**Термины и определения**

1. 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 [2].
2. Узел (англ. host): устройство в сети, имеющее свой уникальный адрес. В данной работе чаше называется сервером [4].
3. 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 [4].
4. Доступность: свойство информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно (англ. availability) [2].
5. 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 дебето́вые и кредитные. Дебето́вые 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) [4].
6. 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 [4].
7. Процессинг – компания или подразделение банка занятое обработкой данных банковских карт [4].
8. Ssh, telnet, rdp, Https, SOAP, NX – протоколы обмена данными широко применяемые в сети интернет [4].
9. Мерчант – организация или лицо, клиент процессинга [4].
10. Изделие: Любая функциональная единица, которую можно рассматривать в отдельности [5].
11. Составная часть: Рассматриваемая часть изделия [5].
12. Уровень разукрупнения (для технического обслуживания): Уровень разделения изделия на составные части с точки зрения операций технического обслуживания [5].
13. Восстанавливаемое изделие: Изделие, которое при данных условиях после отказа может быть возвращено в состояние, в котором оно может выполнять требуемую функцию[5].
14. Сервис (в технике): Набор функций, предлагаемых пользователю [5].
15. Эффективность применения: Способность удовлетворять требованиям к услуге с заданными количественными характеристиками [5].
16. Возможность (в области надежности в технике): Способность изделия при оказании услуг удовлетворять запросам с заданными количественными характеристиками при данном внутреннем состоянии [5].
17. Надежность: Свойство готовности и влияющие на него свойства безотказности и ремонтопригодности, и поддержка технического обслуживания [5].
18. Готовность: Способность изделия выполнить требуемую функцию при данных условиях в предположении, что необходимые внешние ресурсы обеспечены [5].
19. Безотказность: Способность изделия выполнить требуемую функцию в заданном интервале времени при данных условиях [5].
20. Работоспособное состояние: Состояние изделия, при котором оно способно выполнить требуемую функцию при условии, что предоставлены необходимые внешние ресурсы [5].
21. Состояние функционирования: Состояние выполнения изделием требуемой функции [5].
22. Наработка: Интервал времени, в течение которого изделие находится в состоянии функционирования [5].
23. Состояние нефункционирования: Состояние невыполнения изделием ни одной из требуемых функций [5].
24. Продолжительность нефункционирования: Интервал времени, в течение которого изделие находится в состоянии нефункционирования [5].
25. Состояние готовности: Состояние нефункционирования изделия в требуемое время [5].
26. Неработоспособное состояние: Состояние изделия, при котором оно неспособно выполнить требуемую функцию по любой причине [5].
27. Продолжительность неработоспособного состояния: Интервал времени, в течение которого существует неработоспособное состояние [5].
28. Отказ: Потеря способности изделия выполнить требуемую функцию [5].
29. Критерий отказа: Заранее оговоренные признаки нарушения работоспособного состояния, по которым принимают решение о факте наступления отказа [5].
30. Независимый отказ: Отказ, не вызванный прямо или косвенно другим отказом или неисправностью [5].
31. Целевая точка восстановления (RPO): это точка на шкале времени относительно сбоя, до которой требуется сохранить данные. Изменения данных, предшествующие сбою или аварии на интервал, не меньший этого периода, должны быть сохранены процедурой восстановления. Нулевое значение также является допустимым и соответствует требованию "нулевые потери данных" [5].
32. Допустимое время восстановления (RTO) - это период, необходимый для восстановления после простоя (запланированного, незапланированного или аварийного) и для возобновления обычной работы приложения или набора приложений [5].
33. Соглашение об уровне предоставления услуги (англ. Service Level Agreement (SLA)) — термин методологии ITIL, обозначающий формальный договор между заказчиком (в рекомендациях ITIL заказчик и потребитель — разные понятия) услуги и её поставщиком, содержащий описание услуги, права и обязанности сторон и, самое главное, согласованный уровень качества предоставления данной услуги [4]
34. BPMN нотация – формальный, графический язык, предназначенный для описания бизнес-процессов [4].
35. Ценность – значение, представляемое продуктом/услугой для удовлетворения той или иной потребности субъекта, производящего оценку [5].

