Содержание

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

ВВЕДЕНИЕ

Актуальность исследования

Одним из главных направлений развития науки в настоящее время является внедрение информационных технологий во все сферы жизнедеятельности человека. Для современного этапа развития общества характерен непрерывный процесс информатизации и совершенствования информационных технологий. Сфера внедрения коммуникационных и вычислительных систем постоянно расширяется, затрагивая все новые стороны жизни общества [12,25,33].

Финансовые системы не являются исключением и призваны предоставить надежность, безопасность и гарантированность проведения финансовых операцийс отсутствием возможности полного выхода из строя устройств, обеспечивающихпроведение платежей. Электронные расчеты как вид безналичных расчетов появились во второй половине XX века. Они приобрели принципиально новое качество, когда на обоих концах линии связи появились компьютеры (терминалы).Терминал платежнойсистемы — это оборудование, оснащенное специальным программным обеспечением, при помощи которого осуществляется перевод финансовых средств. Качественный скачок выражался в том, что скорость осуществления платежей значительно возросла и появилась возможность их автоматической обработки. В дальнейшем появились электронные эквиваленты различных классических платежных средств[4,8,34,42].

Принцип работы терминала заключается в электронном переводе денежных средств в пользу получателя. Данные о каждой транзакции через терминал в цифровом виде доставляются на сервер, который поддерживает работу платежных систем. После этого деньги переводятся на счет продавца той или иной услуги. Терминалы универсальныи могут быть освоенылюдьми любого возраста.На сегодняшний день платежный терминал позволяет оплачивать услуги связи, производить коммунальные платежи, платить за интернет и другие сервисы. При этом,терминал в процессе транзакций не требует участия оператора, терминал оплаты прост и удобен работе[8,34,42,47,78].

Платежные системы в качестве посредника между продавцами, покупателями и их банками доступны как для правомерных операций, так и для злоумышленных несанкционированных действий. Сделать терминалыплатежных систем как можно более надежными и безопасными – это одна из важнейших задач. От качества решения задачи обеспечения информационной безопасности финансовых транзакций во многом зависят темпы и перспективы развития электронной коммерции в целом и прибыль владельца платежной системы в частности[11,26,81].

Уязвимость платежных систем существенно превышает уязвимость отдельно взятых терминалов. Это связано, прежде всего с масштабностью, открытостью и неоднородностью самих платежных систем. При этом число угроз информационной безопасности и способов их реализации постоянно увеличивается. Основными причинами являются здесь рост сложности программно - аппаратных средств и недостатки современных информационных технологий. На сегодняшний день наиболее распространенным видом мошеннических операций является скимминг, т.е. считывание информации с магнитной полосы пластиковой карты, незаконное получение ПИН-кода и изготовление поддельной пластиковой карты с теми же характеристиками. Доля скимминга составляет более 80% от общего количества преступлений в платежных системах. [11,35,47,69]

Для эффективного решения задач обеспечения безопасности и защиты информации в платежных системах необходим тщательный анализ всех возможных угроз информационной безопасности, что позволит своевременно принять меры противодействия. При анализе угроз особое внимание следует уделить оценке угроз атак несанкционированного доступа к терминалам платежных систем, а также ущербу, который будет нанесен в случае реализации атак несанкционированного доступа [4,8,18,72].

Таким образом, при создании и модернизации систем обработки финансовых транзакций в платежных системах необходимо уделять пристальное внимание обеспечению информационной безопасности терминалам как элементам платежных систем.

В связи с этим важной задачей является обеспечение достаточной степени защищенности терминалов платежных систем для эффективного функционирования в условиях реализации атак несанкционированного доступа и, в конечном счете, минимизации ущерба от их деструктивных воздействий.

Степень проработанности темы

В настоящее время активно ведутся исследования возможности применения риск-модели атак несанкционированного доступа на терминалы платежных систем и возникающих от их реализации ущербов, для обеспечения информационной безопасности платежной системы. Непредсказуемость таких атак не позволяет создать детерминированное описание этих процессов и возникающих от их реализации ущербов. Поэтому, при создании защищенных платежных систем, вполне обоснованно рассмотрение ущерба от реализации атак несанкционированного доступа как случайной величины [15, 52, 81, 92].

