Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студентка: Чепелева Е.Г.

ФИТ 2 курс 4 группа

Преподаватель: Барковский Е.В.

**Что такое информационная безопасность?**

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

**Перечисление основных национальных интересов в информационной сфере**

Нац. интересы – совокупность потребностей гос-ва по реализации сбалансированных интересов личности, общества и гос-ва, позволяющих обеспечивать конституционные права, свободы, высокое качество жизни граждан, независимость, территориальную целостность, суверенитет и устойчивое развитие РБ.

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

**Основные угрозы национальной безопасности, связанные с ИТ-сферой**

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.

**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.

**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.

**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.

**2.Основные положения Оранжевой книги**

С 1983 по 1988 год Министерство обороны США и Национальный комитет компьютерной безопасности разработали систему стандартов в области компьютерной безопасности, основными из которых явились критерии оценки безопасности компьютерных систем", которые по цвету обложки чаще называют **"Оранжевой книгой".**

1.Политика безопасности

* 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.

**Политика безопасности** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

* 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.

2.Аудит

* Идентификация и аутентификация.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.
* Регистрация и учёт. 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.

3.Корректность

* Контроль корректности функционирования средств защитыСредства 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.
* 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.

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

Основными положениями являются:

* 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

**5.Чем отличается «Информационная система» и «продукт информационных технологий»?**

Под информационной системой понимается следующее :

* Это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении

А под информационным продуктом понимают:

* аппаратно-программный “пакет”, который можно купить и по своему усмотрению встроить в ту или иную систему

**7.Что такое Профиль защиты?**

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

**9.Опишите структуру 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

**10.Опишите технологию 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 азализируемого 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.

**11.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

Из вордовского файла найти ответы на вопросы

Из пдф надо вопросы:2,4,5,7,9,10,11