**Введение.**

Целью данной работы является расчёт количественных показателей надёжности информационной системы предназначенной для обработки данных банковских карт. Результаты расчёта показателей надёжности будут использованы для оценки непрерывности бизнес-процессов обработки карточных данных и доступности связанных с ними сервисов.

В настоящий момент в России рынок платежей при помощи различных видов банковских карт переживает период роста. Соответственно также растёт число и ущерб от недоступности возможностей оплаты товаров и услуг при помощи банковских карт.

Технологические процессы обработки информации банковских карт во многом основаны на идеях и наработках созданных на предыдущих этапах развития автоматизации банковской деятельности и интернет проектов. Разумным является применения методов расчёта показателей надёжности применяемых в иных областях автоматизации.

Расчёт значений количественных показателей надёжности информационной системы процессинга банковских карт (коэффициенты простоя, потоки отказов и пр.) произведён аналитическим методом. Также произведен анализ надежности информационной системы логико-вероятностным методом с построением дерева отказов. Рассчитан ущерб от нарушения доступности сервисов предоставляемых при помощи рассматриваемой информационной системы. Выработан комплекс меры по повышению надежности системы.

**Краткое 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.

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. 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.

Структура информационной системы процессинга представлена Рисунок 1



**Описание технологических и бизнес-процессов обработки информации банковских карт**

Обработку данных банковских карт, возможно, рассмотреть как совокупность нескольких связанных бизнес-процессов. Для определённости мы рассмотрим четыре основных бизнес-процесса:

* 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.

Процесс «Подключение или отключение мерчанта». Рисунок 1.



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.

Процесс «Доработка программного обеспечения». Рисунок 2.



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.

Процесс обработки данных банковских карт. Рисунок 3.



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.



**Показатели результативности бизнес-процессов**

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 – 500 тысяч;
* Средняя величина транзакции – 200 рублей;
* Процессинг берёт в качестве комиссии 2% от суммы транзакции.

Тогда в сутки данный процесс напрямую приносит в качестве выручки 2 миллиона 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 35 обращений в сутки. Тогда исходя из того, что выручка компании составляет 2 миллиона рублей в сутки, подключение новых клиентов приносит 7 тысячи рублей выручки в сутки.

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 10 тысячи рублей комиссии в сутки. Тогда доработка программного обеспечения 10 тысяч рублей выручки в сутки.

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.

**Показатели непрерывности бизнес-процессов**

Целью 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. 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;
* среднее 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;
* среднее 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;
* средняя наработка между отказами в предоставлении сервиса;
* среднее время до восстановления предоставления сервиса.

**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 [4].

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 [7]. 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 6.

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 6 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 6 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 6 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 6 г и имеет последовательно-параллельную структуру. На рисунке 6 д приведена параллельная структурная схема надёжности, одна из ветвей которой представляет собой параллельное соединение элементов.

1

2

3 3

а)

2

1

3

б)

1

2

3

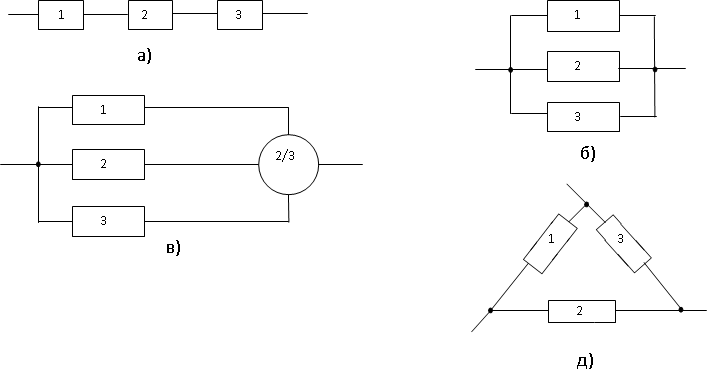
в)

2

1

3

д)



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. Будем определять состояние i-го элемента системы булевой переменной хi такой, что:



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:





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.

