**Реферат**

Отчёт 52 с., 7 ч., 4 рис., 8 табл., 7 источников.

ПРОЦЕССИНГ БАНКОВСКИХ КАРТ, ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРЫ, СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, НАДЁЖНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Объектом исследования является выбор организационных и технических мер защиты информации и повышения надёжности информационной системы процессинга банковских карт.

Цель работы – разработка методики выбора мер защиты информации и повышения надёжности информационной системы на базе методов управления рисками и теории надёжности.

В процессе работы проводились теоритические исследования и расчёты экономической целесообразности применения ряда мер защиты информации в условиях информационной системы процессинга банковских карт.

В результате был выбран набор мер защиты информации и повышения надёжности информационной системы. Для каждой меры рассчитан период окупаемости и показана целесообразность применения.

Степень внедрения – аналогичные методы выбора и обоснования мер повышения надёжности применялись для проектирования ряд информационных систем.

**Содержание**

Введение……………………………………………………………………………………...7

1. Описание объекта защиты………………………………………………………………8

2. Инвентаризация активов………………………………………………………………...10

2.1 Описание технологических и бизнес-процессов процессинга………………………11

2.2 Рассмотрение бизнес-процессов как особого вида активов…………………………18

2.3 Показатели непрерывности бизнес-процессов……………………………………….21

3.Модели угроз////////////……………………………………………………………….……23

4. Оценка рисков информационной безопасности……………………………………….26

5.Методики расчёта показателей надёжности информационной системы…………….30

6.Расчёт текущих показателей надёжности информационной системы и их влияние на результативность бизнес-процессов………………………………………………………37

7.Разработка и обоснование мер минимизации выявленных рисков………………….43

Заключение………………………………………………………………………………….50

Список использованных источников……………………………………………………..51

**Определения, обозначения и сокращения**

* + - 1. Актив (англ. asset) - все, что имеет ценность для организации и находится в ее распоряжении или то, что обладает ценностью или полезностью для организации, в том числе бизнес и технологические процессы[1].
      2. Угроза (безопасности информации): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [3].
      3. Риск - сочетание вероятности нанесения ущерба и тяжести этого ущерба. Потенциальная возможность использования уязвимостей активов организации угрозами ИБ для причинения ущерба организации, измеряемая с учетом вероятности реализации угроз ИБ и величины ущерба от реализации угроз ИБ[5].
      4. Источник угрозы ИБ: субъект (физическое лицо, материальный объект или физическое явление), активизирующий угрозу ИБ и переводящий ее из разряда потенциальной опасности нарушения свойств ИБ (конфиденциальности, доступности, целостности и т. д.) активов организации в реально происходящее нарушение этих свойств[4].
      5. Угроза ИБ (англ. information security threat): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения свойств ИБ – конфиденциальности, доступности и/или целостности информации/информационных активов организации[4].
      6. Уязвимость(информационной системы) (англ. vulnerability); брешь: - Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации. [3].
      7. Межсетевой экран: локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) автоматизированной системы[5].
      8. Бизнес-процесс: множество из одной или нескольких упорядоченных во времени, логически связанных и завершенных видов деятельности, в совокупности поддерживающих деятельность организации и реализующих ее политику, направленную на достижение поставленных целей.
      9. Доступность: свойство информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно (англ. availability)[5].
      10. Конфиденциальность: свойство, обеспечивающие недоступность или не раскрываемость информации для неавторизованного субъекта, устройства или процесса (англ. confidentiality)[5].
      11. Ба́нковская ка́рта — пластиковая карта, привязанная к одному или нескольким расчетным счетам в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных. Карты бывают дебетовые и кредитные. Дебетовые карты используются для распоряжения собственными деньгами, находящимися на расчетном счете в банке. Кредитные карты используется для распоряжения деньгами банка, которые при совершении платежа автоматически берутся у банка в кредит (их требуется вернуть банку).
      12. Linux, Apache, MySQL, PHP – операционная система, web сервер, система управления реляционными базами данных и интерпретируемый язык программирования. Популярны в России, встречаются в реально существующих процессингах.
      13. Процессинг – компания или подразделение банка занятое обработкой данных банковских карт. Часть информационной системы банка ответственная за обработку данных банковских карт.
      14. Ssh, telnet, rdp, Https, SOAP, nx – протоколы обмена данными широко применяемые в сети интернет.
      15. Мерчант – организация или лицо, клиент процессинга.
      16. DDOS – распределённая атака, направленная на отказ в работе сервиса. Обычно путём исчерпания аппаратных ресурсов.
      17. Изделие: Любая функциональная единица, которую можно рассматривать в отдельности [2].
      18. Уровень разукрупнения (для технического обслуживания): Уровень разделения изделия на составные части с точки зрения операций технического обслуживания [2].
      19. Восстанавливаемое изделие: Изделие, которое при данных условиях после отказа может быть возвращено в состояние, в котором оно может выполнять требуемую функцию[2].
      20. Сервис (в технике): Набор функций, предлагаемых пользователю [2].
      21. Эффективность применения: Способность удовлетворять требованиям к услуге с заданными количественными характеристиками [2].
      22. Возможность (в области надежности в технике): Способность изделия при оказании услуг удовлетворять запросам с заданными количественными характеристиками при данном внутреннем состоянии [2].
      23. Надежность: Свойство готовности и влияющие на него свойства безотказности и ремонтопригодности, и поддержка технического обслуживания [2].
      24. Работоспособное состояние: Состояние изделия, при котором оно способно выполнить требуемую функцию при условии, что предоставлены необходимые внешние ресурсы [2].
      25. Неработоспособное состояние: Состояние изделия, при котором оно неспособно выполнить требуемую функцию по любой причине [2].
      26. Продолжительность неработоспособного состояния: Интервал времени, в течение которого существует неработоспособное состояние [2].
      27. Отказ: Потеря способности изделия выполнить требуемую функцию [2].
      28. Критерий отказа: Заранее оговоренные признаки нарушения работоспособного состояния, по которым принимают решение о факте наступления отказа [2].
      29. Независимый отказ: Отказ, не вызванный прямо или косвенно другим отказом или неисправностью [2].
      30. Ценность – значение, представляемое продуктом/услугой для удовлетворения той или иной потребности субъекта, производящего оценку [2].

**Введение**

В настоящий момент в России рынок платежей при помощи различных видов банковских карт переживает период роста. Банковские карты становятся обычным, общеупотребимым средством оплаты.

Также растёт число и ущерб от мошенничеств с банковскими картами. Являясь удобными средствами оплаты покупок в интернете, карты также являются привлекательной целью для злоумышленников.

Клиенты банков ожидают, что банковские карты станут столь же надёжным безопасным средством оплаты, как и наличные средства. Достигнуть ожидаемого клиентами уровня надёжности и доступности платёжных сервисов возможно только при помощью современных научных подходов к выбору средств защиты информации.

Целью данной работы является – Повышение эффективности функционирования комплекса средств обеспечения информационной безопасности и надёжности системы процессинга банковских карт.

В данной работе будет произведена попытка минимизации рисков информационной безопасности основанная на общепринятых методах управления рисками и теории надёжности. Но с учётом специфики индустрии банковских карт.

В настоящий момент уже существует хорошо проработанный и ориентированный на практическое применение набор стандартов безопасности индустрии банковских карт: PCI-DSS. Данная работа не ставит своей целью разработку новых или критику существующих стандартов. Во всех рассуждениях предполагается, что все меры описанные в PCI-DSS уже применены. Рассматриваются некоторые их расширения и возможности более строгой реализации.

Для достижения заявленных целей необходимо рассмотреть информационную систему процессинга, произвести инвентаризацию активов, моделирование угроз и нарушителей. После моделирование угроз и инвентаризации активов произвести анализ рисков, и по его результатам осуществить выбор организационных и технических мер защиты информации.

1. **Описание объекта защиты**

Для придания большей определённости дальнейшим рассуждениям необходимо кратко описать информационную систему компании занятой обработкой данных банковских карт. Данное описание не будет содержать сведений об «офисной» составляющей. Единственной целью данного описания является предоставление всех необходимых для дальнейшего анализа сведений. Кроме того предполагается, что уже применены все необходимые в соответствии с PCI DSS меры безопасности. Также предполагается, что все компоненты информационной системы размещены в центре обработки данных с гарантированным электропитанием, и физическими условиями исключающими возможность выхода из строя оборудования.

В качестве стандартной среды на всех серверах установлена операционная система Debian Linux, применяется web сервер apache, интерпретатор php и система управления базами данных MySQL. Единственным средством удалённого управления серверами и активным сетевым оборудованием является протокол ssh, Удалённая работа с прикладными приложениями, имеющими графический пользовательский интерфейс, строится на основе протокола nx. Обмен информацией, не предназначенной для непосредственного восприятия человеком, происходит при помощи SOAP сообщений через HTTPS или обменом CVS файлами через sftp. Таким образом происходит информационный обмен с банками, иными платёжными системами и клиентами. Ещё раз отметим - все сервера размещены в удалённом центре обработки данных, сертифицированном в соответствии со стандартом PCI-DSS и Tier 4.

