



СОДЕРЖАНИЕ

projectIT	Введение.....	projectIT	9
	1 Постановка задачи математического моделирования и риск-анализа мошеннических операций в распределенных платежных системах		13
	1.1 Функционирование распределенной платежной системы на основе банковских пластиковых карт.....		13
	1.2 Обслуживание банковских пластиковых карт.....		22
	1.3 Операции с использованием банковских пластиковых карт.....		23
	1.4 Мошеннические операции в распределенных платежных системах, на основе банковских карт.....		23
	1.5 Современные виды мошеннических операций с использованием банковских пластиковых карт.....		26
	1.6 Основной подход к оценке рисков возникновения мошеннических операций.....		27
	1.7 Основные выводы по главе.....		28
	2 Построение риск-модели распределенной платежной системы при воздействии мошеннических операций с банковскими картами		29
	2.1 Обоснование выбора и доказательство гипотезы бета- распределения первого рода		29
	2.2 Расчет параметров риска компонент РПС для бета-распределения первого рода плотности вероятности наступления ущерба.....		35
	2.3 Риск-анализ систем в диапазоне ущербов.....		44
	2.4 Расчет риска распределенной платежной системы на основе параметров риска ее компонентов.....		47
	2.5 Основные выводы по главе.....		51
	3 Оценка динамики развития риск-модели распределенной платежной системы при мошеннических операциях с банковскими картами.....		52
	3.1 Функции чувствительности и их применение.....		52
	3.2 Расчет коэффициентов чувствительности риска		54



3.3 Расчет коэффициентов относительной чувствительности риска.59

3.4 Расчет коэффициентов чувствительности риска распределенной платежной системы в условиях синхронных и асинхронных атак64

3.5 Основные выводы по главе.....72

4 Организационно-экономическая часть.....73

4.1 Формирование этапов и перечня работ по исследованию процессов несанкционированного съема конфиденциальной информации по акустическому каналу: анализу и управлению рисками.....73

4.2 Определение трудоемкости исследования мошеннических операций с банковскими картами в распределенных платежных системах: анализа и управления рисками73

4.3 Разработка календарного плана проведения работ по исследованию мошеннических операций с банковскими картами в распределенных платежных системах77

4.4 Расчет сметной стоимости и договорной цены исследования мошеннических операций с банковскими картами в распределенных платежных системах.....82

4.5 Расчет экономической эффективности при оптимальном построении системы защиты от мошеннических операций с банковскими картами в распределенных платежных системах.....85

4.6 Прогнозирование ожидаемого экономического эффекта от внедрения исследования мошеннических операций с банковскими картами в распределенных платежных системах90

5 Безопасность и экологичность.....101

5.1 Безопасность производственной среды.....101

5.1.1 Анализ условий труда.....101

5.1.2 Меры защиты от опасных и вредных факторов.....104



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

5.1.2.1 Освещенность рабочей зоны.....104

5.1.2.2 Микроклимат.....106

5.1.2.3 Электромагнитное излучение.....107

5.1.2.4 Электробезопасность.....109

5.1.2.5 Статическое электричество.....111

5.1.3 Расчет и проектирование средств защиты.....112

projectIT

5.2 Экологичность проекта.....117

5.3 Чрезвычайные ситуации.....118

5.3.1 Оценка возможности возникновения ЧС и план действий по их ликвидации.....118



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

5.3.2 Пожарная безопасность.....118

5.4 Основные выводы по главе.....121

Заключение.....122

projectIT

Список литературы.....123

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



ВВЕДЕНИЕ

Актуальность темы.

С развитием в России рынка банковских услуг широкое распространение получили пластиковые платежные средства, зарекомендовавшие себя в качестве удобного инструмента для осуществления безналичных платежей. В стране уже длительное время функционируют различные платежные системы, все больше предприятий и организаций переходят на использование пластиковых карт для выдачи заработной платы сотрудникам, что ведет к значительному росту числа владельцев кредитных и расчетных карт и других участников системы карточных расчетов.

Однако ситуация в сфере выпуска и обращения банковских карт характеризуется и рядом негативных признаков. Наряду с развитием системы карточных расчетов наблюдается возрастание интереса к сфере обращения банковских карт со стороны криминальных кругов. По мере увеличения в обращении количества карт эти платежные средства становятся предметом разного рода преступлений, выступая как в качестве предмета преступления в уголовно-правовом значении, так и в качестве средства совершения преступлений против собственности. Анализ криминогенной ситуации в кредитно-финансовой сфере показывает, что преступность в этой области растет параллельно с развитием банковских систем. Анализ динамики видов преступлений позволяет сделать вывод об устойчивой тенденции к их росту, который превышает рост всей экономической преступности. Согласно статистическим данным в России с каждым годом наблюдается значительное увеличение материального ущерба от изготовления и сбыта поддельных банковских карт и мошенничества, совершенного с использованием банковских карт.

На практике привлечение к уголовной ответственности за преступления в указанной сфере вызывает определенные затруднения, которые связаны как с высоким уровнем их латентности, так и с многочисленными проблемами,

возникающими при квалификации действий преступников. В основном трудности обусловлены вопросами, возникающими при толковании и применении уголовно-правовых норм, дискуссионностью в понимании значения терминов, употребляемых в соответствующих статьях УК РФ, а также отсутствием специальной литературы и методических рекомендаций. Как известно, правильная квалификация преступления является важнейшим требованием законности и гарантом справедливости применяемых мер ответственности. Совершенное преступление должно быть квалифицировано в точном соответствии с законом, предусматривающим уголовную ответственность за это деяние. Важнейшей предпосылкой правильного применения уголовно-правовых норм выступает четкое уяснение смысла закона, чему способствует научная разработка вопросов уголовного права в целом и квалификации отдельных видов преступлений в частности.

Еще одной проблемой является отсутствие моделей мошеннических операций в распределенных платежных системах (РПС), на основе банковских картах (БК), что снижает вероятность минимизации рисков в данной сфере, а так же лишает возможности управления эффективностью защиты информации в РПС, на основе БК и защищенностью РПС.

Учитывая вышесказанное, вопросы построения риск - моделей мошеннических операций в РПС, на основе БК являются чрезвычайно своевременными и актуальными.

Работа выполнена в соответствии с одним из основных научных направлений Международного института компьютерных технологий «Обработка и защита информации».

Объект исследования. Распределенные платёжные системы на основе банковских карт с магнитной полосой, подверженные угрозам мошеннических операций (МО).

Предмет исследования. Моделирование риск - моделей мошеннических операций в распределенных платежных системах на основе банковских карт.



Цель дипломной работы. Моделирование мошеннических операций в распределенных платежных системах на основе банковских карт.

Основные задачи. Для достижения поставленной цели, в работе необходимо решить следующие задачи:

1. Произвести анализ основных видов мошеннических операций в распределенных платежных системах на основе банковских карт с магнитной полосой;
2. Построение риск-модели для компонентов РПС, плотности вероятностей наступления ущерба в которых имеют заданный вид распределения;
3. Построить модель мошеннических операций в распределенных платежных системах, на основе банковских карт;
4. Осуществления интегральной оценки и регулирования общего риска распределенной системы;
5. Нахождения универсальных методик и алгоритмов управления информационными рисками, базирующихся на анализе возможного ущерба РПС от ожидаемых МО.

Методы исследования. В работе использованы методы теории вероятностей и математической статистики, теории риска, методы построения систем защиты информации.

Научная новизна. В Дипломной работе получены следующие результаты, характеризующиеся научной новизной:

1. Методология построения риск – моделей отличается от аналогов тем, что она адаптирована к построению риск – моделей МО в распределенных платежных системах, на основе банковских карт;
2. Предложено построение математической модели жизненного цикла МО в РПС, на основе БК. Разработана методика определения динамики вероятностей успешных реализаций МО в распределенных платежных системах на основе банковских карт;

3. Разработана структурная схема алгоритма управления эффективностью защиты информации в РПС, на основе БК, от МО, с использованием меры шансориска;

4. Разработана математическая модель, с помощью которой возможно определение срока окупаемости средств, затраченных на защиту информации от МО в РПС, на основе БК.

Практическая значимость полученных результатов. Научные выводы сделанные в работе по построению риск – моделей МО в РПС, позволяют эффективно их использовать для обеспечения безопасности в распределенных платёжных системах, на основе банковских карт.

Разработанный алгоритм по управлению эффективностью защиты информации в РПС на основе БК, от конкретной МО, с использованием мер шансориска, позволяет не только оценивать риск и шанс конкретной МО с БК, но и принимать решение о том, стоит ли защищать РПС, на основе БК данными методами от конкретной МО.

Основные положения, выносимые на защиту.

1. Анализ основных видов мошеннических операций в распределенных платежных системах на основе банковских карт.

2. Математическая модель мошеннических операций в распределенных платежных системах, на основе банковских карт.

3. Математическая модель оценки рисков с использованием бета-распределения (первого рода) плотности вероятности наступления ущерба, позволяющая получить количественные величины общего риска РПС.

4. Методики и алгоритмы управления информационными рисками, базирующихся на анализе возможного ущерба АС от ожидаемых атак.



Заключение

Работа посвящена математическому моделированию мошеннических операций с банковскими картами в распределенных платежных системах. В ходе ее выполнения были получены следующие основные результаты:

1. Рассмотрен и произведен анализ основных видов мошеннических операций в распределенных платежных системах на основе банковских карт с магнитной полосой.

2. Получены аналитические выражения риск-моделей компонент распределенных платежных систем на основе банковских карт, плотности вероятностей наступления ущерба в которых имеют заданный вид распределения.

3. Исследованы аналитические риск-модели распределенных платежных систем, подвергающихся совместному или не совместному воздействию дестабилизирующих факторов, а также проведена оценка и регулирование общего риска системы при таких воздействиях вплоть до синтеза систем с заданной огибающей функцией риска.

4. Исследованы методики и алгоритмы управления информационными рисками системы, базирующихся на анализе возможного ущерба РПС от ожидаемых МО с использованием математического аппарата основанного на бета-распределении первого рода.

Результаты исследования имеют солидную область применения. Построенный математический аппарат, а также приведенные методики и алгоритмы управления риском позволят строить адекватные системы защиты распределенных платежных систем в условиях недетерминированных проявлений дестабилизирующих факторов.



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

Список литературы

1. «Технические и функциональные требования к системе видеонаблюдения для банкоматов EyeTM», ЗАО «СмартКард-Сервис», Москва.
2. Статья по физической безопасности банкоматов. Александр НИКИТИН, Александр КЛИМОВ, Евгений ТЮРИН, НИЦ «Охрана» ГУВО МВД России, Банковское дело в Москве №4. – с. 64.
3. Голубович А.Д., Миримская О.М. "Кредитные и другие банковские карточки в системе автоматизированных денежных расчетов". М., Менатеп - Информ, 1991.-с. 33-43.
4. Голубович А.Д., Клопотовский А.В., Наумов А.В. «Создание системы кредитных карточек для коммерческих банков» М., Менатеп-информ, 1992 г.- с. 1-12.
5. В. Завалев «Пластиковая карточка как платежный инструмент», Центр Информационных технологий, 1997 г.- с. 1- 40.
6. Ю. Пермин, Ю. Товб «Рынок банковских пластиковых карточек: попытка анализа и прогноза», «Банковские технологии» №1/1996 г.- с. 35-52.
7. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000.- с. 5-13.
8. Теория и практика информационной безопасности", под ред. П.Д. Зегжды. М.: изд-во "Яхтсмен". 1996 г.-с.10 – 21.
9. Герасименко В.А. Защита информации в АСОД. В 2-х кн.: Кн. 1. - М.: Энергоатомиздат, 1994. –с. 11-23.
10. Герасименко В.А, Попов Г.А., Таирян В.И. Основы оптимизации в системах управления (Концепции, методы, модели). М., 1990. Деп. В ВИНТИ 10.04.90, №2373-В90. – с. 21-44.
11. Герасименко В.А., Малюк А.А. Основы защиты информации. - М. 1997.- с. 25.
12. Спесивцев А. "Интеллектуальные карты в качестве электронных денег"- АО "Скан-Тэк", Москва, 1995.- с. 34-76.

13. Серегин В.В., Спесивцев А.В. "Технология SmartCard и ее применение"-
Монитор, Москва, 1995.- с. 54- 56.

14. Андреев А.А., Морозов А.Г., Логинов Ю.В. "Пластиковые карты" -
Банковский деловой центр, Москва, 1998. – с. 28, 30 – 42.

15. Липис А., Маршалл Т. "Электронная система денежных расчетов" -
Финансы и статистика, Москва, 1988. – с. 41.

16. Коробов Ю.И., Рубин Ю.Б. "Банковский портфель -3" - "Соминтэк",
Москва, 1995. – с. 13.

17. ПЛАС (платежи, системы, карточки) №9/2002

18. www.security-systems.com.ua/information/dvr-02.statistics/html.

19. С. Горбунов "Банк "Оптиум" автоматизация банка как процесс"
«Банковские технологии» №1/1996 г. – с.3- 11.

20. Гайкович В., Першин А. Безопасность электронных банковских систем. -
М. Единая Европа, 1994.- с. 16- 22.

21. Петраков А.П. Основы практической защиты информа-ции. М.: Радио и
связь, 2001. – с.14-21.

22.Вертузаев М.С., Кондратьев Я.Ю. Способы совершения преступлений с
использованием банковских платёжных карт.
Материалы Центра исследования компьютерных преступлений.- с. 34-46.

23.Strategies for Issuing. Managing risk in the 21th century. VISA, 2010.

24.Aquier Fraud Management Best Practice. Visa international, January 2010

25.Issuer Fraud Management Best Practice. Visa international, January 2010.

26.A guide to monitoring threshold. VisaInternational. 2006.

27.Материалы семинара «Особенности бизнеса с платёжными картами».
НОУ «Учебный центр Банкир.Ру», Май 2005. – с. 1-3.

28. Аглицкий И. Состояние и перспективы информационного обеспечения
российских банков. — Банковские технологии, 1997 г., №1.- с.12-14.

29. Башлыков М. Актуальные вопросы информационной безопасности //
Финансовая газета. Региональный выпуск. - 2006. - № 4. - С. 9-15.

30. Блинова С., Копылов Д. "Клиент-Банк": правила безопасности // Расчет. -

2005. - № 8. - С. 28-32.

31. Бедрань А. Согласованная методика проведения аудита информационной безопасности // Финансовая газета. - 2007. - № 6. - С. 33-36.

32. Бабкин В.В. Модель нарушителя информационной безопасности - превенция появления самого нарушителя // Управление в кредитной организации. - 2006. - № 5. - С. 18-23.

33. Васильев Г. Российский рынок информационной безопасности: новые тенденции // Финансовая газета. - 2007. - № 1. - С. 16-20.

34. Велигура А. Обеспечение информационной безопасности кредитных организаций на основе использования стандартов ЦБ РФ // Бухгалтерия и банки. - 2006. - № 7. - С.3-6.

35. Волков П. Системы обеспечения информационной безопасности как часть корпоративной культуры современной организации // Финансовая газета. - 2006. - № 34. - С.77-80.

36. Белоглазова Г.Н. Регулирование рыночных рисков как элемент эффективности банковского надзора. - Актуальные проблемы финансов и банковского дела: Сборник научных трудов / Под ред. А.И.Михайлушкина, Н.А.Савинской. - СПб.: СПбГИЭА, 2000. - 178 с.

37. Голикова Ю.С., Хохленкова М.А. Банк России: организация деятельности. М.: ДеКА, 2000. - 138 с.

38. Демин В.С. Безопасность электронных банковских систем. — М: Единая Европа, 1994 г. Демин В.С.- 2-34.

39. Титоренко Г.А. и др. Компьютеризация банковской деятельности. — М: Финстатинформ, 1997. — 69 с.

40. Высоковский Д.В. Управление рисками в коммерческом банке // Расчеты и операционная работа в коммерческом банке. - 2006. - № 5. - С. 20-24.

41. Барсуков В.С. Обеспечение информационной безопасности. - М., 1996.- 57-84с.

42. Альбрехт У., Венц Дж., Уильямс Т. Мошенничество. (Луч света на темные стороны бизнеса), СПб, 1996 пер. с англ. 2000. С-45.

43. Аванесян С.Р. Мошенничество как форма хищения // Право: теория и практика. - М.: Тезарус, 2007, № 4 (93). - С. 65-67.

44. Лестер А. Пратт. Обманные операции с банковскими картами: Пер. англ. М.: Перспектива, 1995. – с 33.

45. Диева С.А. Организация и современные методы защиты информации/ С.А. Диева - М.: Концерн «Банковский деловой центр», 1998. - 472с.

46 .Остапенко Г.А. Оценка рисков и защищенности атакуемых кибернетических систем на основе дискретных распределений случайных величин / Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2005. – Вып. 2. – С. 70 – 75.

47 .Остапенко Г.А., Карпеев Д.О., Плотников Д.Г., Батищев Р.В., Гончаров И.В., Маслихов П.А., Мешкова Е.А., Морозова Н.М., Рязанов С.В., Субботина Е.В., Траниин В.А. Риски распределенных систем: Методики и алгоритмы оценки и управления/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 4. - С. 485 – 530.

48. Остапенко Г.А., Карпеев Д.О. Методическое и алгоритмическое обеспечение расчета параметров рисков распределенных систем на основе параметров рисков их компонентов/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 373 – 380.

49. Остапенко Г.А., Маслихов П.А., Субботина Е.В. Способы регулирования рисков распределенных систем/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 435 – 438.

50. Остапенко Г.А., Мешкова Е.А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия / Г.А. Остапенко, Е.А. Мешкова; Под редакцией Ю.Н. Лаврухина. – М: Горячая линия - Телеком, 2007. - 295 с.

51. Остапенко Г.А., Плотников Д.Г., Мешкова Е.А. Методическое и алгоритмическое обеспечение расчета параметров рисков для компонентов распределенных систем/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 335 – 350.

52. Остапенко Г.А., Транин В.А. Алгоритмическое обеспечение риск-анализа систем в диапазоне ущербов/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 447 – 450.

53. Остапенко О.А. Методология оценки риска и защищенности систем/ О.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2005. – Вып. 2. – С. 28 – 32.

54. Остапенко О.А., Карпеев Д.О., Асеев В.Н., Морев Д.Е., Щербаков Д.Е. Риски систем: оценка и управление. – Воронеж: МИКТ, 2007. – 261 с.61. Питерсон Дж. «Теория сетей Петри и моделирование систем», Москва «Мир», 1984, с. 25, 44, 137, 182.

55. Поллард Дж. Справочник по вычислительным методам статистики / Дж Поллард. – М.: Финансы и статистика, 1982. – 575 с.

56. Приходько А.Я. Словарь-справочник по информационной безопасности / А.Я. Приходько – М.: СИНТЕГ, 2001. – 124 с.

57. Радько Н.М., Скобелев И.О. // Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М.: РадиоСофт., 2010. – 230с.

58. Розенвассер Е.Н. Методы теории чувствительности в автоматическом управлении/Р.Н. Розенвассер, Р.М. Юсупов. – Л.: «Энергия», 1971. – 260 с.

59. Розенвассер Е.Н. Чувствительность систем управления/Р.Н. Розенвассер, Р.М. Юсупов. – М.: Наука, 1981. – 464 с.

60. Сачков В.Н. Введение в комбинаторные методы дискретной математики/ В.Н.Сачков. - М.: МЦНМО, 2004. – 421 с.

62. Котов В. Е. Сети Петри. 1984. – с. 31-35.

63. Бандман О. Л. Сети Петри и корректность протоколов передачи данных // Вычислительные системы: Сб. науч. тр. – Новосибирск, 1985. – Вып. 109. – С. 29–51.

64. Руднев В. В. Словарные сети Петри // Автоматика и телемеханика. – 1987. – № 4. – С. 102–108.

65. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М.: Высшая школа, 1998, с. 44, 52, 76.

66. Гмурман В.Е. Теория вероятностей и математическая статистика. М.: Высшая школа, 1977, с. 56, 64, 83.

67. Дынкин Е.Б. «Марковские процессы», Москва, Государственное издательство физико-математической литературы, 1983, с. 87, 121, 249.

68. Кибзун и др. Теория вероятностей и математическая статистика. базовый курс с примерами и задачами. М.: Физматлит, 2002. - 224 с.

69. Математическая статистика: Учеб. для вузов / В. Б. Горяинов, И. В. Павлов, Г. М. Цветкова, О. И. Тескин.; Под ред. В.С. Зарубина, А.П.

Крищенко. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2001. 424 с. (Сер. Математика в техническом университете; Вып. XVII).

70. Баврин И.И. Теория вероятностей и математическая статистика - М.: Высш. шк., 2005.— 160 с .

71. Дынкин Е.Б. «Марковские процессы», Москва, Государственное издательство физико-математической литературы, 1983, с. 87, 121, 249.

72. Орлов А.И. «Цветные сети Петри», Москва, МЗ- Пресс, 2004, с. 236, 98, 32.

73. Семенов Д., Лисицын А. Управление рисками // Технология защиты банковских систем. - 2006. - № 9. - С.17-19.

74. Симонов С. Методология анализа рисков в информационных системах. //Конфидент, № 1, 2001.

75. Петренко С.А. Метод оценивания информационных рисков организации. / С.А. Петренко, А.А. Петренко. // сб.статей «Проблемы управления информационной безопасностью» под ред. д.т.н., профессора Черешкина Д.С., РАН ИСА, - М., Едиториал УРСС, 2002. - С.112-124.

76. Г. Тейл. Экономические прогнозы и принятие решений. М.: «Прогресс» 1970.-с.21-28.

77. Литвак Б. Г. Разработка управленческого решения – М.: Издательство «Дело», 2004 г. – с . 392.



8 (952) 106-88-60



vk.com/a.projectit



a.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



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT