ТАЛЛИННСКИЙ УНИВЕРСИТЕТ
Институт Информатики

Роман Яйк

Разработка методики управления ИТ рисков на примере Таллиннского порта

Магистерская работа

Руководитель: Пауль Лейс

Автор:..... «.....».....2010 г.
Руководитель: ..... «.....».....2010 г.
Директор института: ..... «.....».....2010 г

Tallinn 2010

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud.

....

(kuupäev) (magistritöö kaitsja allkiri)

Содержание:

1. Введение

Целью введения магистерской работы является:

- Дать обзор актуальности темы
- Описать цель работы
- Описать структуру работы

1.1 Актуальность

Стремительное развитие информационных технологий и глобализация интернета привели к тому, что элементы национальной критической инфраструктуры становятся объектом преступной деятельности; преступные и террористические группы получили возможность использования глобальной сети в своих преступных намерениях. Составляющие элементы национальной критической инфраструктуры играют решающую роль в обороноспособности страны, её экономическом и социальном развитии. Поэтому, защита национальной критической инфраструктуры является основополагающим аспектом общественной безопасности и экономической стабильности.

В то время как возможности информационных и телекоммуникационных технологий хорошо известны и в настоящее время широко используются, значимость их взаимодействия внутри критической инфраструктуры до сих пор воспринимается с недостаточной степенью серьёзности. Постоянно растущий объем информации, и возможности электронных средств в ее обработке делают информационные системы привлекательной мишенью для преступных посягательств.

Организации их информационные системы и сети все чаще сталкиваются с различными угрозами безопасности такими как шпионаж, компьютерное мошенничество, вредительство, вандализм, пожары и наводнения. Такие источники ущерба, как компьютерные вирусы, компьютерный взлом и атаки типа отказа в обслуживании, становятся более распространенными более агрессивными и все более изощренными. Зависимость от информационных систем и услуг означает, что такая большая организация, как Таллиннский порт, становится все более уязвима по отношению к угрозам безопасности. Взаимодействие сетей общего пользования и частных сетей, а также совместное использование информационных ресурсов затрудняет управлением доступом информации.

Таллиннский порт является критической инфраструктурой Эстонской Республики. Отказ работы информационных технологий (серверов, компьютеров) не окажет критического воздействия на его работе. Больший ущерб может вызвать тяжелые погодные условия, непроходимый лед в акватории порта, терроризм, столкновения судов, которые могут привести к пожарам, наводнению и человеческим жертвам.

Актуальность темы диссертационного исследования обусловлена необходимостью выявления факторов риска в деятельности Таллиннского порта. По мнению автора работы, разработка методики рисков и внедрение в практику системы контроля и управления рисками является приоритетной задачей.

Мероприятия по управлению в области информационной безопасности обойдутся значительно дешевле и окажутся более эффективными, если будут включены в спецификацию требований на стадии проектировании системы.

1.2 Цель

Целью работы является:

- сделать обзор литературы по методологии и стандартам
- выявление рисков в деятельности Таллиннского порта, их количественная оценка
- составить карту классов безопасности по всем ИТ приложениям, работающих в Таллиннском порту
- после идентификации, определить ИТ риски в матрицу
- составить таблицу по уменьшению ИТ рисков
- разработать методику и определить основные этапы управления ИТ рисками
  Объектом исследования являются ИТ процессы, определяющие принципы эффективного функционирования Таллиннского порта.

1.3 Структура магистерской работы

Магистерская работа состоит из 5 частей, 60 листов, включает 2 фигуры, 13 рисунков. Во введении описывается актуальность исследуемой темы и проблемы различных ИТ рисков.

В второй главе дан обзор информационной безопасности. Определена понятие информация и риск информационных технологий.
В третьей главе проанализированы все ИТ активы и процессы. Привидены термины, которые используются в Таллиннском порту.

Дальше обзор методической литературы, проанализированы методы риск - менеджмента, стандарты в процессах информационной технологии. В этой главе дан перечень методов и стандартов, который автор будет в дальнейшем использовать для развитии методики в Таллиннском порту.

В последней главе дан эталонный метод по управлению ИТ рисками в Таллиннском порту. COBIT и OCTAVE напрямую не используются. Затронуты вопросы критичности бизнесс - процессов. В этой главе автор определил и идентифицировал степени риска, где используется система ISKE, дан алгоритм работ для занесения данных в таблицу карты классов и идентифицирование степени риска, таблицу матрицы рисков, а также в таблицу по уменьшению ИТ рисков.

Все эти таблицы находятся в приложениях 1-4.

Информацию необходимо классифицировать, чтобы определить приоритетность, необходимость и степень защиты.

В приложении 1 листа классов безопасности проанализировано ISKE методом все приложения в Таллиннском порту.
В приложении 2 показана матрица расчета ИТ рисков порта.
В приложении 3 произведена идентификация ИТ рисков.
В приложении 4 показана таблица способов уменьшения ИТ рисков.

Все полученные результаты, были получены автором данной магистерской работы, самостоятельно.

2. Ит риски и безопасность инфраструктуры

2.1 Понятия и термины ИТ риска

Все основные информационные (ИТ) активы предприятия Таллиннского порта учтены и закреплены за каждым владельцем.

Под защитой ИТ актива подразумевается выполнение следующих условий, как целостности, работоспособности, секретности.

К целостности относится:
Обеспечение достоверности и полноты информации и методов ее обработки.

К понятию доступности относится:
своевременного получения достаточной информации.

К понятии секретности относится:
обеспечение информацией только людям, которые имеют на это право.