Также для дальнейших рассуждений введём краткий список серверов и активного сетевого оборудования входящих в состав рассматриваемой информационной системы:

* Сервер приложений. Выполняет роль шлюза для приёма соединений от клиентов мерчантов, и информационного обмена с банками, иными платёжными системами и клиентами. Извне доступен как http, https и ssh сервер. Прикладное программное обеспечения процессинга, исполняемое на сервере может выступать в качестве http, https и ssh клиента. На нём исполняется основная часть приложения процессинга, написанная на php.
* Сервер баз данных. Поддерживает систему управления базами данных MySQL. Из вне недоступен. Доступен с сервера приложений через протокол MySQL.
* Технологический терминальный сервер. На нём происходит настройка серверов, активного сетевого оборудования и доработка программного обеспечения процессинга, для этого установлен php, apache и MySQL. С данного сервера через протокол ssh доступны все остальные узлы и сетевое оборудование.
* Терминальный сервер. Используется техническим персоналом для доступа к ресурсам сети интернет, работы с электронной почтой и редактирования документов. Для этого установлен сервер электронной почты postfix, NX сервер и средства работы с документами.
* Ethernet коммутатор. Объединяет все сервера и активное сетевое оборудование процессинга в локальную сеть.
* Межсетевой экран. Осуществляет межсетевое экранирование на границе локальной сети процессинга и интернет. Весь входящий и исходящий траффик процессинга проходит через него.
* Терминалы. Оконечные устройства, предназначенные для доступа технического персонала в серверам и активному сетевому оборудования процессинга. Выступаю в качестве http, https, ssh и NX клиентов.
* Система хранения данных. Является единственным средством постоянного хранения информации. Базы данных, разработанные программный код, архив электронной почты – всё хранится на ней.

Резервное копирование информации со всех серверов выполняется еженедельно. В качестве хранилища резервных копий выступает жёсткий диск терминального сервера.

Все сервера существуют в единичных экземплярах. Ни один из элементов серверов не имеет резервирования. Средства переноса приложений, прикладного программного обеспечения и настроек между серверами отсутствуют. Исключением являются терминалы используемые техническим персоналом процессинга – они полностью идентичны и взаимозаменяемы.

1. **Инвентаризация активов**

Обработку данных банковских карт, возможно, рассмотреть как совокупность нескольких связанных бизнес-процессов.

Вся деятельности процессинга начинается с подключения нового клиента - мерчанта. Мерчантом называют компанию продающую товары или услуги в сети интернет и принимающей банковские карты к оплате. Бизнес процессы, технологические процессы, и особенности архитектуры информационной системы мерчанта обычно несовместимы напрямую с аналогичными сущностями банка. Это приводит с одной стороны к невозможности непосредственного взаимодействия с автоматизированной банковской системой, с другой к необходимости в существовании информационного посредника – процессинга. Задачей посредника является предоставление возможности взаимодействия информационной системы мерчанта с автоматизированными системами банков таким, образом, чтобы у мерчанта появилась возможность принимать к оплате банковские карты. На входе данного процесса находится поток заявок от клиентов. На выходе – набор заявок к техническому персоналу по разработке или доработке программного обеспечения процессинга.

Вторым бизнес-процессом процессинга является разработка или доработка программного обеспечения процессинга. Обычно для этого создаётся группа технических специалистов занятая разработкой программного обеспечения и эксплуатаций информационной системы процессинга. Результатом данного процесса является программный код и настройки компонентов информационной системы предназначенной для обработки банковских карт.

Третьим бизнес-процессом является собственно процесс обработки данных банковских карт. Данный бизнес-процесс во многом совпадает с технологическим процессом обработки информации о банковских картах поступающей от мерчантов и их клиентов. Кратко его возможно описать как получение нужной информации через сеть интернет и набор платёжных шлюзов. Проверку волосности полученной информации. Архивирование нужных сведений. Аккумуляция полученной информации со справочными данными, например курсами валют и формирование в результате сообщений данных и электронных платёжных поручений в формате принятом в участвующих во взаимодействии банках и платёжных системах.

Четвёртым бизнес процессом является процесс взаиморасчётов процессинга банковских карт с банками и иными платёжными системами. Результатом выполнения данного процесса является своевременные взаиморасчёты между процессингом банковских карт, банками и иными платёжными системами. Процессинг банковских карт может не является и не принадлежать банку. В то же время мерчанты ведут безналичные расчёты через банки и иногда через вне банковские платёжные системы. Процессинг банковских карт во многом необходим именно как посредник для организации взаимодействия между клиентами мерчантов, банками, мерчантами и вне банковскими платёжными системами. Ценность услуг процессинга как раз и состоит в организации и поддержании данного взаимодействия.

После рассмотрения бизнес-процессов нетрудно выделить основные информационные активы компании занятой обработкой данных банковских карт:

* Данные банковских карт;
* Персональные данные держателей карт;
* Денежный поток, проценты от которого формируют доход процессинга;
* Программное обеспечение, применяемое для обработки данных банковских карт.

Проведём приблизительную оценку активов. Данные необходимые для данной оценки получены в ходе неформального общения с представителями ряда российских банков:

* Средний остаток на карточном счёте физического лица – порядка 100 тысяч рублей;
* Среднее количество транзакций, совершаемое за сутки – 100000;
* Средняя величина транзакции – 1000 рублей;
* В среднем 1 из 10000 транзакций имеет мошеннический характер;
* Приблизительная численность уникальных физических лиц, чьи данные находятся в оперативной обработке – 20000 человек;
* Стоимость персональных данных одного пользователя из России – 10000 рублей;
* Стоимость работы квалифицированного программиста – 100000 рублей в месяц;
* Трудозатраты на разработку и доработку программного обеспечения процессинга составляют около 30 человеко-лет или 360 человеко-месяцев.

Следует уточнить, что после завершения оперативной обработки данные банковской карты должны быть переданы в архив в зашифрованном виде. Мы будем считать хранение в архиве надёжным.

Под стоимостью персональных данных понимается сумма иска, который может быть предъявлен за их утечку или ненадлежащую обработку. К сожалению судебная статистика по данному вопросу пока отсутствует, поэтому данная переменная получена полностью эвристическим путём.

Применяя полученные цифры можно легко рассчитать:

* Стоимость данных банковских карт находящихся в оперативной обработке – 20000 карт умножаем на 100000 рублей, получаем 2000000000 рублей;
* Стоимость данных банковских карт проходящих через процессинг в течении суток - 100000 карт умножаем на 100000 рублей, получаем 10000000000 рублей;
* Стоимость персональных данных пользователей, чьи банковские карты находятся в оперативной обработке – 20000 карт умножаем на 10000 рублей, получаем 200000000 рублей;
* Стоимость программного обеспечения – 100 тысяч рублей за один человеко-месяц умножаем на 360 человеко-месяцев, получаем 36000000 рублей;
* Стоимость денежного потока - 100000 транзакций в сутки умножаем на 1000 рублей, получаем 100000000 рублей в сутки или 36000000000 рублей в год. При условии, что процессинг берёт 5% с каждой транзакции – 1800000000 рублей в год выручки.

Суммирую сказанное, возможно составить предварительное представление о стоимости информационных активов процессинга.

Таблица 1. Предварительные сведения о стоимости активов

|  |  |
| --- | --- |
| **Активы** | **Стоимость** |
| Данные банковских карт | 10 млрд рублей |
| Персональные данные держателей карт | 200 млн рублей |
| Денежный поток, проценты от которого формируют доход процессинга | 36 млрд рублей |
| Программное обеспечение, применяемое для обработки данных банковских карт | 36 млн рублей |

**2.1 Описание технологических и бизнес-процессов процессинга**

Приведённые ранее рассуждения позволяют выявить, идентифицировать и оценить целый ряд активов, однако этот перечень не полон. Как уже упоминалось основная ценность услуг процессинга для мерчантов и их клиентов состоит в организации информационного взаимодействия. Информационное взаимодействие возможно только при условии успешного прохождения всех описанных бизнес-процессов. Из этого следует, что бизнес-процессы также ценны для компании занятой обработкой банковских карт и также являются активами.

В целях составления полного перечня всех активов процессинга необходимо проанализировать имеющиеся бизнес-процессы, определить те их параметры, которые важны для клиентов процессинга и получить количественную оценку указанных параметров.

Деятельность процессинга мы рассматриваем как связанную цепочку четырёх бизнес-процессов:

* Подключение или отключение мерчанта;
* Доработка программного обеспечения процессинга;
* Процесс обработки данных банковских карт;
* Процесс расчёта с банками и иными платёжным системами.

