лицензирования и сертификации продукции и услуг.
* НИИ пожарной безопасности (с испытательными Лабораториями).
* Полигон – лучший в Европе.
* **Департамент охраны МВД Республики Беларусь** – определяет политику и тактику построения охраны, обеспечивает охрану объектов от несанкционированного доступа. С 2004 года при выработке основных направлений совершенствования существующих систем охраны, Департамент охраны МВД работает совместно с соответствующими структурными подразделениями НПО «Агат».

Департамент охраны включает в себя Республиканское, областные управления, городские отделы и районные отделения; органы по сертификации продукции и услуг с испытательными лабораториями; учебный центр. В Минском городском и областных управлениях Департамента имеются отделы лицензирования деятельности по проектированию, монтажу, техническому обслуживанию средств и систем охраны.

* **В области защиты информации систему органов защиты информации составляют:**

- Государственный центр безопасности информации (ГЦБИ) при Президенте Республики Беларусь;

- Территориальные центры технической защиты информации;

- Унитарное предприятие «НИИ технической защиты информации»;

- Подразделения по технической защите информации Министерств, органов местного управления и самоуправления, предприятий;

- Орган по сертификации по требованиям защищенности информации и сертификационные испытательные центры (лаборатории);

- Предприятия по оказанию услуг в области технической защиты информации, осуществляющие свою деятельность на основании лицензий, полученных в установленном порядке;

- Учебные заведения по подготовке и повышению квалификации специалистов по технической защите информации.

- Журналы «Управление защитой информации» и «Защита информации» ГЦБИ при Президенте РБ контролирует деятельность по защите информации;

**Лицензирование деятельности и сертификация производства, продукции и услуг.**

**Лицензирование –** это государственное регулирование состава участников производства товаров и услуг в определенной области деятельности.

**Сертификация** – это действия независимой стороны, доказывающее, что продукция, процесс или услуга соответствует конкретному стандарту или другому нормативному документу. Сертификация введена на основании действующего в РБ законодательства с 1 января 1994 года Постановлением СМ РБ № 635 от 22.09.93г. «О введении обязательной сертификации товаров народного потребления, работ и услуг» и является обязательной.

***Лицензирование.***

Порядок лицензирования деятельности по производству товаров и услуг (по определенному и утвержденному Постановлением СМ РБ перечню) в области противопожарной защиты и охраны осуществляется структурами МЧС (Госпожнадзор), МВД (Департамент охраны) и ГЦБИ при Президенте РБ на основании соответствующих положений о лицензировании.

Для получения лицензии на право проектирования, монтажа и обслуживания средств охраны требуется представить следующие документы и осуществить следующие действия:

1. Нотариально заверенная копия свидетельства о государственной регистрации.
2. Нотариально заверенная копия Устава Предприятия.
3. Сведения об учетном номере налогоплательщика.
4. Копия платежного поручения на оплату за выдачу лицензии.
5. Список штатных специалистов, выполняющих работы по заявляемым видам деятельности.
6. Перечень нормативных документов, используемых при осуществлении лицензируемой деятельности.
7. Сведения о технической базе предприятия для осуществления заявленных видов деятельности.
8. План подготовки и переподготовки специалистов, выполняющих лицензируемые виды работ или договор о подготовке специалистов в учреждении, имеющем право на образовательную деятельность в этой области деятельности.
9. Копия приказов и других документов предприятия о создании подразделения для осуществления лицензируемого вида деятельности.
10. Положение о подразделении, согласованного с объединением «Охрана».
11. Копия руководства по качеству для подразделения, осуществляющего заявляемый вид деятельности.
12. Копии ранее выданных лицензий:

В области защиты информации для получения лицензии также необходимо подтвердить документами свою готовность к выполнению лицензируемых видов работ. При этом лицензия, в соответствии с Положением может выдаваться на:

* разработку, производство, реализацию, монтаж, наладку, сервисное обслуживание технических и программных средств защиты информации и контроля ее защищенности, специальных материалов и оборудования для производства этих средств, программно-аппаратных средств защиты от несанкционированного доступа, в том числе с применением средств криптографии;
* проведение специальных исследований технических средств от утечки информации, работ по выявлению устройств съема информации и контроля ее защищенности.

