БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра информатики

Факультет НиДО

Специальность ИиТП

Контрольная работа № 1

по дисциплине «Основы защиты информации»

Выполнил студент: Дегтярев А.А.

группа 393551

Зачетная книжка № 902021-26

Минск 2016

**Указ Президента РБ “Вопросы ГЦБИ при Президенте РБ”.   
Концепция национальной безопасности РБ.**

В указе президента №639 от 28.11.2000 «Вопросы ГЦБИ при Президенте РБ» Устанавливались задачи и функции ГЦБИ. Если обобщить изложенное в документе, то ГЦБИ занимается обеспечением и контролем защиты информации всего государственного аппарата, а также иных организаций.

В настоящее время ГЦБИ не существует, он был преобразован 21 апреля 2008 года очередным указом Президента Республики Беларусь в Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ).

Сейчас ОАЦ – это государственный орган, осуществляющий регулирование деятельности по обеспечению зашиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и преднамеренных воздействий.

Из информации, представленной на сайте ОАЦ, свою историю эта организация ведет с 18 декабря 1973 года. Тогда был создана Государственная техническая комиссия СССР, задачей которой была зашита информации в военно-промышленном комплексе. В июле 1979 г. образована Минская региональная инспекция комплексного технического контроля, на базе которой в августе 1989 г. был создан Минский специальный центр Гостехкомиссии СССР.

12 января 1993 г. решением Правительства страны на базе бывшего Минского специального центра Гостехкомиссии СССР был создан Государственный центр безопасности информации (ГЦБИ) при Министерстве обороны Республики Беларусь.

Задача ГЦБИ заключалась в обеспечении защиты охраняемых сведений инженерно-техническими методами в органах государственного управления, на предприятиях, в учреждениях и организациях в ходе исследований, разработок, производства и эксплуатации вооружения, военной техники, автоматизированных систем управления, электронных вычислительных машин, используемых в интересах обороны и безопасности страны.

В октябре 1994 г. Указом Президента Республики Беларусь ГЦБИ при Министерстве обороны Республики Беларусь был преобразован в ГЦБИ при Совете Безопасности Республики Беларусь.

В ноябре 2000 г. Указом Президента Республики Беларусь ГЦБИ при Совете Безопасности Республики Беларусь был преобразован в ГЦБИ при Президенте Республики Беларусь.

Сейчас ОАЦ является независимым регулятором в сфере информационно-коммуникационных технологий. Также является регистратором РУП «Национальный центр обмена трафиком» (НЦОТ), которое имеет право на пропуск международного интернет-трафика, курирует единую республиканскую сеть передачи данных, и вроде как призвано объединить все гражданские сети передачи данных. Также в подчинении находятся Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» [www.niitzi.by](http://www.niitzi.by/), и Республиканское унитарное преприятие «Национальный центр электронных услуг» - [www.nces.by](http://www.nces.by/)

**Концепция национальной безопасности Республики Беларусь** была утверждена указом Президента Республики Беларусь №575 от 9 ноября 2010 года. Это довольно объемный документ и в рамках данного предмета стоит, естественно, обсудить тему Информационной безопасности.

**Информационная безопасность** в данном документе определена как - *состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;*

**Указывается возросшая важность обеспечения информационной безопасности:**   
 *Информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов на экономическую, политическую и социальную ситуацию. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Происходит эволюция информационного противоборства как новой самостоятельной стратегической формы глобальной конкуренции. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб национальным интересам.*

**Национальные интересы в информационно сфере:**

*реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;*

*формирование и поступательное развитие информационного общества;*

*равноправное участие Республики Беларусь в мировых информационных отношениях;*

*преобразование информационной индустрии в экспортно-ориентированный сектор экономики;*

*эффективное информационное обеспечение государственной политики;*

*обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.*

**Внутренними источниками угроз национальной безопасности в информационно сфере являются:**

*распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;*

*зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;*

*несоответствие качества национального контента мировому уровню;*

*недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;*

*рост преступности с использованием информационно-коммуникационных технологий;*

*недостаточная эффективность информационного обеспечения государственной политики;*

*несовершенство системы обеспечения безопасности критически важных объектов информатизации.*

**Внешними источниками угроз национальной безопасности в информационно сфере являются:**

*открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;*

*доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;*

*информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;*

*нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;*

*развитие технологий манипулирования информацией;*

*препятствование распространению национального контента Республики Беларусь за рубежом;*

*широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;*

*попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.*

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

     **Приоритетным направлением является** совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

     **Нейтрализации ряда внутренних источников угроз национальной безопасности способствует** информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

     Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

**Электромагнитные каналы утечки информации.**

Электронные и радиоэлектронные средства, особенно средства электросвязи, обладают основным электромагнитным излучением, специально вырабатываемым для передачи информации, и нежелательными излучениями, образующимися по тем или иным причинам. В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения, возникающие при работе технических средств:

* возникающие вследствие протекания по элементам средств передачи информации и их соединительным линиям переменного электрического тока;
* побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав средств передачи информации;
* побочные электромагнитные излучения, возникающие вследствиепаразитной генерации в их элементах.

**Побочные электромагнитные излучения.** В некоторых ТСПИ (например, системах звукоусиления) носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону изменения информационного речевого сигнала. При протекании электрического тока по токоведущим элементам ТСПИ и их соединительным линиям в окружающем их пространстве возникает переменное электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

**Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ.**

В состав ТСПИ могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания, элементы радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах высокочастотных генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов, которые излучаются в окружающее пространство.

**Побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ**.

Паразитная генерация в элементах ТСПИ, в том числе, самовозбуждение усилителей низкой частоты (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.), возможна за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота автогенерации (самовозбуждения) лежит в пределах рабочих частот нелинейных элементов усилителей (например, полупроводниковых приборов, электровакуумных ламп и т.п.). Сигнал на частотах самовозбуждения, как правило, оказывается модулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе усилителя в нелинейный режим работы, т.е. в режим перегрузки.

Побочные электромагнитные излучения возникают при  
- выводе информации на экран монитора;  
- вводе данных с клавиатуры;  
- записи информации на накопители на магнитных носителях;  
- чтении информации с накопителей на магнитных носителях;  
- передаче данных в каналы связи;  
- выводе данных на внешние печатные устройства

- запись данных со сканера

Для перехвата побочных электромагнитных излучений могут использоваться как обычные средства радио-, радиотехнической разведки, так и специальные средства разведки.

Используя характеристики приемного устройства, можно рассчитать значение напряженности электромагнитного поля в точке размещения средства разведки, при котором отношение “информационный сигнал/помеха” на входе приемного устройства будет равно некоторому условному значению, при котором возможно или обнаружение средством разведки информационных сигналов с требуемой вероятностью, или измерение их параметров с допустимыми ошибками, а значит – и выделение полезной информации.

Пространство вокруг источника, в пределах которого напряженность электромагнитного поля превышает установленное значение, называется **зоной 2**, в пределах которой возможен перехват средством разведки побочных электромагнитных излучений ТСПИ с требуемым качеством

Наряду с пассивными способами перехвата информации, обрабатываемой ТСПИ, и рассмотренными выше, возможно использование и активных способов, в частности, способа ***“высокочастотного облучения”*** При взаимодействии облучающего электромагнитного поля с элементами источника происходит его переизлучение. На нелинейных элементах ТСПИ происходит модуляция вторичного излучения информационным сигналом. Переизлученный сигнал принимается приемным устройством средства разведки и детектируется.

Для перехвата информации, также возможно использование электронных устройств перехвата информации, скрытно внедряемых в технические средства и системы. Они представляют собой миниатюрные передатчики, излучение задающих генераторов которых модулируется информационным сигналом. Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается в специальное запоминающее устройство, а уже затем по команде управления передается по радиоканалу.

Защита от утечки информации за счет побочных электромагнитных излучений самого различного характера предполагает:

— размещение источников и средств на максимально возможном удалении от границы охраняемой (контролируемой) зоны;

— экранирование зданий, помещений, средств кабельных коммуникаций;

— использование локальных систем, не имеющих выхода за пределы охраняемой территории (в том числе систем вторичной часофикации, радиофикации, телефонных систем внутреннего пользования, диспетчерских систем, систем энергоснабжения и др.);

— развязку по цепям питания и заземления, размещенных в границах охраняемой зоны;

— использование подавляющих фильтров в информационных цепях, цепях питания и заземления.

Для обнаружения и измерения основных характеристик ПЭМИ используются:

— измерительные приемники;

— селективные вольтметры;

— анализаторы спектра;

— измерители мощности и другие специальные устройства.

**Практическая часть**

**Контрольное задание.** Анализ угроз информационной безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование угрозы | Источник | Метод парирования угрозы |
| Компьютерный класс | | | |
| 1. | Несанкционированный доступ в сети | Компьютер в сети, внешняя атака при подключении к глобальной сети, | Локализация сети, поиск и уничтожение вредоносного кода, строгое администрирование сети и ограничение доступа |
| 2. | Нарушение работы сети | Повреждение сетевого оборудования из-за перепадов напряжения, использование поврежденного сетевого оборудования, сетевое оборудование с вредоносным кодом | Замена поврежденного оборудования, поиск и уничтожение вредоносного кода, использование заземления и сетевых фильтров |
| 3. | Нарушение работы компьютеров в сети | Повреждение из-за перепадов напряжения, уничтожение данных на диске вредоносным кодом | использование заземления и сетевых фильтров, |
| **Банковская карточка** | | | |
| 1. | Размагничивание (делает карту непригодной для использования) | Сильное электромагнитное излучение выводящее карту из строя (размагничивание ленты) | Технически экранирование карты от сильного э/м излучения |
| 2. | Утечка информации о карте(угроза конфиденциальности) (имя владельца, CVV код, номер карты, информация о банке, тип карты и прочее) | Сама карта, на которой данная информация нанесена и злоумышленник | Сокрытие данной информации. Технические ограничения на возможность использование данной информации |
| 3. | Несанкционированное использование привязанного банковского счета с помощью карты | Злоумышленник | Дополнительная верификация пользователя карты при расчетах |
| **Банкомат** | | | |
| 1. | Несанкционированный сбор данных, кража данных карточек | Скиммер или иные технические средства вблизи банкомата, | Какая-то система идентифицирующая вмешательство в устройство банкомата |
| 2. | Несанкционированный доступ к процессу передачи данных к банку | Сеть передачи данных, злоумышленник | Защита сети, экранирование, дополнительные способы верификации данных карты, шифрование данных |
| 3. | Нарушение работы | Физическое взаимодействие, Электромагнитное, иной способ связанный с несанкционированным доступом,  Нарушение связи с банком | Сделать его крепким, охраняемым, использовать беспроводную связь(что не всегда безопасно), |

**Источники**  
<http://oac.gov.by/info/history.html>

<http://www.nestor.minsk.by/sr/2003/06/30617.html>  
http://www.bnti.ru/showart.asp?aid=644&lvl=04.02.  
Текст указа Президента №575 от 9 ноября 2010