Вся деятельности процессинга начинается с подключения нового клиента - мерчанта. Мерчантом называют компанию продающую товары или услуги в сети интернет и принимающей банковские карты к оплате. Бизнес процессы, технологические процессы, и особенности архитектуры информационной системы мерчанта обычно несовместимы напрямую с аналогичными сущностями банка. Это приводит с одной стороны к невозможности непосредственного взаимодействия с автоматизированной банковской системой, с другой к необходимости в существовании информационного посредника – процессинга банковских карт. Задачей посредника является предоставление возможности взаимодействия информационной системы мерчанта с автоматизированными системами банков таким, образом, чтобы у мерчанта появилась возможность принимать к оплате банковские карты. На входе данного процесса находится поток заявок будущих мерчантов. На выходе – набор задач техническому персоналу по изменению настроек программного обеспечения процессинга и предоставления реквизитов подключаемому клиенту. Целью процесса является подключение или отключение клиента в максимально короткие сроки. Заявки поступают при помощи электронной почты на терминальный сервер (он же сервер электронной почты). На этом же узле технический персонал процессинга принимает сообщения электронной почты, в том числе заявки на подключение новых клиентов. Получив заявку, системные администраторы подключается к технологическому терминальному серверу. Далее системные администраторы в режиме удалённого управления изменяют настройки межсетевого экрана, сервера приложений, прикладного программного обеспечения сервера и приложений.

Структура данного бизнес-процесса показана на рисунке 1.



Рисунок 1. - Процесс «Подключение или отключение мерчанта»

Вторым бизнес-процессом процессинга является разработка или доработка программного обеспечения процессинга. На входе данного процесса находится поток заявок на доработку программного обеспечения процессинга. Заявки создаются техничесим персоналом процессинга, в том случае если имеющийся функционал недостаточен для подключения нового мерчанта или организации взаимодействия с банком или иной платёжной системой. Результатом данного процесса являются новые, установленные и подготовленные к работе релизы программного обеспечения процессинга. Целью процесса является создание программного кода реализующего необходимую клиенту функциональность в максимально короткие сроки. Заявки на разработку и доработку программного обеспечения поступают при помощи электронной почты на терминальный сервер (он же сервер электронной почты). На этом же узле технический персонал процессинга принимает сообщения электронной почты, в том числе заявки на подключение новых клиентов. Получив заявку, программисты подключается к технологическому терминальному серверу. Разработка нового кода производится на нём в специальной тестовой среде. Сборка новой версии прикладного программного обеспечения процессинга происходит автоматически. Собранное приложение передаётся на сервер приложений. Также программисты в режиме удалённого управления изменяют настройки сервера приложений, прикладного программного обеспечения сервера и приложений и сервера баз данных.

Структура данного бизнес-процесса показана на рисунке 2.



Рисунок 2. - Процесс «Доработка программного обеспечения»

Третьим бизнес-процессом является собственно процесс обработки данных банковских карт. Данный бизнес-процесс во многом совпадает с технологическим процессом обработки информации о банковских картах поступающей от мерчантов и их клиентов. Кратко его возможно описать как получение нужной информации через сеть интернет и набор платёжных шлюзов. Проверку корректности полученной информации. Обработка и аккумуляция полученной информации со справочными данными, например курсами валют. Архивирование нужных сведений. Формирование запросов на проведение расчётов с банками, иными платёжными системами и ответные сообщения для мерчантов. На входе данного процесса находится поток сообщений данных или заявок от клиентов мерчантов. На выходе ответные сообщения, предназначенные для информирования клиентов мерчантов и программного обеспечения клиентов процессинга о статусе транзакции и заявки на проведения расчётов с банками и иными платёжными системами. Целью процесса является обработка максимально большого количества запросов на оплату при помощи банковских карт. Запросы на проведения транзакций поступают от клиентов из сети интернет, проходят межсетевой экран, обрабатываются сервером приложений в взаимодействий с сервером баз данных.

Структура данного бизнес-процесса показана на рисунке 3.



Рисунок 3. - Процесс обработки данных банковских карт

Процесс расчёта с банками и иными платёжным системами. На входе данного процесса находится поток заявок на проведение расчётов. Информация из заявок проверяется на корректность, обрабатывается, объединяется с справочными данными, например курсами валют. Производится архивация необходимых сведений, и формируются сообщения данных в формате пригодном для обмена с информационными системами банков. Целью процесса является проведение всех необходимых расчётов не позднее заранее заданных сроков. В процессе расчёт участвует сервер приложений в взаимодействии с сервером баз данных. Все информационные взаимодействия с банками и иными платёжными системами производятся через интернет через межсетевой экран.

Структура данного бизнес-процесса показана на рисунке 4.



Рисунок 4. - Процесс расчёта с банками и иными платёжным системами

**2.2 Рассмотрение бизнес-процессов как особого вида активов**

Ведём количественные показатели результативности рассмотренных бизнес-процессов.

Целью процесса «Обработка данных банковских карт» является обработка максимально большого количества запросов на оплату. Результатом выполнения данного процесса является осуществление платежа клиентом мерчанта при помощи его банковской карты.

Оценим результативность данного бизнес- процесса количественно.

* Среднее количество транзакций, совершаемое за сутки – 100000;
* Средняя величина транзакции – 1000 рублей;

Процессинг берёт в качестве комиссии 5% от суммы транзакции.

Тогда в течении года данный процесс приносит выручку в размере 1800000000 рублей.

Бизнес-процесс «Подключение или отключение мерчанта» имеет своей целью подключение или отключение клиента в максимально короткие сроки. Результатом выполнения данного процесса является изменение статуса мерчанта.

Будем считать, что у компании десять тысяч клиентов. В среднем каждый клиент приносит 0,01% выручки. Клиенты крайне редко отказываются от услуг. Новые клиенты приходят с интенсивностью 30 обращений в сутки. Тогда исходя из того, что выручка компании составляет 1800000000 рублей в год, или 5000000 рублей в сутки, подключение новых клиентов приносит 15000 рублей выручки в сутки или 5400000 рублей в год.

Целью бизнес-процесс «Доработка программного обеспечения процессинга» является создание программного кода реализующего необходимую клиенту функциональность в максимально короткие сроки. Результатом выполнения данного процесса является создание программного обеспечения реализующего изложенные в заявке и техническом задании функции. Обращений на разработку или доработку программного обеспечения поступают со средней интенсивностью – одно в сутки. Доработка или разработка программного обеспечения производится только при условии, что клиент приносит более 10000 рублей комиссии в сутки. Тогда доработка программного обеспечения 10000 рублей выручки в сутки или 3600000 рублей в год.

Бизнес-процесс «Расчёт с банками и иными платёжным системами» имеет цель проведение всех необходимых расчётов не позднее заранее заданных сроков. Непосредственно данный процесс выручки не приносит. Расчёты не реже одного раза в сутки. В случае нарушения сроков расчётов на процессинг накладываются штрафные санкции в размере одного процента от суммы просроченных расчётов за каждые сутки.

Несмотря на то, что данный бизнес-процесс непосредственно не участвует в формировании выручки, его успешное выполнение является необходимым условием функционирования процессинга. Мерчанты обращаются к услугам компании занятой обработкой данных банковских карт именно по причине необходимости в посреднике способном организовать и поддерживать взаимодействие с банками. В ином случае процессинг для них является только лишним посредником между участниками платежа. Таким образом мы можем рассматривать данный бизнес процесс как естественное продолжение бизнес-процесса «Обработка данных банковских карт» и приписать ему некую часть стоимости последнего. Разумным является разделение ценности бизнес процесса «Обработка данных банковских карт» с ценностью процесса «Расчёт с банками и иными платёжным системами» в равных далях.

Суммируя сказанное возможно утверждать, что все указанные бизнес-процессы являются активами. Стоимости этих активов приведены в таблице 2.

Таблица 2. Стоимость бизнес-процессов

|  |  |
| --- | --- |
| **Активы** | **Стоимость** |
| «Обработка данных банковских карт» | 900 тыс. рублей |
| «Подключение или отключение мерчанта» | 5,4 млн. рублей |
| «Доработка программного обеспечения процессинга» | 3,6 млн рублей |
| «Расчёт с банками и иными платёжным системами» | 900 тыс. рублей |

Соединив две таблицы вместе возможно получить общий перечень активов подлежащих защите вместе с их стоимостью. Данные сведения приведены в таблице 3.