Таким образом, исходя из актуальности и степени научной разработанности проблемы нарастания ущербареализации атак несанкционированного доступа к терминалам платежных систем, можно сделать вывод о целесообразности проведения комплексных исследований в данном направлении.

Объектом исследования являются терминалы платежной системы, распределѐнной на расстоянии, осуществляющие платежные операции, в отношении которых реализуются атаки несанкционированного доступа.

Предметом исследования является математическая модель оценивания защищѐнности платежной системы в результате реализации атак несанкционированного доступа.

Цель и задачи исследования.

Цель настоящей работы заключается в оценке рисков реализации атак несанкционированного доступа на терминалы платежной системы как объект защиты от деструктивных воздействий на технологический процесс. Для достижения указанной цели предполагается решить следующие задачи:

1. Построить аналитическую модель платежной системы, как среды реализации основных видов угроз реализации атак несанкционированного доступа;

2.Провести анализ основных видов угроз, воздействующих на терминалы платежной системы;

3. Оценить и изучить функции полезности и выживаемости терминалов платежной системы;

4. Разработать риск-модель платежной системы, терминалы которой подвергаются воздействию атак несанкционированного доступа;

5. Разработать новый подход к вычислению рисков в платежных системах, терминалы которых подвергаются реализации атак несанкционированного доступа.

1. **Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе**, обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

Методы исследования.

В исследовательской работе применялись: методы из аппарата теории вероятности и математической статистики, теория графов, методы системного анализа, теории рисков, а так же теории надѐжности.

На защиту выносятся следующие основные положения работы:

1 Аналитическая модель терминалов платежной системы, как средыреализации основных видов угроз реализации атак несанкционированного доступа;

2 Риск-модель платежной системы, терминалы которой подвергаются воздействию атак несанкционированного доступа;

3 Алгоритм подхода к изучению рисков реализации атак несанкционированного доступа и выживаемости платежной системы, терминалы которой подвергаются реализации атак несанкционированного доступа.

Научная новизна исследования.

В настоящей работе получены следующие основные результаты, характеризующиеся научной новизной:

1. В исследовании основных угроз, связанных с работой платежных систем, были учтены результаты их количественного и качественного развития, а также особенности реализации при различных условиях и типах терминалов.

2. В отличие от аналогичных работ, полученная риск-модель платежной системы включает в себя выражения для экстремумов интегрального риска терминалов платежной системы;

3. Отличительной особенностью подхода к изучению безопасности платежной системы, в отношении которойреализуются атаки несанкционированного является изучение выживаемости системы.

4. Разработана динамическая риск-модель платежной системы, терминалы которой подвергаются деструктивному воздействию,получена функция чувствительности.

Практическая ценность работы заключается в том, что:

2. Анализ основных видов угроз, воздействующих на терминалы платежных систем, позволяет выявить наиболее опасные их виды и дает возможность уделить особое внимание защите от атак несанкционированного доступа.

3. Доказательство выдвинутых гипотез о распределении ущерба от реализации атак несанкционированного доступа позволяет обосновано применять рассматриваемую риск-модель для решения задач безопасности платежных систем.

4. Построенная риск-модель может применяться для оценки рисков в платежных системах, использующих распределенные системы как основное средство для обмена информацией и контроля работы, а также построения платежных систем, устойчивых к воздействию атак несанкционированного доступа.

5. Полученная динамическая риск-модель может быть использована для построения в государственных и коммерческих организациях платежных систем, устойчивых к реализации атак несанкционированного доступа, приводящих к полной утрате работоспособности терминалов.

6. Полученные выражения для интегрального риска платежной системы и его экстремумов позволяют оценитьэффективность обеспечения защиты от

реализации атак несанкционированного доступа в данных организациях и выявить наиболее уязвимые терминалы платежной системы.

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT