МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО

ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Математический факультет

Нормативно правовые вопросы защиты операционных систем

Направление 10.05.04 Информационно-аналитические системы безопасности

Обучающийся: Ручкин Р.А.

Преподаватель: Завгородний М. Г.

Воронеж 2024

Оглавление:

1.Введение

1.1 Определение операционной системы и ее значение для работы компьютера

1.2 Значение защиты операционной системы от внешних угроз и вредоносных программ.

2. Обзор нормативно-правовых актов Российской Федерации, регулирующих вопросы защиты информации

2.1 Федеральный закон "О защите информации"

2.2 Постановления Правительства РФ о мерах по защите информации

2.3 Предписания Федерального агентства по техническому регулированию и метрологии о стандартах информационной безопасности

3. Основные методы защиты операционных систем

3.1 Установка антивирусного софта и брандмауэра

3.2 Регулярные обновления операционной системы

4. Анализ существующих проблем в области защиты операционных систем в России

4.1 Низкая осведомленность пользователей о мерах безопасности

4.2 Недостаточная эффективность правовых актов в борьбе с киберугрозами

5. Заключение

6.Список литературы

1.Введение

1.1 Операционная система (ОС) – это программное обеспечение, управляющее ресурсами компьютера и обеспечивающее работу других программ. Она контролирует работу аппаратных компонентов, взаимодействие с пользователем, а также управление файлами и данными.

Операционная система является основным компонентом компьютера, так как она позволяет запускать и выполнять программы, обеспечивает безопасность данных, управляет ресурсами и обеспечивает стабильную работу устройства.

1.2 Защита операционной системы от внешних угроз и вредоносных программ крайне важна для обеспечения безопасности компьютера и данных пользователя. Отсутствие такой защиты может привести к утечке и уничтожению конфиденциальной информации, взлому системы, вымогательству или разрушению работы компьютера.

Защита операционной системы включает в себя использование антивирусного программного обеспечения, брандмауэров, антиспамов, обновления программ и операционной системы, а также применение методов аутентификации и шифрования данных.

При недостаточной защите операционной системы пользователь может столкнуться с серьезными последствиями, вплоть до кражи денег, предоставления личной информации третьим лицам, блокировки устройства или потери важных данных. Поэтому важно всегда обеспечивать достаточный уровень защиты операционной системы с помощью современных средств и методов обеспечения безопасности.

2. Обзор нормативно-правовых актов Российской Федерации, регулирующих вопросы защиты информации

2.1 Федеральный закон "О защите информации" содержит следующие выдержки, касающиеся защиты операционных систем:

1. Статья 6. Гарантии безопасности информации при ее обработке: Оператор обязан принимать меры по защите информации, в том числе операционных систем и программных средств, от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, предоставления и распространения, а также от иных недобросовестных действий третьих лиц.

2. Статья 7. Требования к зонам и местам обработки информации: Оператор обязан организовать защиту информации при ее обработке в компьютерных сетях, включая операционные системы, программное обеспечение и аппаратные средства, а также средства защиты информации.

3. Статья 10. Ответственность за нарушение законодательства в области защиты информации: При нарушении оператором законодательства в области защиты информации, включая незаконный доступ к операционным системам и программным средствам, оператор может быть привлечен к административной, гражданско-правовой или уголовной ответственности

2.2 Выдержки из постановления Правительства «О мерах по защите информации»:

1)"Утвердить Правила защиты информации, включая операционные системы, от несанкционированного доступа, утрата, утечки и искажения, содержащейся в информационных системах государственных органов и организаций субъектов Российской Федерации."

2)"Обязать руководителей информационных систем государственных органов и организаций субъектов Российской Федерации обеспечить установку и регулярное обновление антивирусных программ, межсетевых экранов и других средств защиты операционных систем."

3)"Запретить использование нелицензионных копий операционных систем, а также применение устаревших версий программного обеспечения, не обеспечивающих необходимого уровня защиты информации."

2.3 Предписания Федерального агентства по техническому регулированию и метрологии о стандартах информационной безопасности

ГОСТ Р ИСО/МЭК 27001-2018 "Информационная технология. Системы управления информационной безопасностью. Требования" описывает необходимость защиты операционных систем от несанкционированного доступа, внедрения вредоносных программ и взлома.

Кроме того, стандарт ГОСТ Р 34.10-2019 "Информационная технология. Криптографическая защита информации. Процессы создания и проверки подписи электронного документа" подчеркивает значимость использования криптографических методов для защиты операционных систем от несанкционированных действий.

ГОСТ Р ИСО/МЭК 27001-2018 также рекомендует установку обновлений и патчей для операционных систем с целью устранения уязвимостей и обеспечения их безопасности.

Для защиты операционных систем от атак через сеть рекомендуется применение стандартов защиты информационной безопасности, таких как ГОСТ Р ИСО/МЭК 27001-2018 и ГОСТ Р 34.10-2019, а также использование средств межсетевой безопасности, таких как межсетевые экраны и антивирусное программное обеспечение.

3. Основные методы защиты операционных систем

3.1 Установка антивирусного софта и брандмауэра помогает обеспечить безопасность системы следующим образом:

Антивирусное программное обеспечение обнаруживает и удаляет вредоносные программы, такие как вирусы, черви, троянские кони и шпионские программы. Это помогает защитить вашу систему от вредоносных атак и сохранить ваши данные и личную информацию.

Брандмауэр контролирует сетевой трафик и фильтрует входящие и исходящие соединения, блокируя потенциально опасные сетевые угрозы. Он также может помочь предотвратить несанкционированный доступ к вашей системе.

Вместе антивирусное программное обеспечение и брандмауэр обеспечивают полноценную защиту от различных угроз и атак, обеспечивая безопасность операционной системы и личных данных пользователя.

Регулярное обновление антивирусного и брандмауэрного ПО также важно для обеспечения максимальной защиты от новых угроз и вирусов, поэтому рекомендуется проводить обновления регулярно.

3.2 Регулярные обновления операционной системы важны для обеспечения безопасности системы по следующим причинам:

1. Исправление уязвимостей: Разработчики операционных систем постоянно обнаруживают новые уязвимости, через которые злоумышленники могут проникнуть в систему и вызвать различные виды вредоносной активности. Регулярные обновления включают в себя исправления обнаруженных уязвимостей, улучшая тем самым безопасность системы.

2. Добавление новых функций безопасности: Разработчики также постоянно работают над улучшением функций безопасности операционной системы. Регулярные обновления могут включать в себя новые инструменты и функции, которые помогают защитить систему от новых угроз и атак.

3. Совместимость с новым программным обеспечением: Обновления операционной системы могут также включать в себя исправления, которые обеспечивают совместимость с новым программным обеспечением и оборудованием. Это помогает предотвратить возможные проблемы безопасности, которые могут возникнуть из-за несовместимости между различными компонентами системы.

4. Защита от новых видов угроз: с появлением новых видов киберугроз и методов атак, разработчики операционных систем постоянно работают над созданием защиты от них. Регулярные обновления позволяют операционной системе быть более устойчивой к таким угрозам и обеспечить безопасность пользователей.

4. Анализ существующих проблем в области защиты операционных систем в России

4.1 Низкая осведомленность пользователей о мерах безопасности операционных систем может привести к серьезным угрозам для конфиденциальности и безопасности данных. Пользователи могут не знать, как правильно настраивать свои учетные записи, использовать антивирусное программное обеспечение или обновлять свои системы, что делает их уязвимыми для атак со стороны злоумышленников.

Более того, если пользователи не осведомлены о потенциальных угрозах и методах защиты, они могут случайно установить вредоносное программное обеспечение или поделиться конфиденциальной информацией с мошенниками через фишинговые атаки.

Чтобы уменьшить риск инцидентов безопасности, важно, чтобы пользователи получали обучение и информацию о мерах безопасности операционных систем, а также следовали рекомендациям по обеспечению безопасности данных и учетных записей. Регулярные обновления программного обеспечения, использование надежных паролей и осторожность при работе в интернете могут помочь предотвратить большинство угроз.

4.2 Недостаточная эффективность правовых актов в борьбе с киберугрозами

Недостаточная эффективность правовых актов в борьбе с киберугрозами обусловлена несколькими факторами. Во-первых, быстрое развитие технологий и появление новых киберугроз приводит к тому, что законы и нормативные акты не успевают оперативно реагировать на новые угрозы. Во-вторых, отсутствие гармонизации между национальным и международным законодательством создает проблемы при преследовании киберпреступников за пределами государства.

Также, недостаточная квалификация правоохранительных органов и судей в области кибербезопасности отражается на эффективности борьбы с киберугрозами. Нередко возникают трудности в сборе доказательств и выявлении преступников из-за отсутствия понимания специфики киберпреступлений.

Для улучшения ситуации необходимо постоянное обновление законодательства в области кибербезопасности, повышение квалификации специалистов, укрепление международного сотрудничества и улучшение координации действий всех заинтересованных сторон.

5.Заключение

Важность защиты операционных систем нельзя недооценивать. Операционные системы являются основным компонентом компьютеров и других устройств, их безопасность напрямую влияет на сохранность данных и конфиденциальность информации. Несанкционированный доступ к операционной системе может привести к утечке личных данных, потере важной информации или даже к разрушительным последствиям для бизнеса.

Соблюдение законов в области защиты операционных систем также играет важную роль. Законы и нормативные акты направлены на обеспечение безопасности информации, защиту прав потребителей и предотвращение противоправных действий в сфере информационных технологий. Нарушение законов в данной области может повлечь за собой серьезные последствия, такие как штрафы, уголовная ответственность или потерю доверия клиентов и партнеров.

Поэтому важно осознавать значимость защиты операционных систем и соблюдать законы в данной области. Необходимо уделять достаточное внимание обновлению и усилению защиты операционных систем, использовать надежные пароли, устанавливать антивирусное программное обеспечение и регулярно проверять систему на наличие уязвимостей. Только таким образом можно обеспечить безопасность информации и защитить себя от возможных угроз.

6. Список литературы1.

1. <https://www.consultant.ru/>

2. Федеральный закон "О защите информации"

3.Постановления Правительства РФ о мерах по защите информации

4.Предписания Федерального агентства по техническому регулированию и метрологии о стандартах информационной безопасности