Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
Информатики и радиоэлектроники»

УДК 004.932.72

Мешков
Александр Святославович

Модели и инструментальные средства аутентификации в распределенных компьютерных системах

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-45 80 02 Телекоммуникационные системы и компьютерные сети

_____

Научный руководитель

Ширинский Валерий Павлович

к.т.н., доцент

_____

Минск 2019

КРАТКОЕ ВВЕДЕНИЕ

Безопасность информационных систем является частью более широкой проблемы – безопасности компьютерных систем, или еще более общей проблемы – информационной безопасности. Информация, как продукт, удовлетворяющий определенным потребностям субъектов, который они получают посредством информационных систем, должна обладать следующими свойствами.

Доступность – возможность за приемлемое время выполнить ту или иную операцию над данными или получить нужную информацию.

Целостность – это актуальность и непротиворечивость хранимой информации.

Непротиворечивость информации – это соответствие содержимого информационном базы логике предметной области.

Конфиденциальность – защищенность информации от несанкционированного доступа.

Проблема обеспечения защиты информации является одной из важнейших при построении надежной информационной структуры учреждения на базе ЭВМ. Эта проблема охватывает как физическую защиту данных и системных программ, так и защиту от несанкционированного доступа к данным, передаваемым по линиям связи и находящимся на накопителях, являющегося результатом деятельности, как посторонних лиц, так и специальных программ-вирусов.

Для защиты от несанкционированного доступа к персональным компьютерам, серверам и другому оборудованию применяются механизмы аутентификации, использующие различные характеристики пользователей

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью данной работы является исследование моделей и инструментальные средства аутентификации в распределенных компьютерных системах и определение оптимизированных параметров процедуры аутентификации для снижения уровня ошибок распознавания.

В задачи исследования входят:

– знакомство с научной литературой, используемыми методами распознавания и аппаратурой считывания лиц;

– моделирование процессов реализации угроз;

– изучение характеристик веб-камер;

– распознавание изображений, полученных веб-камерой, анализ результатов;

– подведение итогов по работе, определение требований применения методики.

Апробация результатов диссертации

Основные положения диссертации обсуждались на 53-й научно – технической конференции аспирантов, магистрантов и студентов БГУИР.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе – распределенная компьютерная система (РКС) как объект атак, связанных с несанкционированным доступом к её элементам рассматриваются механизм взаимодействия и процессы реализации несанкционированного доступа в операционную среду компьютера.

Во второй главе – уязвимости РКС в отношении угроз несанкционированного доступа рассматриваются классификация угроз НДС, классификация атак, описание процессов реализации удаленных атак.

В третьей главе – политика информационной безопасности рассматриваются непрерывность защиты в пространстве и времени, разделение обязанностей, минимизация привилегий, определение перечня возможных аварий, Разработка стратегии восстановительных работ.

В четвертой главе – о объектов защиты от угроз НСД рассматриваются.

В пятой главе – аналитическое моделирование процессов реализации угроз НСД к элементам РКС проводится моделирование процессов реализации сетевого анализа, моделирование процесса реализации атаки «Отказ в обслуживании», моделирование процессов реализации внедрения в сеть ложного объекта.

В шестой главе – аутентификация на основе распознавания лица рассматриваются методы распознавания по лицу и проводится обзор используемого в работе оборудования с экспериментальной оценкой.

СУЩНОСТЬ ПОНЯТИЯ БЕЗОПАСНОСТИ РКС

Достаточно четко сформулировать понятие безопасности некоторой системы не просто. Ставить же задачу обеспечения безопасности функционирования какой-либо системы, не определив само понятие безопасности, неправильно, так как отсутствие ясного понимания цели проекта обычно ведёт к нерациональному использованию ресурсов и, возможно, к срыву всего проекта. Поэтому на государственном уровне сформулированы и законодательно оформлены документы, определяющие концепцию безопасности и концепцию экономической безопасности.

В этих документах, а также во многих научных работах понятие безопасности связывается с защитой некоторых активов от угроз. Угрозы классифицируются в зависимости от возможности нанесении ущерба защищаемым активом. В качестве основных обычно рассматриваются угрозы, которые связаны с умышленными действиями или непреднамеренными действиями людей. Помимо угроз, связанных с деятельностью человека, существуют и рассматриваются угрозы, связанные с объективными процессами, происходящими в природе, такими, как стихийные бедствия, физически процессы, влияющие на распространение радиоволн, и т.п.