**Расчёт текущих 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 – умозрительны.

Таблица 1- Исходные данные для проведения расчётов надежности информационной системы

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Элемент | Общее количество | Минимально необходимое количество работоспособных единиц | , 1/год | , год |  |  |
| Сервер приложений | 1 | 1 | 0,02 | 0,001 | 0,003 | 2 |
| Сервер баз данных | 1 | 1 | 0,02 | 0,005 | 0,003 | 4 |
| Технологический терминальный | 1 | 1 | 0,05 | 0,003 | 0,003 | 1 |
| Терминальный сервер | 1 | 1 | 0,03 | 0,001 | 0,001 | 1 |
| Ethernet коммутатор | 1 | 1 | 0,02 | 0,001 | 0,001 | 0,5 |
| Межсетевой экран | 1 | 1 | 0,01 | 0,001 | 0,0001 | 0,5 |
| Терминалы | 10 | 1 | 0,02 | 0,001 | 0,0001 | 0,1 |
| Система хранения данных | 1 | 1 | 0,02 | 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:



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:



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



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



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



Результаты вычислений показывают:

* В случае неисправности любого из требуемых для выполнения бизнес-процесса элементов информационной системы максимальное время, за которое будет предоставлен сервис подключения нового мерчанта превысит 0,5 часа, что приемлемо для данного бизнес-процесса;
* Коэффициент готовности сервиса равен 0,00007, что также приемлемо для данного бизнес-процесса;
* Среднее время до восстановления предоставления сервиса равно 0,62 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 27 часа, говорит о возможности существенных проблем при одновременном возникновении ряда отказов.

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:



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



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



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



Результаты вычислений показывают:

* 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;
* Коэффициент готовности сервиса равен 0,00008, что приемлемо для данного бизнес-процесса;
* Среднее время до восстановления предоставления сервиса равно 0,752 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 31 час, говорит о возможности существенных проблем при одновременном возникновении ряда отказов.

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:



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



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



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



Результаты вычислений показывают:

* В случае неисправности любого из требуемых для выполнения бизнес-процесса элементов информационной системы максимальное время, за которое будет предоставлен возможность оплаты при помощи банковской карты превысит 0,7 часа, что не допустимо для данного бизнес-процесса;
* Коэффициент готовности сервиса равен 0,0000813, что приемлемо для данного бизнес-процесса;
* Среднее время до восстановления предоставления сервиса равно 0,713 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 7 час, говорит о возможности существенных проблем при одновременном возникновении ряда отказов.

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:



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



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



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



Результаты вычислений показывают:

* В случае неисправности любого из требуемых для выполнения бизнес-процесса элементов информационной системы максимальное время, за которое будет предоставлен возможность оплаты при помощи банковской карты превысит 0,7 часа, что не допустимо для данного бизнес-процесса;
* Коэффициент готовности сервиса равен 0,0000858, что приемлемо для данного бизнес-процесса;

Среднее время до восстановления предоставления сервиса равно 0,752 часа, что приемлемо для данного бизнес-процесса, но максимальное время восстановления равное 31 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.

**Выводы**

Применение теории надёжности сложных технических систем к расчёту показателей непрерывности бизнес-процессов возможно. Существующие проблемы вызванные различиями в терминологии принятой в теории надёжности в теории непрерывности преодолимы. Более существенной проблемой является вопрос корректности выделения подмножества информационной системы от которой зависит протекание бизнес-процесса и вопрос выбора оптимального уровня разукрупнения.

Интересным представляется рассмотрения данной задачи с применением реальных данных по надёжности аппаратных средств, реалистичными сведениями о возможностях восстановления системы с дальнейшим выбором технических и организационных мер повышения надёжности, в том числе с кластеризацией.

**Использованные источники**

1. ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».
2. «Управления инцидентами информационной безопасности» Н.Г. Милославская,

М.Ю. Сенаторов, А.И. Толстой

1. «Управление рисками информационной безопасности» Н.Г. Милославская,

М.Ю. Сенаторов, А.И. Толстой

1. [http://wikipedia.ru](http://wikipedia.ru/)
2. ГОСТ Р 27.002-2009 «Надёжность в технике. Термины и определения».
3. ГОСТ Р ИСО 9000-2008 «Системы менеджмента качества. Основные положения и словарь»
4. Воронин А.А., Морозов Б.И. Надежность информационных систем: Учебное пособие. СПб.: Изд-во СПбГТУ, 2001, 89 с.