Учреждение образования

«Белорусский государственный технологический университет»

**Практическое занятие №1**

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

Выполнил:

Студент 2 курса 1 группы ФИТ

Парибок Илья Александрович

**2022 г.**

**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;

**2.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.

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

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.

**4.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.

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

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.

**Вопросы для самоконтроля**

**2.Охарактеризуйте основные положения Оранжевой книги.**

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 самих средств защиты.

**Политика безопасности**

Система должна поддерживать точно определённую политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основе их идентификации и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации, отмеченной грифом секретности: «секретно», «сов. Секретно» и т.д.).

**Метки**

С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

**Аудит**

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 ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

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. 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 эффективность его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

**Корректность**

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 учёт, 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.

**Непрерывность защиты**

Все средства защиты (вт. ч. 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, eгo выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

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

Европейские критерии рассматривают следующие задачи средств информационной безопасности:

• 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.

**5.Чем отличаются «информационная система» и «Продукт информационных технологий»?**

Система - это конкретная аппаратно-программная конфигурация, построенная с вполне 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.

Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом 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.

**7.Что такое Профиль защиты?**

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

**Профиль защиты** - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

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

Единые критерии регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов, используя схему из Федеральных критериев. Единые критерии предлагают достаточно сложный процесс разработки и квалификационного анализа ИТ-продуктов, требующий от потребителей и производителей составления и оформления весьма объемных и подробных нормативных документов.

Задачи защиты - базовое понятие Единых критериев, выражающее потребность потребителей ИТ-продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

Проект защиты - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования.

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

Каталог функциональных классов:

• аудит,

• связь (подтверждение приёма/передачи информации),

• криптографическая поддержка,

• защита данных пользователя (конфиденциальность, целостность, доступность),

• идентификация и аутентификация,

• управление безопасностью,

• приватность (конфиденциальность работы в системе),

• надежность средств защиты,

• контроль за использованием ресурсов,

• контроль доступа к объекту оценки,

• доверенный маршрут/канал (прямое взаимодействие).

Требования уверенности в безопасности (адекватности)

• управление проектом,

• дистрибуция,

• разработка,

• документация,

• процесс разработки,

• тестирование,

• анализ защиты.

«Единые критерии» содержат совокупность предопределённых оценочных уровней уверенности в безопасности, составленных из компонентов семейств требований уверенности в безопасности. Эти уровни предназначены:

• для достижения совместимости с исходными критериями;

• для обеспечения потребителя пакетами компонентов общего назначения.

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

Основное назначение международных стандартов - это создание на межгосударственном уровне единой основы для разработки новых и совершенствования действующих систем качества. Сотрудничество в области стандартизации направлено на приведение в соответствие национальной системы стандартизации с международной. Международные стандарты не имеют статуса обязательных для всех стран-участниц. Любая страна мира вправе применять или не применять их. Решение вопроса о применении международного стандарта связано в основном со степенью участия страны в международном разделении труда.