Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студентка: Сятковская Е.Д.

ФИТ 2 курс 4 группа

Минск 2022

**Практическое занятие 1**

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

Цель: Изучить концепцию национальной безопасности РБ.

1. **Что такое информационная безопасность?**

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

1. **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:**

* деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;
* снижение научно-технологического и образовательного потенциала до уровня, не способного обеспечить инновационное развитие;
* 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. **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?**

Последовательно реализуются демократические принципы свободы слова, права граждан на получение информации и ее использование. Государство создает необходимые условия для развития средств массовой информации и национального сегмента глобальной сети Интернет. Во все сферы жизнедеятельности общества активно внедряются современные информационно-коммуникационные технологии.

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. 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.

**6. Основные положения Оранжевой книги:**

Основными положения Оранжевой книги являются: 6 базовых требований безопасности это:

* Политика безопасности:
* Метки
* Идентификация и аутентификация
* Регистрация и учет
* Контроль корректности функционирования средств защиты
* Непрерывность защиты

**7. Основные положения Европейских критериев безопасности информационных технологий:**

* Защита информации от несанкционированного доступа с целью обеспечение конфиденциальности;
* Обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;
* Обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

**8. Отличия «информационной системы» от «продукта информационных систем»:**

Система – конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

Продукт- аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

Таким образом главное отличие состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

**9. Что такое Профиль защиты?**

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

**10. Структура Общих критериев безопасности информационных технологий:**

Общие критерии содержат совокупность предопределенных оценочных уровней в безопасности, составленных из компонентов семейств уверенности в безопасности. Эти уровни предназначены:

* Для достижения совместимости с исходными критериями
* Для обеспечения потребителя пакетами компонентов общего назначения

**11. Технология применения Общих критериев безопасности информационных технологий:**

Процесс квалификационного анализа включает 3 стадии:

* Анализ Профиля защиты на предмет его полноты, непротиворечивости, реализуемости и возможности использования в качестве набора требований для анализируемого объекта.
* Анализ Проекта защиты на предмет его соответствия требованиям Профиля защиты, а также полноты, непротиворечивости, реализуемости и возможности использования в качестве эталона при анализе ИТ-продукта.
* Анализ ИТ-продукта на предмет соответствия Проекту защиты. Результатом квалификационного анализа является заключение о том, что проанализированный ИТ-продукт соответствует представленному Проекту защиты. Заключение состоит из нескольких отчетов, отличающихся уровнем детализации и содержащих мнение экспертов по квалификации об ИТ-продукте на основании критериев квалификации Единых критериев.

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

Согласование позиций и целей производителей, потребителей и аналитиков-классификаторов в процессе создания и эксплуатации продуктов информационных технологий