Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Лабораторная работа №1**

**Тема «Концепция национальной безопасности Республики Беларусь»**

Выполнила:

Студентка 2 курса 7 группы ФИТ

Курносенко Софья Андреевна

Проверил:

Барковский Евгений Валерьевич

**Цель**: Изучить концепцию национальной безопасности РБ.

**Задание для выполнения.**

Ответить на следующие вопросы:

1. **Что такое информационная безопасность?**

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

1. **Перечислить основные национальные интересы в информационной сфере?**

Основными национальными интересами в информационной сфере являются:

▪ 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.

1. **Основные угрозы национальной безопасности, связанные с ИТ-сферой?**

Основными потенциальными либо реально существующими угрозами национальной безопасности в информационной сфере являются:

▪ деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

▪ нарушение функционирования критически важных объектов информатизации;

▪ недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

▪ снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;

▪ утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности.

1. **Назвать основные внутренние и внешние источники угроз национальной безопасности в информационной сфере?**

В информационной сфере *внутренними* источниками угроз национальной безопасности 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.

В информационной сфере *внешними* источниками угроз национальной безопасности 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.

1. **Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере?**

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.

**Обзор международных стандартов информационной безопасности**

**Вопросы для самоконтроля:**

**1. Охарактеризуйте основные положения Оранжевой книги.**

Критерии оценки безопасности компьютерных систем" (Trusted Computer System Evaluation Criteria -TCSEC), получившие неформальное название "Оранжевая книга", были разработаны и опубликованы Министерством обороны США в 1983 г. с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному программному и информационному обеспечению компьютерных систем, и выработки методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах, в основном, военного назначения.

В "Оранжевой книге" предложены три категории требований безопасности: политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних – на качество средств защиты. Рассмотрим эти требования подробнее.

**Политика безопасности**

*Требование 1.* Политика безопасности. Система должна поддерживать точно определенную политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом. Там, где это необходимо, должна использоваться политика мандатного управления доступом, позволяющая эффективно реализовать разграничение доступа к информации различного уровня конфиденциальности.

*Требование 2.* Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Для реализации мандатного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и режимы доступа к этому объекту.

**Аудит**

*Требование 3.* Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

*Требование 4.* Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе (т.е. должен существовать объект компьютерной системы, потоки от которого и к которому доступны только субъекту администрирования). Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

**Гарантии (корректность)**

*Требование 5.* Контроль корректности функционирования средств защиты. Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

*Требование 6.* Непрерывность защиты. Все средства защиты (в том числе и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одной из ключевых аксиом, используемых для формального доказательства безопасности системы.

**2. Каковы основные положения Европейских критериев безопасности информационных технологий?**

"Европейские Критерии" рассматривают следующие составляющие информационной безопасности:

- конфиденциальность – защита от несанкционированного получения информации;

- целостность – защита от несанкционированного изменения информации;

- доступность – защита от несанкционированного удержания информации и ресурсов.

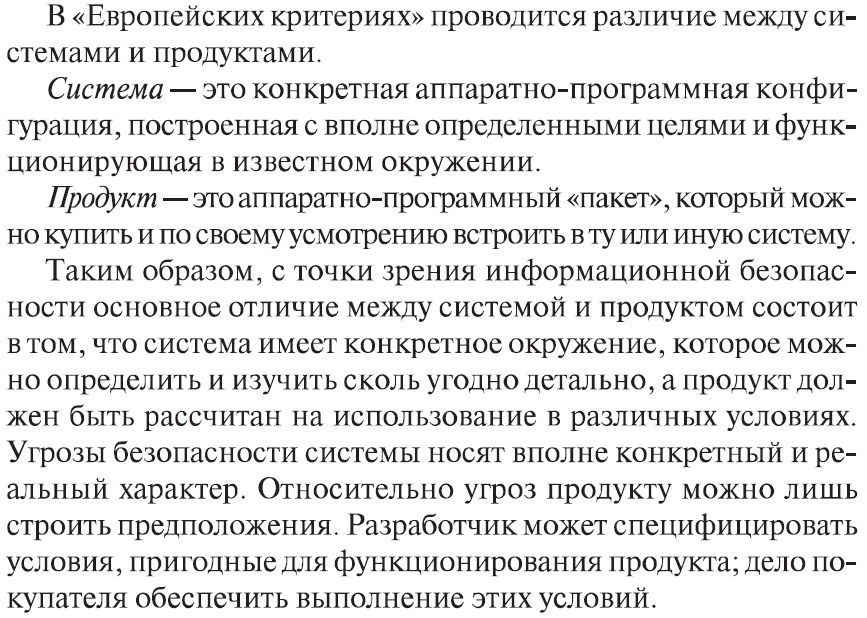
- адекватность (эффективность (соответствие средств безопасности решаемым задачам) и корректность (правильность и надежность реализации функций безопасности))

- обеспечение работоспособности

В "Критериях" дается определение различия между системами и продуктами.

**3. Чем отличаются «информационная система» и «продукт информационных технологий»?**

Продукт информационных технологий – совокупность аппаратных и/или программных средств, которая представляет собой поставляемое конечному потребителю готовое к использованию средство обработки информации.



**4. Что такое Профиль защиты?**

Профиль защиты – это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, технологии разработки и квалификационному анализу.

**5. Опишите структуру Общих критериев безопасности информационных технологий.**

Общие критерии оперируют понятием ИТ-продукта и используют концепцию Профиля защиты.

Общие критерии рассматривают информационную безопасность как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом. Регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов. «Единые критерии» содержат совокупность предопределенных оценочных уровней уверенности в безопасности, составленных из компонентов семейств требований уверенности в безопасности.

**6. Опишите технологию применения Общих критериев безопасности информационных технологий.**

Этот процесс основан на уточнении требований безопасности, отображенных в краткой спецификации в составе задания по безопасности. Каждый последующий уровень уточнения представляет декомпозицию проекта с его дополнительной детализацией. ОК устанавливают базовую структуру для проведения оценок. Представлением требований к свидетельствам и анализу может достигаться получением более объективных и, следовательно, более значимых результатов оценки. В ОК вводятся общая совокупность конструкций и язык для выражения и взаимосвязи аспектов, относящихся к безопасности ИТ, что дает возможность воспользоваться накопленным опытом и специальными знаниями.

**7. Каковы тенденции развития международной нормативной базы в области информационной безопасности?**