ГЦБИ при Президенте Республики Беларусь, при получении комплекта документов от Заявителя создает комиссию из компетентных специалистов, проводит всесторонний анализ возможностей Заявителя, (по уровню квалификации специалистов, наличию оборудования, производственных помещений и условий, нормативно-методической документации и т.п.) указанному в заявке виду деятельности.

При оценке уровня квалификации специалистов принимается во внимание не только (и не столько) уровень базового образования, но и практическая работа в той сфере деятельности, на которую испрашивается лицензия. В ходе экспертизы проверяются представляемое оборудование (его возможности, характеристики), наличие помещений, полнота соответствующей нормативно-методической и технической документации. В необходимых случаях анализируется и качество продукции, которая предлагается тем или иным субъектом хозяйствования. Приоритет здесь, безусловно, имеют те организации (юридические лица), которые обладают собственными производственными мощностями, разработками и подготовленными профессиональными кадрами. Для исследования разработанных технических, программно-аппаратных или программных средств защиты информации лицензируемого вида деятельности заявитель представляет их опытные или рабочие образцы с комплектом технической документации, исходные тексты программ, а при реализации - образец технического средства с комплектом эксплуатационной документации.

Отказ в выдаче лицензии производится в случаях:

• отсутствия необходимых условий для проведения работ по заявленному виду деятельности;

• несоответствия установленным требованиям профессиональной подготовки лиц, представленных в заявке для проведения лицензируемой деятельности;

• недостоверности сведений, указанных в представленных для получения лицензии документах;

• если заявитель в установленном законом порядке признан виновным в недобросовестной конкуренции в лицензируемой области деятельности.

Организации-заявители, получившие лицензии, обязаны осуществлять свою деятельность в строгом соответствии с требованиями нормативных документов по защите информации, обеспечить тайну переписки, телефонных переговоров, документальных и иных сообщений юридических и физических лиц, пользующихся их услугами.

ГЦБИ ведет контроль за выполнением субъектами хозяйствования требований Временного положения. В случае нарушения правил осуществления лицензируемой деятельности действие лицензии может быть приостановлено, а при повторном или грубом нарушении она может быть аннулирована Государственным центром безопасности информации.

***Сертификация.***

В Республике Беларусь наблюдается тенденция увеличения количества производителей и поставщиков средств защиты, заполняющих рынок изделиями, качество и защитные свойства которых в лучшем случае неизвестны. Эта тенденция привела к повышению интереса к сертификации как механизму, подтверждающему некоторый уровень качества систем и средств защиты информации.

Сертификат как документ, отражающий мнение группы экспертов о соответствии сертифицируемого продукта некоторым требованиям, сам по себе не дает достаточных гарантий, но снимает ответственность с покупателя за приобретение некачественной продукции.

ГЦБИ, МЧС и Департамент охраны ежегодно составляют перечни средств разрешенных к использованию в системах защиты ресурсов от различных угроз. С апреля 2006 года МЧС запретил применение технических средств ППА на территории РБ без сертификата РБ.

По линии ГЦБИ (СТБ 5.1.04-96, РБ) сертификации подлежит:

1. продукция, предназначенная для реализации потребителю, представляющая собой готовое, законченное изделие единичного, массового или серийного производства, а в отдельных случаях - и опытный образец.

2. продукция, которая используется в качестве средства обработки, хранения, накопления, передачи защищаемой информации или представляет собой специальное устройство или программу для защиты такой информации.

3. продукция иностранных информационных технологий, которая применяется для обработки защищаемой информации.

**Перечень классов средств обработки, хранения, передачи и защиты информации, подлежащих сертификации представлен в таблице.**

