Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №1**

Концепция национальной безопасности Республики Беларусь

Выполнила:

Студентка 2 курса 1 группы ФИТ

Шимчёнок Елизавета Константиновна

2021 г.

**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. *Перечислить основные национальные интересы в информационной 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.

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

* Недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;
* снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;
* нарушение функционирования критически важных объектов информатизации.

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

Внутренние:

* 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.

Внешние:

* 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.

1. *Основные положения Оранжевой книги.*

1. Политика безопасности.

1.1. Политика безопасности: система должна поддерживать точно определенную политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основе их идентификации и набора правил управления доступом.

1.2. Метки: с объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа.

2. Аудит.

2.1. Идентификация и аутентификация: все субъекты должны иметь уникальные идентификаторы.

2.2. Регистрация и учет: для определения степени ответственности пользователей за действия в системе все происходящее в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе.

3. Корректность.

3.1. Контроль корректности функционирования средств защиты: средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты.

3.2. Непрерывность защиты: все средства защиты должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы.

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

Защита информации от несанкционированного доступа с целью обеспечения конфиденциальности;

обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;

обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

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

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

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

1. *Что такое Профиль защиты?*

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

1. *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.

1. *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 получение 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.

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

Международные стандарты не имеют статуса обязательных для всех стран. Международные стандарты принимаются Международной организацией по стандартизации – ИСО. Сфера деятельности ИСО касается стандартизации во всех областях, кроме электротехники и электроники.