Безопасность РКС можно определить как состояние защищённости РКС от угроз её нормальному функционированию. Под защищённостью понимается наличие средств РКС и методов их применения, обеспечивающих снижение или ликвидацию негативных последствий, связанных с реализацией угроз. Изложенный подход к определению понятия безопасности РКС предполагает, что перечень и содержание угроз достаточно хорошо определены и достаточно стабильны во времени.

Безопасность РКС можно определить, как свойство системы адаптироваться к агрессивным проявлениям среды, в которой функционирует система, обеспечивающее поддержку на экономически оправданном уровне характеристики качества системы. В сформулированном определении основной акцент делается не на перечне и содержании угроз, нейтрализация которых обеспечивается, а на особую характеристику качества системы. При этом основной критерий качества РКС является экономическим, т. е. оценка средств и методов обеспечения безопасности осуществляется на основе учета затрат на реализацию механизмов безопасности и потенциальных выгод от недопущения ущерба, связанного с целенаправленным или случайным агрессивным проявлением среды.

Уверенность в безопасности РКС может быть достигнута в результате согласованных действий, предпринимаемых в процессе разработки, оценки и эксплуатации объекта оценки. Функциональное назначение оценки безопасности РКС – получение определенной степени уверенности в том, насколько система удовлетворяет предъявляемым к ним требованиям. Результаты оценки должны помочь потребителю установить, достаточен ли уровень безопасности системы для предполагаемых применений этой системы и являются ли приемлемыми остаточные риски.

Уязвимость РКС - это некая ее характеристика, которая делает возможным существование угрозы. Другими словами, именно из-за наличия уязвимостей в системе могут происходить нежелательные события.

Атака на РКС - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости для реализации некоторой угрозы ИБ РКС. Таким образом, под атакой будем понимать процесс реализации угрозы. Заметим, что такое толкование атаки (с участием человека, имеющего злой умысел), исключает присутствующий в определении угрозы элемент случайности, но, как показывает опыт, часто бывает невозможно различить преднамеренные и случайные действия, и система защиты должна адекватно реагировать на любое из них.

Угрозы, связанные с несанкционированным доступом, выделяются из всего комплекса угроз по способу реализации. При этом под несанкционированным доступом понимается доступ к информации заинтересованным субъектом с нарушением установленных прав или правил доступа к информации. Сам несанкционированный доступ угрозой как таковой не является. Угрозы могут появиться в связи с НСД. При этом может быть несанкционированное ознакомление с информацией, несанкционированное

копирование (хищение) информации и/или несанкционированное воздействие на информацию (уничтожение, блокирование и т.д.).

ЗАКЛЮЧЕНИЕ

Информационная безопасность относится к числу дисциплин, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс информационных технологий, так и постоянное противоборство нападающих и защищающихся.

К сожалению, подобная динамичность объективно затрудняет обеспечение надежной защиты.

Обеспечение информационной безопасности современных информационных систем требует комплексного подхода. Оно невозможно без применения широкого спектра защитных средств, объединенных в продуманную архитектуру. Далеко не все эти средства получили распространение в РБ, некоторые из них даже в мировом масштабе находятся в стадии становления.

В части эксперимента по разрабатываемой темой были получены данные о точности аутентификации по ранее разработанному набору параметров.

Подводя итог работы можно сказать следующее. Развитие технологий позволяет внедрять разработку в повседневную жизнь. Удобство для пользователей и дешевизна могут стать хорошим подспорьем в рамках внедрения в домашнем использовании или малого предприятия.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Мешков, А. С. Защита ИТКС от угроз несанкционированного доступа/ А. С. Мешков // Тезисы докладов 53-й науч.-техн. конф. аспирантов, магистрантов и студентов БГУИР, Минск, 3-5 мая 2017 г. – Минск: БГУИР, 2017.

2-А. Мешков, А. С Защита ИТКС от угроз несанкционированного доступа / А. С. Мешков // Технические средства защиты информации: тезисы докладов XV Белорусскороссийской науч.-техн. конф. Минск, 6 июня 2017 г. – Минск : БГУИР, 2017 – с.61