| **№№**  **пп** | **Класс**  **Средств** | **Вид продукции, подлежащей сертификации** |
| --- | --- | --- |
| 1 | Аппаратные (технические) средства защиты информации | * Средства акустической и вибрационной защиты разговорной речи (генераторы шума). * Средства нейтрализации побочных электромагнитных излучений и наводок (генераторы шума, фильтры и т.п.). * Средства защиты информации, передаваемой по каналам радиосвязи (скремблеры и т.п.). * Средства обнаружения и нейтрализации подслушивающих и звукозаписывающих устройств. * Средства защиты телефонной сети связи (скремблеры, фильтры и т.п.). * Средства защиты от прослушивания речевой информации через ТА в режиме ожидания вызова |
| 2 | Программные средства защиты информации | * Программы, обеспечивающие разграничение доступа к информации по мандатному, дискретному или многоуровневому принципу (матрица и диспетчер доступа, электронный журнал регистрации доступа пользователей к информации, метки конфиденциальности и т.д.). * Программные средства разграничения межсетевого доступа. * Программы идентификации и аутентификации терминалов и пользователей по различным признакам (пароль, дополнительное кодовое слово, биометрические данные и т.п.), в том числе программы повышения достоверности идентификации (аутентификации). * Программы проверки функционирования системы защиты информации от НСД. * Программы контроля целостности средств защиты. * Антивирусные программы. * Программы защиты операционных систем ЭВМ (модульная программная интерпретация и т.п.) * Программы контроля целостности общесистемного и прикладного программного обеспечения. * Программы, сигнализирующие о нарушении правил использования ресурсов. * Программы уничтожения остаточной информации в запоминающих устройствах (оперативная память, видеопамять и т.п.) после использования. * Программы контроля файловой структуры на внешних запоминающих устройствах и средствах восстановления. * Программы имитации работы системы или ее блокировки при обнаружении фактов НСД. * Программы определения фактов НСД и сигнализации (передачи сообщений) об их обнаружении. * Программы обнаружения и локализации программных закладок. |
| 3 | Защищенные программные средства обработки информации | * Пакеты прикладных программ автоматизированных рабочих мест. * Программы испытаний вычислительных средств на побочные излучения и наводки. * Базы данных вычислительных сетей. * Программные средства автоматизированных систем управления. * Программные средства идентификации изготовителя программного (информационного) продукта, включая средства идентификации авторского права. |
| 4 | Программные средства общего применения | * Операционные системы. * Системы управления базами данных. * Языки программирования. * Средства разработки программного обеспечения. * Редакторы текстовые и графические. |
| 5 | Программно-аппаратные средства защиты информации от НСД | * Устройства прерывания программы пользователя при нарушении им правил доступа. * Устройства стирания данных. * Устройства выдачи сигнала тревоги при попытке НСД к информации. * Устройства локализации электронных закладок. * Устройства локализации действий программных и программно-аппаратных закладок. * Средства разграничения доступа к информации, встроенные в информационные технологии. * Средства разграничения межсетевого доступа. * Сетеобразующие компоненты. * Средства телекоммуникаций. * Устройства идентификации. * Средства обнаружения нарушителя или нарушающего воздействия. |
| 6 | Защищенные технические средства обработки и хранения информации | * Средства вычислительной техники, в том числе:   - электронные вычислительные машины (ЭВМ) различного уровня и назначения;  - принтеры ЭВМ;  - клавиатура ЭВМ;  - периферийные устройства ЭВМ;  - электронные блоки ЭВМ;  - видеомониторы ЭВМ.  - запоминающие устройства ЭВМ.   * Средства звукозаписи, звукоусиления и звуковоспроизведения. * Электронные средства изготовления и тиражирования документов. |
| 7 | Технические средства передачи информации | * Средства радио- и кабельной связи, радиовещания, включая спутниковые системы и волоконно-оптические линии связи и их компоненты. * Переговорные устройства. |
| 8 | Средства телевидения | * Телевизионные системы охраны и наблюдения. * Системы и аппаратура видеозаписи и воспроизведения. |
| 9 | Технические средства контроля эффективности защиты информации | * Приборы для анализа сигналов в различных частотных диапазонах. * Измерители мощности, уровня шума и т.д. * Индикаторы электромагнитных излучений. |
| 10 | Физические средства защиты информации | * Различного рода замки. * Сейфы и т п. |
| 11 | Средства криптографической защиты информации | * Аппаратные, программные и программно-аппаратные средства, реализующие криптографические алгоритмы преобразования информации. |
| 12 | Общетехнические средства | * Электрические датчики разных типов. * Устройства преобразования сигналов (модемы). |
| 13 | Специальные материалы | * Специальные материалы (краски, ткани, твердые пластины и т.п.) с экранирующими или поглощающими свойствами. |

**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.
4. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия –Телеком, 2000. - 452 с., ил
5. Компьютерная преступность и информационная безопасность / А.П.Леонов [и др.]; под общ. Ред. А.П.Леонова. – Минск: АРИЛ, 2000. – 552 с.