Таблица 3. Стоимость активов

|  |  |
| --- | --- |
| **Активы** | **Стоимость** |
| Данные банковских карт | 10 млрд рублей |
| Персональные данные держателей карт | 200 млн рублей |
| Денежный поток, проценты от которого формируют доход процессинга | 36 млрд рублей |
| Программное обеспечение, применяемое для обработки данных банковских карт | 36 млн рублей |
| «Обработка данных банковских карт» | 900 тыс. рублей |
| «Подключение или отключение мерчанта» | 5,4 млн рублей |
| «Доработка программного обеспечения процессинга» | 3,6 млн рублей |
| «Расчёт с банками и иными платёжным системами» | 900 тыс. рублей |

**2.3 Показатели непрерывности бизнес-процессов**

Целью данной работы является выбор организационных и технических мер направленных на повышение уровня безопасности и надёжности информационной системы компании занятой обработкой данных банковских карт. Правильный выбор мер защиты строится, в том числе и на нарушение каких свойств безопасности направлены угрозы. Для информации или данных, обычно предполагается нарушение целостности, доступности или конфиденциальности. Необходимо ввести аналогичные атрибуты и для бизнес-процессов рассматриваемых как активы. Разумным является введение аналогичных свойств исходя из теории непрерывности бизнеса.

Целью анализа и изучения непрерывности является повышение эффективности и результативности бизнес бизнес-процессов. Нарушение непрерывности приводит к снижению результативности, повышению расхода ресурсов и уменьшению эффективности.

Ведём количественные показатели непрерывности рассмотренных бизнес-процессов.

Целью процесса «Обработка данных банковских карт» является обработка максимально большого количества запросов на оплату товаров или услуг. Чем быстрее будет обработан каждый запрос тем более удовлетворены будут клиенты мерчантов и сами мерчанты. Кроме того, чрезмерно большая продолжительность ожидания обработки данных банковской карты и прохождения платежа может привести к тому что держатель карты откажется от покупки и от использования интернет-магазина принадлежащего мерчанту. Недоступность сервиса также может привести к аналогичным результатам. Разумно предположить, что для данного сервиса будут иметь смысл следующие показатели:

* максимальное время, за которое будет предоставлен сервис;
* коэффициент готовности сервиса;
* максимальное время до восстановления предоставления сервиса.

Бизнес-процесс «подключение или отключение мерчанта» имеет своей целью подключение или отключение клиента в максимально короткие сроки. От быстроты подключения нового клиента зависит то как скоро он сможет приступить к активной деятельности, к продаже товаров или услуг и то как скоро процессинг начнёт получать свою комиссию. Разумно предположить что для данного сервиса будут иметь смысл следующие показатели:

* максимальное время, за которое будет произведено подключение клиента;
* коэффициент готовности сервиса;
* максимальное время до восстановления предоставления сервиса.

Целью бизнес-процесс «Доработка программного обеспечения процессинга» является создание программного кода реализующего необходимую клиенту функциональность в максимально короткие сроки. Разумно предположить что для данного сервиса будут иметь смысл следующие показатели:

* максимальное время, за которое будет выполнена заявка на создание программного кода;
* коэффициент готовности сервиса;
* максимальное время до восстановления предоставления сервиса.

Бизнес-процесс «Расчёт с банками и иными платёжным системами» имеет цель проведение всех необходимых расчётов не позднее заранее заданных сроков. Расчёты не реже одного раза в сутки. В случае нарушения сроков расчётов на процессинг накладываются штрафные санкции в размере одного процента от суммы просроченных расчётов за каждые сутки.

Разумно предположить что для данного сервиса будут иметь смысл следующие показатели:

* максимальное время, за которое будет предоставлен сервис;
* коэффициент готовности сервиса;
* максимальное время до восстановления предоставления сервиса.

Интересующие нас в данной работе показатели непрерывности рассматриваемых бизнес-процессов практически идентичны. Дополнив их необходимым в дальнейшем показателем «количество отключений в год» можно сказать что для всех бизнес-процессов целесообразно рассчитывать:

* Количество отключений в год;
* Максимальное время, за которое будет предоставлен сервис превысит 31 часов;
* Коэффициент готовности сервиса равен 0,9919;
* Минимальное и максимальное время восстановления;
* Максимальное время простоя в связи с длительными отключениями.

1. **Модели угроз**

Выделив активы, возможно, найти направленные на них угрозы. Следует только сопоставить возможные источники угроз с активами и исключить невозможные физически сочетания.

В качестве источников угроз мы будем рассматривать:

* Отказы аппаратуры;
* Ошибки персонала;
* Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью;
* Внешние нарушители.

Стихийные бедствия не вошли в данный список, по той причине, что центры обработки данных прошедшие проверку на соответствие требованиям PCI DSS имеют высокую степень защиты от всех природных и техногенных катастроф, которые могут произойти в их окружении. Также мы считаем, что применяемые средства проыверки лояльности и контроль за действиями делает надёжным и не несущим угрозы персонал центра обработки данных.

Внутренние и внешние нарушители могут быть источниками угрозы прекращения обработки карточных данных. Также они могут нарушать конфиденциальность данных банковских карт, персональных данных клиентов мерчантов или пытаться скопировать исходный код программного обеспечения процессинга.

Возможно, предположить, что внешние нарушители могут пытаться прекратить процесс обработки данных банковских карт при помощи атаки на отказ в обслуживании. Скорее всего, это будет распределённая атака на отказ в обслуживании. Стандарт PCI DSS требует применения межсетевых экранов с целью исключения доступа извне в сеть, где обрабатываются карточные данные, кроме как к необходимым сервисам. Исходя из этого мы можем свести угрозу прекращения обработки карточных данных исходящую от внешних нарушителей к возможности DDOS атаки платёжные шлюзы. Или к получению на них возможности исполнять произвольный код.

Внутренние нарушители могут получить доступ к данным банковских карт, персональным данным или коду программного обеспечения процессинга при помощи стандартных средств удалённого управления – ssh, telnet, rdp. Применение иных протоколов, возможно, ограничить при помощи межсетевых экранов.

Угрозой направленной на возможность получения оплаты за предоставленные услуги процессинга (Денежный поток, проценты от которого формируют доход процессинга) являются фродовые т.е. мошеннические транзакции инициированные внешними нарушителями. При помощи кражи персональных данных и данных банковских карт внешние нарушители могут пытаться купить товары или услуги предоставляемые клиентами процессинга. Владельцы украденных карт, обнаружив кражу денежных средств, откажутся оплачивать покупки совершённые злоумышленниками. Результатом этого будет отказ банка эмитента и расчётного центра принять транзакцию к обработке и недополученные процессингом прибыли.

Взаимосвязь угроз и источников приведена ниже, в таблице 4:

Таблица 4. Взаимосвязь угроз и источников

|  |  |
| --- | --- |
| Угроза | Источники |
| Прекращение бизнес-процесса «Обработка данных банковских карт» | • Отказы аппаратуры; • Ошибки персонала; • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью; • Внешние нарушители. |
| Прекращение бизнес-процесса «Подключение или отключение мерчанта» | • Отказы аппаратуры; • Ошибки персонала; • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью. |
| Прекращение бизнес-процесса «Доработка программного обеспечения процессинга» | • Отказы аппаратуры; • Ошибки персонала; • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью. |
| Прекращение бизнес-процесса «Расчёт с банками и иными платёжным системами» | • Отказы аппаратуры; • Ошибки персонала; • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью. |
| Кража данных банковских карт | • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью; • Внешние нарушители. |
| Кража персональных данных клиентов | • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью; • Внешние нарушители. |
| Кража исходного кода программного обеспечения процессинга | • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью; • Внешние нарушители. |

Продолжение таблицы 4

|  |  |
| --- | --- |
| Потеря части денежного потока вследствие отказа банков оплачивать мошеннические транзакции | • Внешние нарушители. |

1. **Оценка рисков информационной безопасности**

Определив активы, угрозы и источники угроз информационной безопасности, возможно, перейти к количественной оценке рисков. Как уже было сказано риск - сочетание вероятности нанесения ущерба и тяжести этого ущерба. Потенциальная возможность использования уязвимостей активов организации угрозами ИБ для причинения ущерба организации, измеряемая с учетом вероятности реализации угроз ИБ и величины ущерба от реализации угроз ИБ. В данной работе, как в классической теории управления рисками информационной безопасности вообще рассматриваются чистые риски. Это обозначает, что риски приводят к убыткам или недополученной прибыли и не могут приводить к увеличению прибыли.

В качестве источника информации для численной оценки вероятности реализации угроз будут использованы ряд криминологических исследований, расчёты выполненные с применением методов теории надёжности и экспертное мнение научного консультанта.

Рассмотрим угрозу прекращения процесса «Обработка данных банковских карт». Данная угроза имеет четыре источника:

* Отказы аппаратного обеспечения;
* Ошибки персонала;
* Внешние злоумышленники;
* Внутренние злоумышленники.

Расчёт вероятности реализации отказа аппаратного обеспечения будет выполнен и подробно описан ниже в соответствующих разделах. Для предварительных рассуждений примем, что вероятность отказа аппаратуры характеризуется величиной называемой «наработка на отказ». Большинство производителей серверного оборудования указывают наработку на отказ около года непрерывной работы. Существуют производители, указывающие и большие значения данной величины. Учитывая, что информационная система рассматриваемой компании состоит из нескольких серверов, и выход из строя одного из них равносилен неработоспособности всей системы - будем считать значением данной величины – год непрерывной работы.

В случае выхода из строй сервера, потребуется, диагностика неисправности, замена вышедшего из строя блока, и перенастройка или переустановка аппаратного обеспечения. Будем считать, что на все указанные действия суммарно потребуются сутки. Для выполнения подобных действий в удалённом центре обработки данных это реалистичное предположение.

Под ошибками персонала будем понимать неправильно введённые настройки активного оборудования или ошибки в разрабатываемом программном обеспечении процессинга, которые приводят к его неработоспособности. Процесс обнаружения, выявления причины и устранения ошибок также может занимать длительное время. Разумно предположить, что подобные ситуации случаются как минимум раз в год и могут продолжаться до одних суток.

Внешние злоумышленники могут пытаться осуществить DDOS атаки. Как показывает практика априорная вероятность стать целью такой атаки составляет 0,1 в год. Средняя продолжительность атаки может достигать пары недель. Примем вероятность 0,1 и продолжительность атаки – 10 суток. В течение всего этого времени сервис обработки данных банковских карт предполагается недоступным.

Внешние злоумышленники могут использовать неизвестные поставщикам системного программного обеспечения уязвимости с целью остановки работы важных системных процессов и вызывания отказа в работе сервиса. Средний период между обнаружением уязвимости и выпуском исправлений, различается у разных поставщиков между несколькими днями и неделями и даже месяцами. Для стека Linux+Apache+Php он составляет около двух недель.

Для нас эта величина и характеризует период времени, на который злоумышленник сможет остановить работу процессинга. Примем вероятность подобной атаки 0,01 в течении года, срок выпуска исправления безопасности – 10 дней.

Суммируя произведения вероятностей на величину простоя получаем суммарное время простоя – 4 суток в год. Как уже говорилась – данная оценка примерна, и будет уточнена с учётом расчёта вероятности отказа аппаратного обеспечения с применением теории надёжности.

Применим аналогичный подход к оценки вероятностей реализаций угроз:

* Прекращение бизнес-процесса «Подключение или отключение мерчанта»;
* Прекращение бизнес-процесса «Доработка программного обеспечения процессинга»;
* Прекращение бизнес-процесса «Расчёт с банками и иными платёжным системами».

Для всех трёх перечисленных угроз множество источников идентично и включает в себя:

* Отказы аппаратуры;
* Ошибки персонала;
* Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью.

Из этого следует, что суммируя произведения вероятностей на величину простоя получаем суммарное время простоя для каждого бизнес-процесса – 3 суток в год.

Рассмотрим вероятность утечки данных банковских карт. Существует два источника данной угрозы:

* Внешние нарушители;
* Внутренние нарушители.

Предположим, что внешние нарушители используют неизвестные поставщикам системного программного обеспечения уязвимости с целью получения доступа к обрабатываемой на серверах информации. Как уже рассматривали средний период между обнаружением уязвимости и выпуском исправлений, для стека Linux+Apache+Php он составляет около двух недель. Вероятность подобной атаки 0,01. В результате можем сказать что злоумышленник «в среднем» сможет украсть данные банковских карт в объеме «дневного» траффика процессинга – 20 тысяч штук.

Вероятность того, что персонал процессинга станет учувствовать в махинациях с банковскими картами составляет около 0,01. Это крайне приблизительная экспертная оценка. Более точные данные можно получить только путём обследования конкретного коллектива. Учитывая тот факт, что данные после оперативной обработки отправляются в архив, где хранятся в защищённой криптографическими методами форме, внутренний нарушитель может получить доступ к ограниченному количеству информации – до 20 тысяч записей о банковских картах.

Аналогично возможно рассчитать вероятность и последствия кражи персональных данных физических лиц. Отличием будет гораздо более низкая мотивация злоумышленника. Тем более получив доступ к внутренним компонентам процессинга иррационально ограничить свою деятельность только персональными данными, не затронув информацию о платёжных картах.

Источником угрозы кражи исходного кода программного обеспечения процессинга является внутренний нарушитель. Программное обеспечение разрабатывается на отдельном сервере недоступном из сети интернет. Поэтому внешние нарушители могут быть исключены. По аналогии с предыдущим пунктом вероятность того, что персонал процессинга станет учувствовать в подобной махинации, составляет около 0,01.

Ещё одним активом, крайне важным для компании занимающейся обработкой данных банковских карт является поток денежных средств, состоящий из платежей клиентов мерчантов. Обработка информации об этих платежах составляет одну из основных задач процессинга, а отчисления мерчантов в виде определённого процента с выручки, полученной при помощи оплаты банковскими картами – выручку рассматриваемой компании. В среднем как минимум один платёж из ста является мошенническим. Источником данной угрозы являются внешние нарушители.

Взаимосвязь между активами, свойствами безопасности и вероятности реализации угроз показана в таблице 5.

Таблица 5. Взаимосвязь активов, и вероятности реализации угроз

|  |  |  |  |
| --- | --- | --- | --- |
| **Активы** | **Стоимость** | **Вероятность потери свойства безопасности** | **Средние потери от реализации рисков** |
| Сервис «Обработка данных банковских карт» | 900 млн рублей | 4 сутки простоя в год.  Вероятность – 1 | 10 млн рублей |
| Данные банковских карт | 10 млрд рублей | Вероятность 0,1  20 тысяч карт | 200 тыс. рублей |
| Сервис «Подключение или отключение мерчанта» | 5,4 млн рублей | 3 сутки простоя в год.  вероятность – 1 | 45 тыс. рублей |
| Сервис «Доработка программного обеспечения процессинга» | 3,6 млн рублей | 3 сутки простоя в год.  Вероятность – 1 | 30 тыс. рублей |
| Сервис «Расчёт с банками и иными платёжным системами» | 900 тыс. рублей | 3 сутки простоя в год.  Вероятность – 1 | 10 млн рублей |
| Персональные данные держателей карт | 200 тыс. рублей | Вероятность 0,001  Потеря информации о 20 тысячах субъектах | 20 тыс. рублей |
| Денежный поток, проценты от которого формируют доход процессинга | 36 млрд рублей | 0,01 процента транзакций фродовые | 360 млн рублей |
| Программное обеспечение, применяемое для обработки данных банковских карт | 36 млн рублей | Вероятность несанкционированного копирования 0,01 | 360 тыс. рублей |

1. **Методики расчёта показателей надёжности информационной системы**

Теория надёжности — наука, изучающая закономерности распределения отказов технических устройств, причины и модели их возникновения. Теория надёжности изучает методы обеспечения стабильности работы объектов (изделий, устройств, систем и т.п.) в процессе проектирования, производства, приёмки, эксплуатации и хранения. Устанавливает и изучает количественные показатели надёжности. Исследует связь между показателями эффективности и надёжности [6].

Базой математического аппарата теории надёжности являются:

* теория вероятностей;
* математическая статистика;
* математическая логика;
* теория случайных процессов;
* теория массового обслуживания;
* теория графов;
* теория оптимизации.

Одним из способов расчёта количественных показателей надёжности является логико-вероятностным методом. Под логико-вероятностным методом будем понимать метод расчета надежности технических систем, при котором структура системы описывается методами математической логики, а количественная оценка ее надежности производится с помощью теории вероятностей.

Это определение включает в себя и многие другие аналогичные методы (например, вероятностную оценку дерева неисправностей, метод анализа дерева отказов и др.), в которых рассматривались только структурные простые системы [6]. Однако современное состояние логико-вероятностных методов позволяет решить ряд проблем, связанных как с аналитическими методами исследования надежности структурно-сложных систем, так и с автоматизированным логико-вероятностным моделированием. При использовании логико-вероятностного метода процесс анализа надежности информационной системы начинается с изучения ее состава, принципа работы, функциональных связей между элементами и особенностей эксплуатации. Все множество состояний системы можно разделить на два подмножества - работоспособных и неработоспособных состояний. Такое разделение производится в соответствии с выбранным (или заданным) критерием отказа системы.

Критерий отказа есть признак или совокупность признаков неработоспособного состояния системы, установленные в нормативно-технической и (или) конструкторской документации.

Признаками неработоспособного состояния могут являться нарушение способности системы выполнять свое назначение или несоответствие значений ее выходных параметров заданным требованиям, установленным в документации на систему.

Примером критериев отказа системы могут быть:

* Недоступность предоставляемого системой сервиса;
* Невозможность получения сервиса за заданное время;
* Неспособность системы обрабатывать запросы с определённой скоростью.

Условия работоспособности формулируются для того, чтобы составить представление, при каких состояниях элементов, режимах их функционирования, условиях эксплуатации и т.д. информационная система будет находиться в работоспособном состоянии, а при каких - в неработоспособном. Условия работоспособности могут быть описаны словесно, графически или аналитически. Как правило, словесное описание предшествует построению графической логической модели, на базе которой осуществляется переход к аналитическому описанию. Этап графического описания имеет особое значение, т.к. является переходным этапом от неформального к формальному анализу, и от его качества зависит достоверность получаемых оценок показателей надежности системы. Этот переходный этап - самое ответственное звено в расчетах показателей надежности систем. Именно на этом этапе, как правило, принимаются все основные упрощающие окончательную модель допущения. Кроме того, могут возникнуть методические ошибки из-за замены функциональных связей между реальными элементами, логическими связями, учитывающими лишь некоторые возможные состояния системы. Ошибки, совершаемые на данном этапе, при дальнейших расчетах практически не обнаруживаются.

При графическом представлении условий работоспособности систем чаще всего применяют модели в виде структурной схемы надежности.

По структурной схеме надёжности определяют структурную функцию - работоспособности, либо дерево отказов, по которым определяют количественные показатели надежности - функцию надежности системы h(r). Этапы преобразования включают в себя:

* Функциональная и структурная схема;
* Структурная схема надёжности системы;
* Структурная функция или дерево отказов;
* Функция надёжности системы.

Под структурной схемой надежности понимают некоторую условную схему, учитывающую влияние элементов и особенно связей между ними на работоспособность системы в целом. В ходе ее составления анализируются возможные виды отказов элементов и влияние отказов элементов и их различных комбинаций на работоспособность системы. При этом функциональные элементы системы заменяются логическими элементами, принимающими значение либо 1, либо - 0, где 1 - соответствует работоспособному состоянию элемента, а 0 - неработоспособному, а функциональные связи заменяются логическими.

Важно, что разбивка системы на элементы должна учитывать удобства дальнейшего анализа как надежности элементов, так и надежности системы в целом. Из сказанного следует, что структурная схема надёжности может существенно отличаться от функциональной схемы этой же системы, учитывающей прохождение информации.

Чтобы проиллюстрировать структурную схему надёжности, рассмотрим небольшой фрагмент информационной сети, состоящий из трех линий связи (в общем случае разнотипных), соединяющих два абонента, представленный на рисунке 5.

В зависимости от требований, предъявляемых к данной сети, можно построить различные структурные схемы надёжности, в которых каждая линия представлена в виде элемента. Так, если необходима работа непременно всех трех линий, то структурная схема надёжности сети будет вид такой, как на рисунке 5 а. В этом случае структура рассматриваемой системы - последовательная. Если для успешной работы сети достаточно одной линии (неважно какой), то структурная схема надёжности будет такой, как на рисунке 5 б. В этом случае структура системы - параллельная. Если же для работы необходимо иметь минимум две из трех линий, то структурная схема надёжности будет иметь вид, изображенный на рисунке 5 в. В этом случае говорят, что система связи имеет конфигурацию "2 из З". Возможны и другие случаи, например, система считается работоспособной, если работоспособны непременно первая линия и любая из двух остальных. Структурная схема надёжности такой информационной системы приведена на рисунке 5 г и имеет последовательно-параллельную структуру. На рисунке 5 д приведена параллельная структурная схема надёжности, одна из ветвей которой представляет собой параллельное соединение элементов.

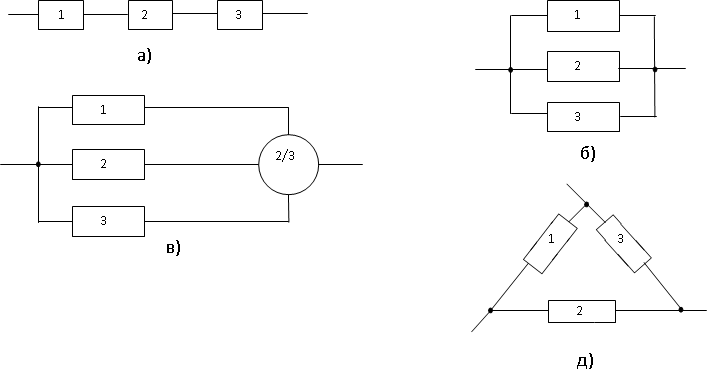


Рисунок 5. – Структурная схема надёжности

Таким образом, можно графически представить условия работоспособности различных вариантов систем через их структурные схемы надежности. На такой схеме все элементы системы в каком-то смысле равноценны, и это подчеркивается их одинаковым обозначением (одной и той же буквой Xi с различными номерами, произвольно присвоенными этим элементам) и одинаковым графическим изображением (в виде прямоугольника или кружка). Способ соединения элементов (не в физическом, а в функциональном смысле) и раскрывает условия работоспособности.

Аналогичным образом бинарная переменная у обозначает состо­яние системы yi = 1, если система работоспособна, 0, если система отказала. Предположим, что состояние системы определено полностью состоянием ее элементов, и будем далее записывать:

  (1)

Функция у(Х) принимает значение либо 1, либо 0 и связывает условия работоспособности элементов с работоспособностью всей системы. Тем самым мы предполагаем, что состояние системы в смысле работоспособности детерминировано зависит от состояния ее элементов. Функция y(X) является функцией от x1, x2, ......xn, которые, в свою очередь, могут находиться только в двух несовместных состояниях: либо 1 (работоспособное состояние), либо 0 ( состояние полного отказа) В целом это предположение является до некоторой степени условным и ограничительным, так как оно исключает (хотя и не полностью) возможность частичного функционирования системы. Однако оно обладает тем достоинством, что приводит к модели, которая имеет строгое аналитическое решение и является достаточно реальной.

Каждой структурной схеме надёжности можно сопоставить функцию алгебры логики, заменив связи между элементами х1, х2,... хn конъюнкциями и дизъюнкциями или иными действия алгебры логики. Такую функцию будем называть функцией алгебры логики. Каждой системе через структурную схему надёжности однозначно сопоставляется функция алгебры логики, которую будем называть функцией работоспособности системы или структурной функцией системы.

Основной трудностью в практическом применении логико-вероятностных методов исследования надежности и безопасности структурно-сложных систем является преобразование произвольных ранее рассмотренной функции алгебры логики в формы перехода к полному замещению, позволяющие рассчитывать вероятность нахождения системы в работоспособном состоянии. Чтобы сделать это преобразование направленным (стандартным) и математически строгим, необходимо было построить своеобразный “мостик” между алгеброй логики и теорией вероятностей.

В теории надежности существует большое число методов расчета надежности. Наиболее известны:

* метод разрезания;
* метод ортогонализации;
* рекуррентный метод;
* метод наращивания путей;
* схемно-логический метод.

1. **Расчёт показателей надёжности информационной системы и их влияние на результативность бизнес-процессов**

Аналитический метод расчета количественных показателей надежности информационной системы для конкретных бизнес-процессов.

Для определения показателей надёжности информационной системы аналитическим методом необходимо составить расчётную схему, описывающую соединения её элементов. При этом все описанные элементы, важны с точки зрения непрерывности рассматриваемого бизнес-процесса. Расчётная схема отражает логику связей между элементами с точки зрения надёжности работы информационной системы и непрерывности конкретного процесса.

Основные допущения аналитического расчета заключаются в следующем:

* Уровень разукрупнения исследуемой информационной системы выберем так чтобы наименьшей рассматриваемой единицей был сетевой узел. Сервера, терминалы, активное сетевое оборудование перечисленное в описание объекта защиты будем считать сетевыми узлами;
* Наименьшую рассматриваемую единицу будем считать восстановимым изделием;
* Будем считать что отказы независимы друг от друга;
* Для длительных отключений и неисправностей (ремонт, диагностика или замена элементов) рассматриваются также отказы параллельных цепей элементов информационной системы, вызванные наложениями повреждений одного элемента на аварийное восстановление другого и аварийных повреждений на плановые отключения;
* Аналитические расчёты основываются на предположении, что поток отказов элементов на расчетном промежутке – простейший, пуассоновский, а закон распределения вероятности восстановления – экспоненциальный.

Исходные данные необходимые для проведения дальнейших расчётов представлены в таблице ниже.

* – интенсивность случайного события (отказа);
* – время восстановления системы;
*  – коэффициенты планового простоя;
*  – коэффициенты аварийного простоя;
*  – удельная длительность планового ремонта (за 1 год).

Исходные данные выбраны исходя из обычной практики представления сведений о надёжности изделий со стороны поставщиков. Конкретные значения – получены путём экспертной оценки.

Таблица 6. Исходные данные для проведения расчётов надежности информационной системы

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Элемент | Общее количество | Минимально необходимое количество работоспособных единиц | , 1/год | , год |  |  |
| Сервер приложений | 1 | 1 | 1 | 0,001 | 0,003 | 2 |
| Сервер баз данных | 1 | 1 | 1 | 0,005 | 0,003 | 4 |
| Технологический терминальный | 1 | 1 | 1 | 0,003 | 0,003 | 1 |
| Терминальный сервер | 1 | 1 | 1 | 0,001 | 0,001 | 1 |
| Ethernet коммутатор | 1 | 1 | 0,5 | 0,001 | 0,001 | 0,5 |
| Межсетевой экран | 1 | 1 | 0,5 | 0,001 | 0,0001 | 0,5 |
| Терминалы | 10 | 1 | 0,02 | 0,001 | 0,0001 | 0,1 |
| Система хранения данных | 1 | 1 | 1 | 0,01 | 0,003 | 24 |

При сделанных допущениях для показателей надёжности элементов информационной системы справедливы следующие формулы теории надёжности. Для коэффициентов простоя:

Для последовательного соединения элементов, где  – интенсивность отказов

i-го элемента:

 (2)

Расчёт показателей надёжности для процесса «Подключение или отключение мерчанта» приведён ниже.

Для успешного прохождения процесса отключения или подключения нового мерчанта необходимо наличие работоспособного состояния у следующих элементов информационной системы:

* межсетевой экран;
* Ethernet коммутатор;
* Система хранения данных;
* терминальный сервер (он же сервер электронной почты);
* технологической терминальный сервер;
* сервера приложений.

Исходя из сказанного, кратковременные неисправности элементов приведут:

(3)

Рассчитаем максимальное значение времени восстановления всех элементов информационной системы необходимых для выполнения исследуемого бизнес-процесса:

 (4)

Рассчитаем максимальное время невозможности выполнения бизнес-процесса и предоставления сервиса в связи с длительными отключениями:

(5)

Коэффициент готовности сервиса – есть вероятность того, что объект окажется в работоспособном состоянии в произвольный момент времени, кроме планируемых периодов, в течении которых применение объекта по назначению не предусматривается[6].

(6)

Результаты вычислений показывают:

* Неисправности элементов приведут к 5 отключениям в год. Что больше того, что мы предполагали в первом приближении – одно отключение в год;
* В случае неисправности любого из требуемых для выполнения бизнес-процесса элементов информационной системы максимальное время, за которое будет предоставлен сервис подключения нового мерчанта превысит 29 часов;
* Коэффициент готовности сервиса равен 0,987;
* Минимальное время до восстановления предоставления сервиса равно 0,5 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 29 часа, говорит о возможности существенных проблем при одновременном возникновении ряда отказов;
* Максимальное время простоя в связи с длительными отключениями – 112 часов.

Расчёт показателей надёжности для процесса «Доработка программного обеспечения процессинга» приведён ниже.

Для успешного прохождения процесса «Доработка программного обеспечения процессинга» необходимо наличие работоспособного состояния у следующих элементов информационной системы:

* межсетевой экран;
* Ethernet коммутатор;
* Система хранения данных;
* терминальный сервер (он же сервер электронной почты);
* технологической терминальный сервер;
* сервер баз данных
* сервера приложений.

Исходя из сказанного, кратковременные неисправности элементов приведут:

 (7)

Рассчитаем максимальное значение времени восстановления всех элементов информационной системы необходимых для выполнения исследуемого бизнес-процесса:

(8)

Рассчитаем время невозможности выполнения бизнес-процесса и предоставления сервиса в связи с длительными отключениями:

(9)

Коэффициент готовности сервиса – есть величина обратная среднему времени невозможности выполнения бизнес-процесса.

(10)

Результаты вычислений показывают:

* Неисправности элементов приведут в среднем к 7 отключениям в год;
* В случае неисправности любого из требуемых для выполнения бизнес-процесса элементов информационной системы максимальное время, за которое будет предоставлен возможность доработки программного обеспечения превысит 0,5 часа, что приемлемо для данного бизнес-процесса;
* В случае неисправности любого из требуемых для выполнения бизнес-процесса элементов информационной системы максимальное время, за которое будет предоставлен сервис превысит 31 час;
* Коэффициент готовности сервиса равен 0,9839, что приемлемо для данного бизнес-процесса;
* Минимальное время до восстановления предоставления сервиса равно 0,5 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 31 час, говорит о возможности существенных проблем при одновременном возникновении ряда отказов;
* Максимальное время простоя в связи с длительными отключениями – 143 часа.

Расчёт показателей надёжности для процесса «Процесс обработки данных банковских карт» приведён ниже.

Для успешного прохождения процесса обработки данных банковских карт необходимо наличие работоспособного состояния у следующих элементов информационной системы:

* межсетевой экран;
* Ethernet коммутатор;
* сервера приложений;
* сервер баз данных.

Исходя из сказанного, кратковременные неисправности элементов приведут:

(11)

Рассчитаем максимальное значение времени восстановления всех элементов информационной системы необходимых для выполнения исследуемого бизнес-процесса:

(12)

Рассчитаем среднее время невозможности выполнения бизнес-процесса и предоставления сервиса в связи с длительными отключениями:

(13)

Коэффициент готовности сервиса – есть величина обратная среднему времени невозможности выполнения бизнес-процесса.

(14)

Результаты вычислений показывают:

* Неисправности элементов приведут к 4 отключениям в год. Что больше того, что мы предполагали в первом приближении – одно отключение в год;
* В случае неисправности любого из требуемых для выполнения бизнес-процесса элементов информационной системы максимальное время, за которое будет предоставлен сервис превысит 7 часов;
* Коэффициент готовности сервиса равен 0,9917;
* Минимальное время до восстановления предоставления сервиса равно 0,5 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 7 часа, говорит о возможности существенных проблем при одновременном возникновении ряда отказов;
* Максимальное время простоя в связи с длительными отключениями – 73 часа.

Расчёт показателей надёжности для процесса «Процесс расчёта с банками и иными платёжным системами» приведён ниже.

Для успешного прохождения процесса «Процесс расчёта с банками и иными платёжным системами» необходимо наличие работоспособного состояния у следующих элементов информационной системы:

* межсетевой экран
* Ethernet коммутатор
* сервера приложений
* сервер баз данных
* Система хранения данных.

Исходя из сказанного, кратковременные неисправности элементов приведут:

(15)

Рассчитаем максимальное значение времени восстановления всех элементов информационной системы необходимых для выполнения исследуемого бизнес-процесса:

(16)

Рассчитаем среднее время невозможности выполнения бизнес-процесса и предоставления сервиса в связи с длительными отключениями:

(17)

Коэффициент готовности сервиса – есть величина обратная среднему времени невозможности выполнения бизнес-процесса.

(18)

Результаты вычислений показывают:

* Неисправности элементов приведут к 4 отключениям в год. Что больше того, что мы предполагали в первом приближении – одно отключение в год;
* В случае неисправности любого из требуемых для выполнения бизнес-процесса элементов информационной системы максимальное время, за которое будет предоставлен сервис превысит 31 часов;
* Коэффициент готовности сервиса равен 0,9919;
* Минимальное время до восстановления предоставления сервиса равно 0,5 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 31 часа, говорит о возможности существенных проблем при одновременном возникновении ряда отказов;
* Максимальное время простоя в связи с длительными отключениями – 71 час.

Среднее время до восстановления предоставления сервиса равно 0,5 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 71 часу, говорит о возможности существенных проблем при одновременном возникновении ряда отказов. Несвоевременное осуществление расчётов с банками и иными платёжными системам может привести к существенным штрафным санкциям и даже разрыву договорных отношений.

1. **Разработка мер минимизации выявленных рисков**

В целях минимизации угрозы «прекращение обработки данных банковских карт» предлагается:

* Внедрить отказоустойчивый кластер серверов. Каждый сервер, задействованный в контуре обработке карточных данных дублируется.
* Внедрить стандартизированную процедуру внесения изменений в настройки оборудования и запуска новой версии программного обеспечения в «промышленной среде». Процедура должна определять как порядок согласования и документирования изменений так и автоматизированные средства распространения настроек и программного обеспечения. Данные средства должны позволять «откатить» изменения в случае отсутствия подтверждений корректности работы от системных администраторов.
* В целях противодействия внешним злоумышленникам внедрить специализированные средства противодействия атакам на отказ обслуживания и межсетевой экран прикладного уровня позволяющей нейтрализовать уязвимости в программном обеспечении до выхода исправлений от производителя.
* В целях предотвращения деятельности внутренних злоумышленников предлагается внедрение систему записи сессий удалённого управления серверами.

Аналогичный набор мер предлагается внедрить в целях нейтрализации угроз прекращение бизнес-процесса «Подключение или отключение мерчанта», прекращение бизнес-процесса «Доработка программного обеспечения процессинга», прекращение бизнес-процесса «Расчёт с банками и иными платёжным системами». Исключениями являются средства противодействия атакам на отказ в обслуживании и межсетевой экран прикладного уровня.

Ранее уже упоминалось, что средства создания резервных копий обрабатываемой информации уже внедрены и функционируют. Следует распространить практику создания резервных копий на настройки компонентов информационной системы, системное и прикладное программное обеспечение.

Кража данных банковских карт возможна как со стороны внешних, так и со стороны внутренних нарушителей. В целях предотвращения реализации данной угрозы предполагается внедрить:

* Систему записи сессий удалённого управления серверами;
* Межсетевой экран прикладного уровня позволяющей нейтрализовать уязвимости в программном обеспечении до выхода исправлений от производителя.

Первое средство позволит выявить нарушителей среди персонала процессинга, если такие появятся, и послужит хорошим сдерживающим фактором. Межсетевой экран прикладного уровня позволит предотвращать атаки использующие неисправленные уязвимости в стеке приложений Linux+Apache+Php+MySQL.

Противодействие угрозе кражи персональных данных клиентов аналогично предотвращению кражи данных банковских карт.

* Систему записи сессий удалённого управления серверами;
* Межсетевой экран прикладного уровня позволяющей нейтрализовать уязвимости в программном обеспечении до выхода исправлений от производителя.

Аналогична ситуация и с противодействием краже программного обеспечения процессинга. За исключением того, что источником данной угрозы является только внутренние нарушители и единственной защитной мерой является внедрение системы записи сеансов работы с серверами процессинга.

Более сложной является задача противодействия мошенническим транзакциям. Для её решения потребуется внедрение специализированной системы противодействия мошенничеству. Подобное программное средство анализирует параметры транзакции, особенности рабочей станции клиента, строит профили типичного поведения для каждого пользователя и сравнивает с ними текущее обращение клиента.

Ожидается, что внедрение:

* кластера серверов – приведёт к отсутствию простоя процессинга вследствие аппаратных отказов;
* стандартизированной процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения в «промышленной среде» - уменьшит время простоя процессинга вследствие ошибок персонала до одного часа в год;
* средств противодействия атакам на отказ в обслуживании - уменьшит время простоя до одного часа в год;
* Межсетевой экран прикладного уровня - уменьшит время простоя до одного часа в год;
* средств записи сеансов удалённого управления серверами сведёт к нулю прости процессинга вследствие деятельности внутренних нарушителей.

Также ожидается, что внедрение:

* Межсетевой экран прикладного уровня уменьшит на порядок вероятность кражи данных банковских карт и персональных данных со стороны внешних злоумышленников;
* средств записи сеансов – приведёт к нулевой вероятности кражи данных, банковских карт, персональных данных и исходного кода программного обеспечения процессинга;
* средства выявления мошеннических транзакций - уменьшит на порядок величину фрода.

Сведения об экономической эффективности мер направленных на нейтрализацию угроз приведены в таблице 7.

Таблица 7. Экономическая эффективность мер направленных на нейтрализацию угроз

|  |  |  |  |
| --- | --- | --- | --- |
| **Угроза** | **Средние потери от реализации рисков** |  | **Меры противодействия и средние потери после их применения** |
| Прекращение процесса «Обработка данных банковских карт» | 10 млн. рублей |  | * отказоустойчивый кластер серверов * стандартизированной процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения * средство противодействия атакам на отказ обслуживания * Межсетевой экран прикладного уровня * средств записи сеансов удалённого управления серверами   Результат – уменьшение потерь до  1 млн рублей год. |
| Прекращение процесса «Подключение или отключение мерчанта» | 45 тыс. рублей |  | * отказоустойчивый кластер серверов * стандартизированной процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения * средств записи сеансов удалённого управления серверами   Результат – уменьшение потерь до 2 тыс.рублей год. |
| Прекращение процесса «Доработка программного обеспечения процессинга» | 30 тыс. рублей |  | * отказоустойчивый кластер серверов * стандартизированной процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения * средств записи сеансов удалённого управления серверами   Результат – уменьшение потерь до 1000 рублей год. |
| Прекращение процесса «Расчёт с банками и иными платёжным системами» | 10 млн рублей |  | * отказоустойчивый кластер серверов * стандартизированной процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения * средств записи сеансов удалённого управления серверами   Результат – уменьшение потерь до  1 млн рублей год. |
| Кража данных банковских карт | 200 млн рублей |  | * Межсетевой экран прикладного уровня * средств записи сеансов удалённого управления   Результат – уменьшение потерь до  2 млн рублей год. |
| Кража персональных данных клиентов | 20 тыс. рублей |  | * Межсетевой экран прикладного уровня * средств записи сеансов удалённого управления   Результат – уменьшение потерь до  1 тыс. рублей год. |
| Кража исходного кода программного обеспечения процессинга | 360 тыс. рублей |  | * средств записи сеансов удалённого управления.   Результат – уменьшение потерь до  36 тыс. рублей год. |
| Потеря части денежного потока вследствие отказа банков оплачивать мошеннические транзакции | 36 млн рублей |  | * средства выявления мошеннических транзакций.   Результат – уменьшение потерь до  36 млн рублей год. |

Данные по возврату инвестиций в меры по снижению угроз информационной безопасности приведены в таблице 8.

Таблица 8. Возврат инвестиций и снижение угроз информационной безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры противодействия и эффект от их применения** | **Стоимость мер** |  | **Период возврата инвестиций** |
| Отказоустойчивый кластер серверов и дублирование активного сетевого оборудования.  Устранение  10 млн рублей потерь в год. | 10 млн рублей; |  | 1 год. |
| Cтандартизированные процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения.  Устранение 9000000 рублей потерь в год. | 0 рублей |  | «мгновенно» |
| Средство противодействия атакам на отказ обслуживания (Arbor Prevail). Устранение  3 млн рублей потерь в год. | 1 млн рублей. |  | Около 4-ёх месяцев. |
| Межсетевой экран прикладного уровня (Imperva WAF).  Устранение  3 млн рублей потерь в год. | 1 млн рублей. |  | Около 4-ёх месяцев. |

Продолжение таблицы 8

|  |  |  |
| --- | --- | --- |
| Межсетевой экран прикладного уровня (Imperva WAF) как средство защиты от внешних злоумышленников. Против кражи данных банковских карт.  Устранение  10 млн рублей потерь в год. | 1 млн рублей. | Около 2 дней. «Мнгновенно» |
| Средство записи сеансов удалённого управления.  Против кражи данных банковских карт.  Устранение  12 млн рублей потерь в год. | 1 млн рублей. | 1 месяц. |
| Межсетевой экран прикладного уровня (Imperva WAF) как средство защиты от внешних злоумышленников. Против кражи персональных данных.  Устранение 20 тыс. рублей потерь в год. | 1 млн рублей. | 50 месяцев. |
| Средство записи сеансов удалённого управления.  Против кражи персональных данных.  Устранение  20 тыс. рублей потерь в год. | 1 млн рублей. | 50 месяцев. |
| Средство записи сеансов удалённого управления.  Против кражи исходного кода.  Устранение  324 тыс. рублей потерь в год. | 1 млн рублей. | 4 месяца. |
| Средство выявления мошеннических транзакций.  Предотвращают потерю  32 млн рублей в год. | 10 млн рублей. | 4 месяца. |

Последовательное применение методов управления рисками и теории надёжности позволяет сформировать экономически обоснованный набор мер по повышению надёжности и улучшению защищённости информационных активов. Как показал анализ, стоимость различных мер различается в широких пределах. В столь же широких пределах различаются периоды окупаемости применяемых мер. Результатом является необходимость тщательного анализа представленных на рынке. Выбор конкретных решений должен строится не только на основе их технических характеристик но и учитывать сроки и периоды финансового планирования компании.

**Заключение**

В результате выполнения данной работы удалось выбрать набор организационных и технических мер позволяющий повысить надёжность информационной системы процессинга банковских карт и улучшить состояние информационной безопасности.

**Список использованных источников**

1. Стандарт Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»
2. ГОСТ Р 53480-2009 «Надёжность в технике. Термины и определения»
3. ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения»
4. «Управления инцидентами информационной безопасности» Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой
5. «Управление рисками информационной безопасности» Н.Г. Милославская,

М.Ю. Сенаторов, А.И. Толстой

1. Воронин А.А., Морозов Б.И. Надежность информационных систем: Учебное пособие. СПб.: Изд-во СПбГТУ, 2001, 89 с.
2. Ушаков И.А. Курс теории надежности систем: Учебное пособие. — М.: Дрофа, 2008. — 239 с.