2.1.1 Защита паролей. Термины

Признак пользователя – наделяется пользователю идентификационное имя.

Под паролем понимается используемая комбинация букв и цифр.
Если личный пароль, то используется совместно с идентификационным именем.

Личные пароли установлены:

- На компьютерах, на серверах, приложениях

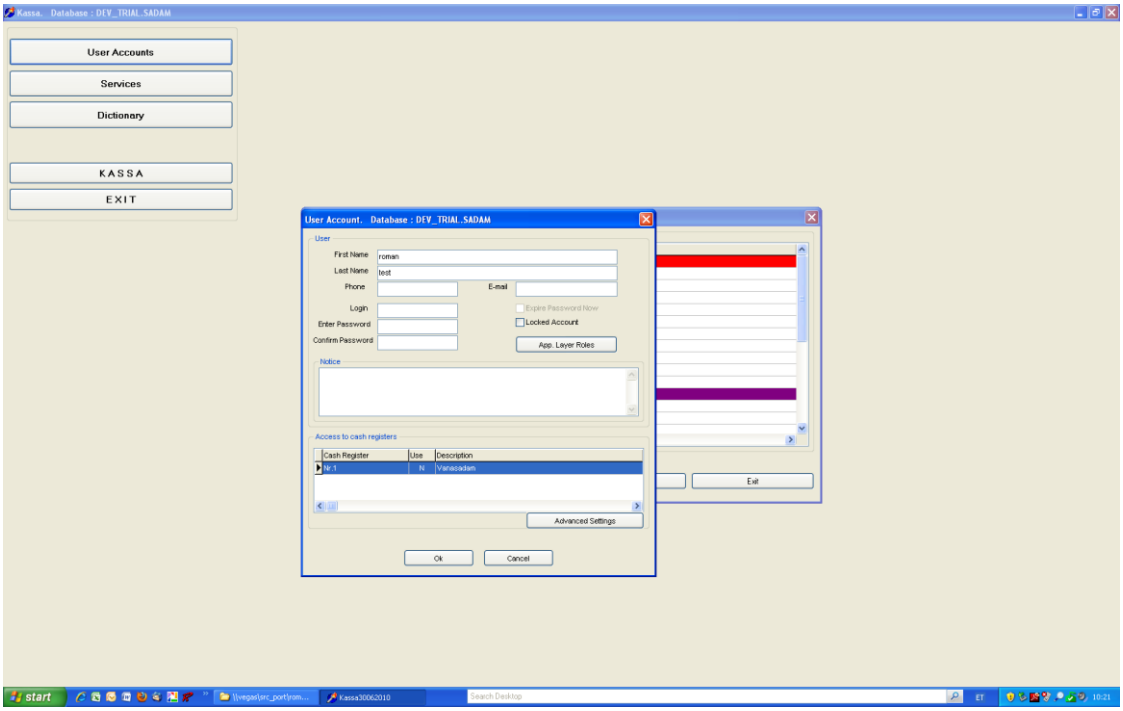


Рис 1. Пример установки пароля через приложение

2.1.2 Требования к паролям

- Пароль должен состоять как минимум из 6 символов
- С паролями, при потере которыми теряется важная информация, делается копия и хранятся в специальном шкафу или в закрытом конверте. Доступ к паролю должен иметь как минимум еще один человек

Пароль должен состоять как минимум из 4 символов, в этом числе как минимум один не алфавитный знак;
Пароль, не должен в себе хранить данные как имена, числа, марка машины и телефонные номера.

2.1.3 Защита от вирусов. Термины

Под опасным программным кодом понимается специфический код программы, который создан для того чтобы причинить ущерб пользователю, завладев данными.

Вирусы -

программы – паразиты, которые проникают в файлы**,** диски, размножаясь в них.

Открытая компьютерная сеть –
сеть, которая не находится в подчинении административного контроля Таллиннского порта.

2.2 Информационная безопасность

Информация – это актив, который подобно другим активам имеет ценность и следовательно должен быть защищен надлежащим образом.
Информация может существовать в различных формах. Она может быть напечатана или написана на бумаге, хранится в электронном виде, передаваться по почте или с использованием электронных средств связи. Безотносительно формы выражении информации, средств ее распространения или хранения она должна быть адекватно защищена.

Исторически под термином риск информационных технологий, или ИТ-риск, подразумевалась вероятность возникновения негативных событий из-за реализации специфичных угроз информационной безопасности – вирусов, хакерских атак, хищений информации, умышленного уничтожения оборудования.

Информационная безопасность — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) — состояние защищенности информации (данных), при котором обеспечиваются конфиденциальность, доступность и целостность.

Безопасность информации (при применении информационных технологий) — состояние защищенности информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы — состояние защищенности автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность её ресурсов.

Указанные риски возникают как на этапе создания информационных систем, так и в процессе их эксплуатации. При проектировании, документировании, разработке и внедрении информационных систем это происходит вследствие:

- выбора не оптимального решения по автоматизации;
- ошибок при проектировании;
- нарушения расчетных сроков и бюджета проекта;
- несоответствия между инфраструктурой и решениями по автоматизации

2.3 Защита ИТ критической инфраструктуры

В то время как возможности информационных и телекоммуникационных технологий хорошо известны и в настоящее время широко используются, значимость их взаимодействия внутри критической инфраструктуры до сих пор воспринимается с недостаточной степенью серьёзности. Постоянно растущий объем информации, и возможности электронных средств в ее обработке делают информационные системы привлекательной мишенью для преступных посягательств.

Стремительное развитие информационных технологий и глобализация интернета привели к тому, что элементы национальной критической инфраструктуры становятся объектом преступной деятельности; появляется больше возможностей для противоправных посягательств; преступные и террористические группы получили возможность использования глобальной сети в своих преступных намерениях. Составляющие элементы национальной критической инфраструктуры играют решающую роль в обороноспособности страны, её экономическом и социальном развитии.

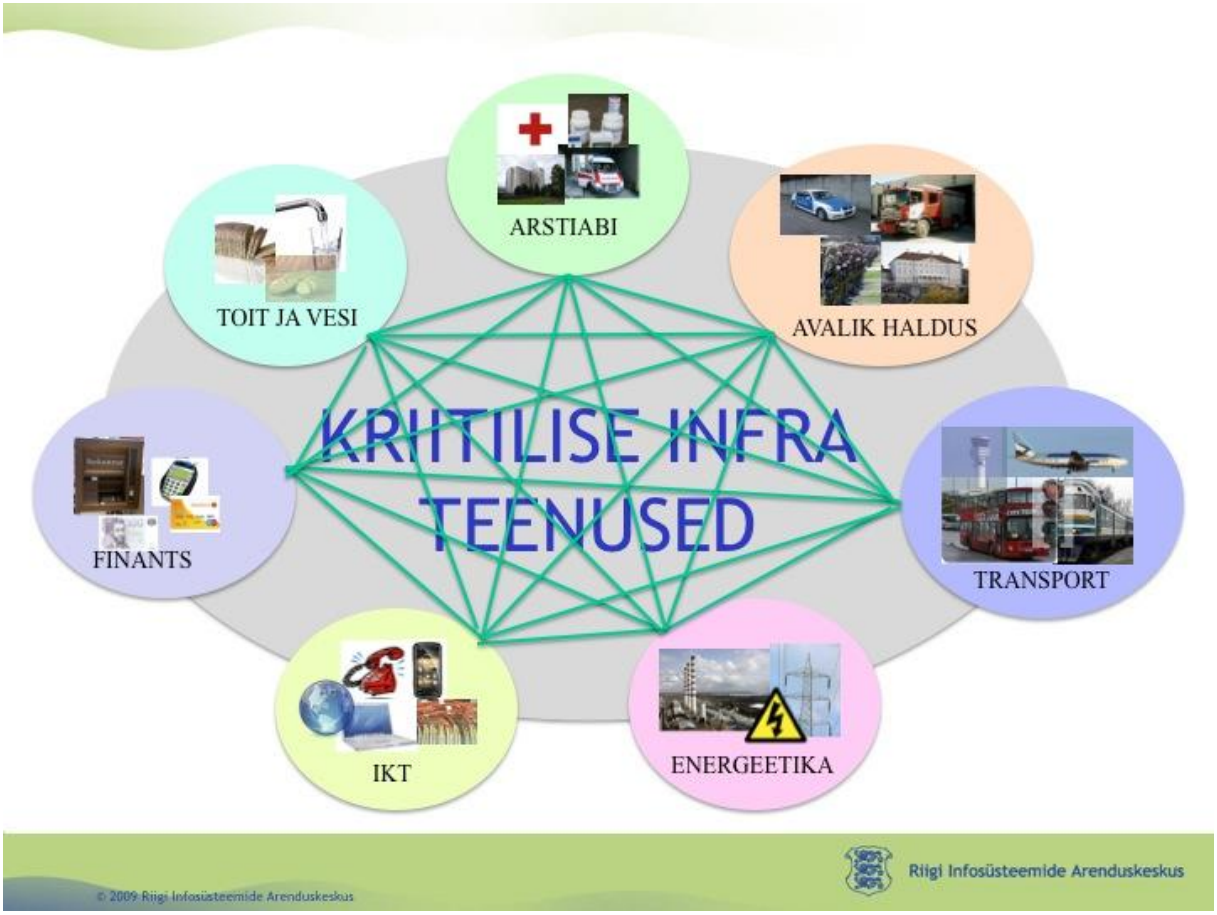
Институт проблем защиты информационной инфраструктуры - консорциум из двадцати трех академических и бесприбыльных исследовательских организаций. Основная задача Института заключается в разработке приоритетных направлений исследований, содействие сотрудничеству и обмену информацией между академическими, промышленными и правительственными учреждениями в области кибернетической безопасности. В основу принципа создания и работы этой организации положены исследования, проведенные в период с 1998 по 2000 гг. Консультативным комитетом по науке и технике при президенте США, Институтом оборонных исследований и Управлением по научно-технической политике.

2.3.1 Защита критической ИТ инфраструктуры в Эстонской Республике

В государственном инфоситемном центром, который подчиняется министерству Экономики и Коммунникаций, также занимаются вопросами безопасностью критической ИТ инфраструктуры.

Из материалов по киберстратегии опубликованных на сайте министерства, становится ясно, насколько Эстонская Республика готова к кибер-атакам. После отражения атак, были опрошены другие государства, как по мнению этих государств Эстонская Республика готовам к атакам, и что делает для предотвращения. Ответ прозвучал, что

Рис.2 Схема критической ифраструктуры Эстонской Республики



налажено хорошее взаимодействие между частными и государственными ИТ секторам в области критической информационной безопасностью. (Riigi Infosüsteemid 2010)

Этот центр курирует государственным инфоситемном отделом развития.

Основные цели отдела:

- хранит всю информацию по критической ИТ инфраструктуры Эстонской Республики

- составляет рапорты анализа рисков

- разрабатывает методику по защите критической ИТ инфраструктуры

- развивает систему ISKE и обновляет инструкции по ее использованию

Инфоситемном отделом развития занимается наиболее значимыми вопросами защитой критической инфраструктуры Эстонской Республики. (Riigi Infosüsteemide Arenduskeskus 2010)

3. ИТ процессы Таллиннского порта

3.1 ИТ активы

ИТ активы Таллиннского порта:

1. Информационный актив

- база данных DEV

Собирается информация о клиентах, персонале, грузе, счетах.

- процедуры баз данных DEV

Обеспечивают поддержку данных, транзакции

1. Актив программ, которые подразделяются на две группы:

– приложения баз данных

Такие приложения, как Client, Disb, Scap

– системные программы

Пакеты (packages) и утилиты (utilities)

2. Физические активы

– компьютерное оборудование

a) Ящики компьютеров сервера десктопы
b) Модемы рутеры факс машины
c) Диски
d) Различные крепления

3. Сервисы

– сервисы

Сервисы работающие с интернетом

К детализированным эксплуатационным процессам автор причисляет те процессы, которые объединены с процессами риск менеджмента (оли, поток информации).

В Таллиннском порту существует системное управление, которое состоит из запросов установленных ошибок по безопасности.
Меры защиты необходимы для того, чтобы вести наблюдения за требованиями безопасности, которые определены отделом информационных систем в сотрудничестве с владельцем рассматриваемых информационных потоков. Эти информационные потоки отвечают требованиям целостности и конфиденциальности.
Избегаются обратной транзакции сделок и записей. Вводятся в базу все заключенные сделки и записи.
Храниться важная информация только в директории My Documents ноутбука и на рабочих станциях и на файловом сервере предприятия.

Дублирование коммуникационных каналов обеспечивается для всех коммуникационных каналов Таллиннского порта.
Шифрованная информация находится на жестких дисках ноутбуков. Предусмотрены ноутбуки в личном пользовании служащих.
Используется антивирусное программное обеспечения (Microsoft Security Essentials), выполняются работы установки, ограничивающие распространение вирусов.

Рис.3 Файловый сервер предприятия

Доступ к рабочей информации предоставляются служащему, основанному на задачах, и даются права администратором.

- **Выполнение ИТ процесса:**

• Осуществляется выполнение между эксплуатационными процессами процесса и риск менеджментом

• Роли, информация, поток информации между процессами

• Синхронизация данных по файловому серверу с данными, хранившими на рабочих станциях и ноутбуках

Инфосистемный отдел разрабатывает защитные средства ИТ актива совместно с их обладателем.

3.2 Поддержка данных

- **Процесс монитора**

Контролируются процессы, обнаруживаются проблемы.
Его главные функции:

• Реакции на подозрительные действия
• Сосредоточения на события

- **Поддержка ответственного персонала**

Оказание поддержки персоналу, который выполняет процессы для распознавания инцидента.

- **Инциденты**

Инциденты требуют обычно своевременной обработки. Быстрое разрешение инцидента могло предотвратить связанную с ним угрозу, и в дальнейшем предотвращают с этим возникающие ущербы.

3.3 Компьютерная защита от вирусов в сети

Антивирусником ИТ отдела сканируются следующие каналы:

- интернет, сервер, движение данных по электронной почте – прежде чем попадут во внутреннюю сеть компьютеров
- открытые сервера

Обеспечивается постоянное обновление 2 раза в день антивирусником в базе данных.

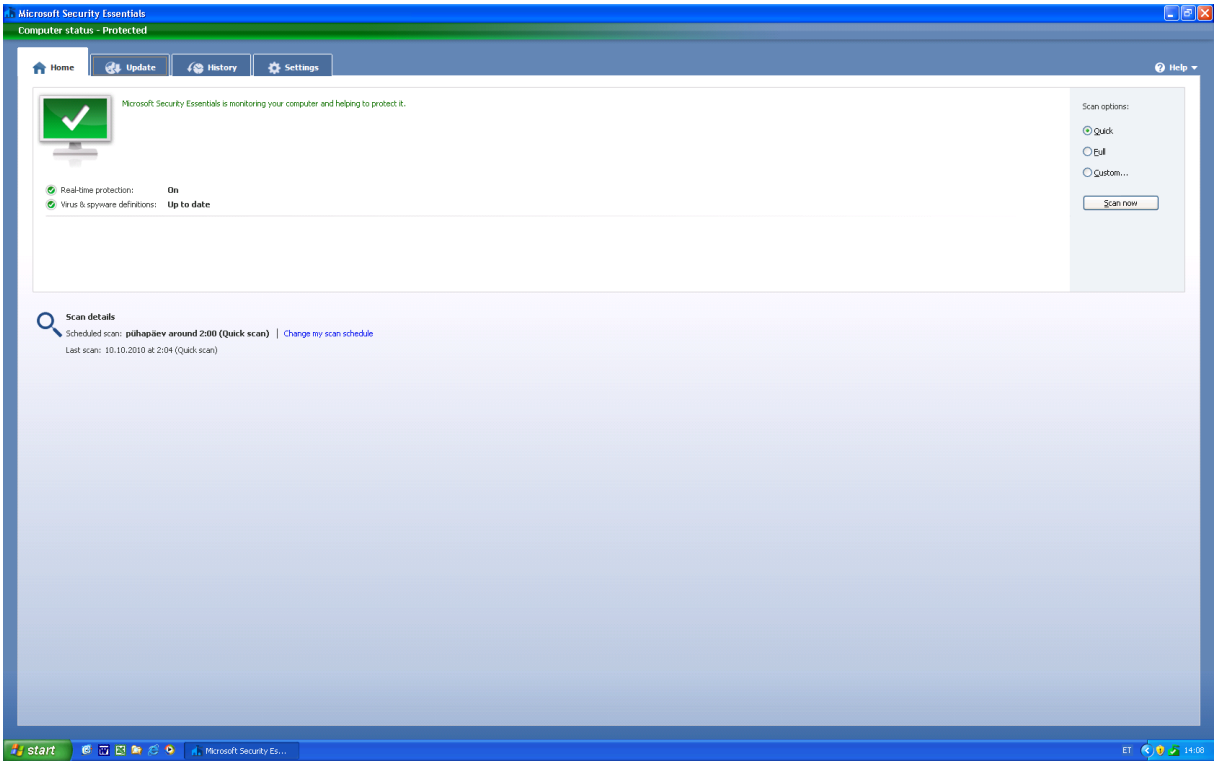


Рис 4. Антивирусник от Microsoft-а, установленный на компьютере

Все входящие и выходящие данные, которые могут в себе носить опасный код сканируется антивирусником ИТ отдела.

Все инфосистемные файлы сканируются антивирусником ИТ отдела прежде чем запускать во внутреннюю сеть компьютеров.

3.4 Развитие и внедрение новых программ

Для развития программ используется стандартные технологии с наименьшей степенью риска.

Все новые решения сканируются с помощью антивирусника. Если всё же произошло заражение, после сообщения, все системы отключаются под руководством ИТ отдела.

3.5 Методы контроля входа в систему

Существуют такие методы контроля, как администрирование. Все различные процедуры охраны системы документируются.

При идентифицировании:

- закрепляется каждому пользователю индификатор ID (user ID);
- происходит прослеживания каждого пользователя вхождения в базу

Контроль доступа к программам определяется исходя из существующих рабочих задач. Определяется, если существующие права на программы. Все изменения согласовываются с ИТ отделом Таллиннского порта.

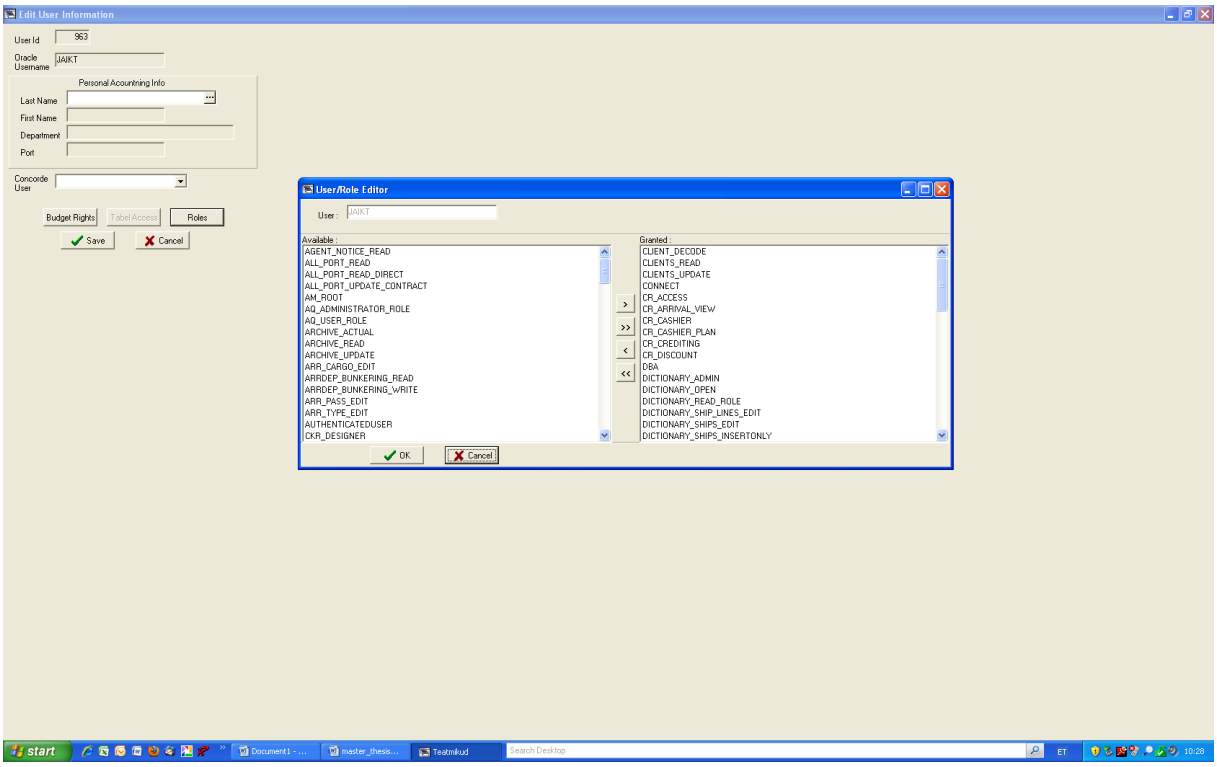


Рис 5. Доступ к программе через приложение

3.6 Управление доступом на основе ролей

Развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

Избирательное управление доступом — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

Субъект доступа «Пользователь № 1» имеет право доступа только к объекту доступа № 3, поэтому его запрос к объекту доступа № 2 отклоняется. Субъект "Пользователь «№ 2» имеет право доступа как к объекту доступа № 1, так и к объекту доступа № 2, поэтому его запросы к данным объектам не отклоняются.

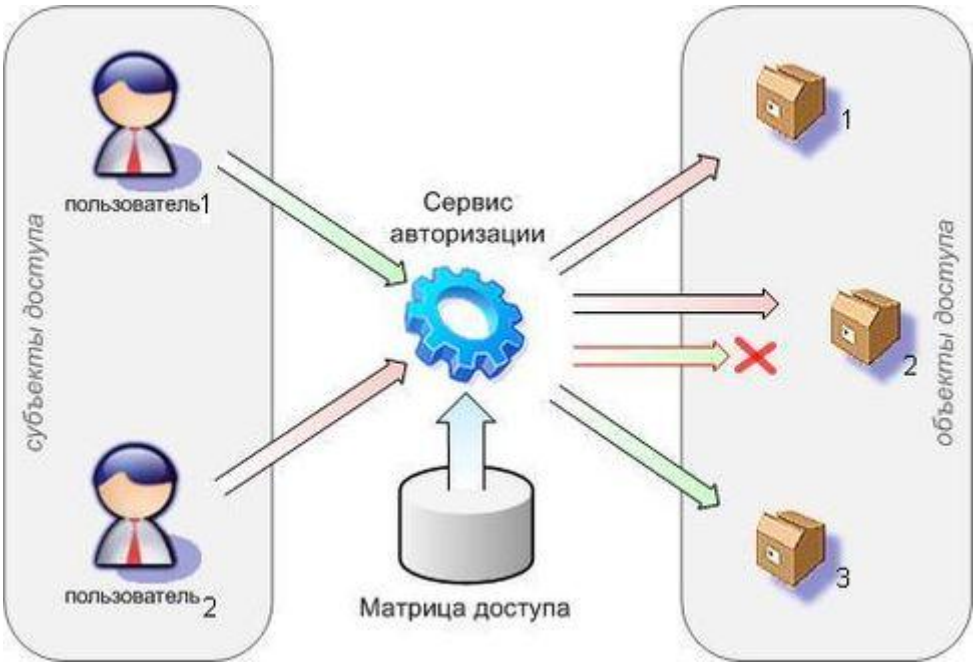


Рис 6. Схема дискреционной модели управления доступом

Для каждой пары (субъект — объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), то есть тех типов

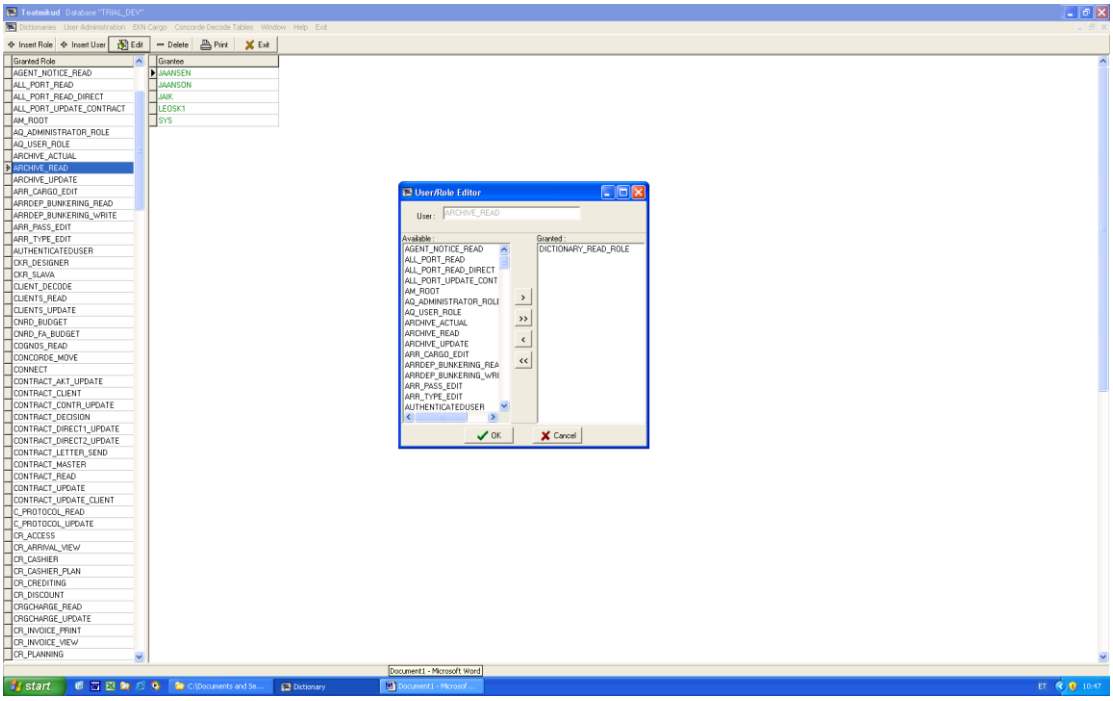
доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту).

Возможны несколько подходов к построению дискреционного управления доступом:

- Каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту.
- Система имеет одного выделенного субъекта — суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.
- Субъект с определенным правом доступа может передать это право любому другому субъекту.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и изменения его владельца. Избирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

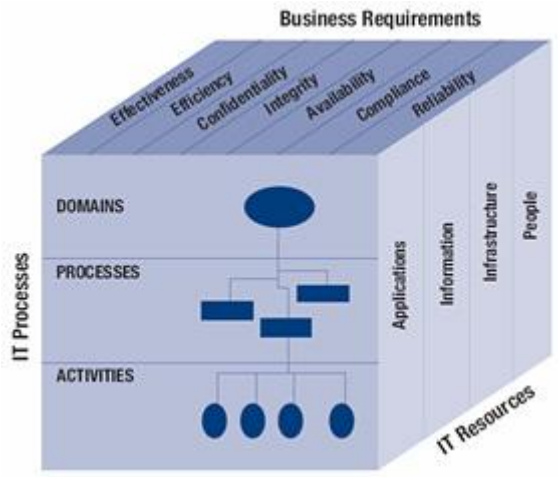
Рис 7. Пример установки роли через приложение



4. Обзор методической литертуры

4.1 COBIT

COBIT (Control Objectives for Information and related Technology) – подход к управлению информационными технологиями, созданный Ассоциацией контроля и аудита систем и Институтом руководства ИТ в 1992 году. Он предоставляет менеджерам, аудиторам и ИТ пользователям набор утверждённых метрик, процессов и лучших практик с целью помочь им в извлечении максимальной выгоды от использования информационных технологий и для разработки соответствующего руководства и контроля ИТ в компании. Первая редакция COBIT увидела свет в 1996 году. В настоящее время используется версия COBIT 4.1, выпущенная в мае 2007 года. Готовиться к выпуску пятая версия COBIT 5.



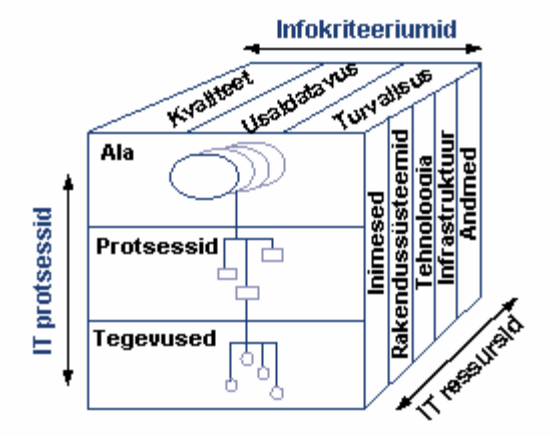
Фигура 1.Схема COBIT

Ключевые области управления ИТ включает в себя :

Управление активами посвящено вопросам, связанным с управлением критичными ИТ активами, а именно, оптимизацией инвестиций и должному руководству приложениями, информацией, инфраструктурой и персоналом. Ключевые вопросы касаются оптимизации инфраструктуры. (COBIT 2010)

Опишем домены управления, в которых группируются процессы COBIT.

- Планирование и организация (Planning and organisation). Включает стратегию и тактику, а также определение способов наиболее эффективного использования ИТ для достижения бизнес-целей. Реализацию стратегических замыслов надо спланировать и согласовать; необходимо создать соответствующую организационную и ИТ-инфраструктуру.



Фигура 2. Куб COBIT

- Комплектование и внедрение (acquisition and implementation). Для реализации ИТ-стратегии нужно идентифицировать, разработать или приобрести соответствующие ИТ-решения, которые должны быть внедрены и интегрированы в бизнес-процессы, а также внести изменения в информационные системы.

- Предоставление и поддержка (delivery and support). Включает предоставление требуемых информационных служб, обеспечение безопасности и непрерывности бизнеса, обучение, а также обработку данных прикладными системами.

- Мониторинг (monitoring). Качество и соответствие ИТ-процессов требованиям контроля должны оцениваться на регулярной основе. Этот домен включает в себя

надзор со стороны руководства за процессами управления в организации, а также независимый контроль со стороны внутренних и внешних аудиторов. (Leis 2010)

4.2 Методология OCTAVE

Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) разработана в университете Карнеги-Мелон, США и означает оценка критичных угроз, активов и уязвимостей.

Методологию OCTAVE используют широко во всем мире при выполнении работ по оценке информационных рисков и внедрению процессов управления рисками в организации. Данная методика имеет ряд модификаций, рассчитанных на организации разного размера и области деятельности.

Методология OCTAVE была разработана в Институте программной инженерии при Университете Карнеги — Меллона и предусматривает активное вовлечение владельцев информации в процесс определения критичных информационных активов и ассоциированных с ними рисков.

Ключевые элементы OCTAVE:

- идентификация критичных информационных активов;
- идентификация угроз для критичных информационных активов;
- определение уязвимостей, ассоциированных с критичными информационными активами;
- оценка рисков, связанных с критичными информационными активами.

OCTAVE предусматривает высокую степень гибкости, достигаемую путем выбора критериев, которые предприятие может использовать при адаптации методологии под собственные нужды.

OCTAVE подразумевает адаптацию методологии к конкретным условиям применения, например к размеру компании, виду бизнеса, требованиям законодательства и тех или иных стандартов. (OCTAVE 2010)

4.3 ISKE

ISKE является инфосистемной трехступенчатой эталонно - защитной системой.

Для разработки и развития системы ISKE взято за основу разработанный Немецким Государственным Отделом Безопасности (BSI) стандарт безопасности (IT Baseline Protection Manual).

В данный момент действует 5 версия инструкции. В мае 2011 готовиться к выпуску 6 версия.

В ISKE описаны 3 степени защиты – низкая (L), средняя (M) и высокая (H). В последней версии ISKE инструкции добалена W версия степени защиты.

Данная система определяет такие понятия, как классы безопасности, которые состоят из:

T - Целостность

K – Критически по времени

R– Взвешивание в последствии результатов

S – Секретность

(ISKE 2010)

4.4 Комплект Стандартов ISO 27000

Семейство Международных Стандартов на Системы Управления Информационной Безопасностью 27000 разрабатывается ISO/IEC JTC 1/SC 27. Это семейство включает в себя Международные стандарты, определяющие требования к системам управления

информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

ISO27000	ISO/IEC 27000:2009 Information technology. Security techniques. Information security management systems. Overview and vocabulary (Определения и основные принципы). Выпущен в июле 2009 г.
ISO27001	ISO/IEC 27001:2005/BS 7799-2:2005 Information technology. Security techniques. Information security management systems. Requirements Информационные технологии (Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования). Выпущен в октябре 2005 г.
ISO27002	ISO/IEC 27002:2005, BS 7799-1:2005,BS ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management (Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью). Выпущен в июне 2005 г.
ISO27003	ISO/IEC 27003:2010 Information Technology — Security Techniques - Information Security Management Systems Implementation Guidance (Руководство по внедрению системы управления информационной безопасностью). Выпущен в январе 2010 г.
ISO27004	ISO/IEC 27004:2009 Information technology. Security techniques. Information security management. Measurement (Измерение эффективности системы управления информационной безопасностью). Выпущен в январе 2010 г.
ISO27005	ISO/IEC 27005:2008 Information technology. Security techniques. Information security risk management (Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности). Выпущен в июне 2008 г.
ISO27006	ISO/IEC 27006:2007 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems (Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью). Выпущен в марте 2007 г.
ISO27007	Руководство для аудитора СУИБ (в разработке).
ISO27011	ISO/IEC 27011:2008 Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Руководство по управлению информационной безопасностью для телекоммуникаций). Выпущен в мае 2009 г.
ISO27033-1	ISO/IEC 27033-1:2009 Information technology. Security techniques. Network security. Overview and concept (Основные концепции управления сетевой

безопасностью). Выпущен в январе 2010 г.

(ISO 27000 2010)

Опишем **Стандарт ISO 27002** более подробно. Стандарт предоставляет лучшие практические советы по менеджменту информационной безопасности для тех, кто отвечает за создание, реализацию или обслуживание систем менеджмента информационной безопасности. Информационная безопасность определяется стандартом как сохранение конфиденциальности, целостности и доступности.

Текущая версия стандарта состоит из следующих основных разделов:

- Политика безопасности (Security policy)
- Организация информационной безопасности (Organization of information security)
- Управление ресурсами (Asset management)
- Безопасность персонала (Human resources security)
- Физическая безопасность и безопасность окружения (Physical and environmental security)
- Управление коммуникациями и операциями (Communications and operations management)
- Управление доступом (Access control)
- Приобретение, разработка и поддержка систем (Information systems acquisition, development and maintenance)
- Управление инцидентами информационной безопасности (Information security incident management)
- Управление бесперебойной работой организации (Business continuity management)

Соответствие нормативным требованиям (Compliance)

(ISO/IEC 27002 2010)

4.5 Стандарт BS 25999

Британским стандартом BS 25999, содержащим лучшие мировые практики по обеспечению непрерывности деятельности;

Услуга по разработке стратегии непрерывности деятельности позволяет идентифицировать критичные бизнес-процессы и области деятельности и спланировать меры по обеспечению их непрерывности.

В рамках данной услуги производится:

- идентификация критически важных для организации процессов и поддерживающих их ресурсов;
- оценка возможного ущерба от нарушения критичных процессов в случае чрезвычайных ситуаций;
- оценка рисков нарушения непрерывности бизнеса;
- определение требований непрерывности;
- выбор общих способов обеспечения непрерывности для критически важных бизнес-процессов на основе технического и финансового анализа;
- разработка стратегии обеспечения непрерывности бизнеса организации, определяющей общие подходы к созданию системы обеспечения непрерывности деятельности и описывающей программу ее создания.

(BS25999 2010)

5. Методика управления ИТ рисками в Таллиннском порту

5.1 Выявление угрозы безопасности крититической инфраструктуры Таллиннского порта

Обеспечение информационной безопасности систем в Таллиннском порту требует особого подхода, учитывающего эти особенности. Для того чтобы выработать такой подход, необходимо, прежде всего, оценить серьезность проблемы в целом, затем, опираясь на накопленную статистику инцидентов, подвергнуть тщательному анализу специфические для систем угрозы и уязвимости и на основании этого анализа определить особые требования к режиму обеспечения информационной безопасности критической инфраструктуры.

5.2 Выбранная методика управления Таллиннского порта

COBIT и OCTAVE, а также стандарты являются основой методики управления ИТ риска Таллиннского порта.

По мнению автора - мониторинг рисков, не является сильной стороной OCTAVE. OCTAVE предусматривает регулярное проведение оценки ИТ рисков и обновление их величин как части процесса оценки рисков. В случае когда стратегия управления рисками определена, OCTAVE предполагает использование в качестве способов снижения рисков, только его снижение и принятие.

OCTAVE не дает количественной оценки рисков, однако качественная оценка может быть использована в определении количественной шкалы их ранжирования. В оценку могут включаться различные области рисков, которые, за исключением технических рисков и рисков нарушения законодательства, напрямую не включены в методологию. Таковые учитываются косвенно, в ходе проведения интервью с владельцами информационных активов, во время которых выясняется, какие последствия могут наступить в случае реализации угроз.
Данная методология не дает четких инструкций по организации мониторинга состояния рисков, но подчеркивает важность его наличия. Методология полностью удовлетворяет требованиям по оценке эффективности мер по снижению рисков и структурированному подходу к управлению рисками.

В COBIT-е автор выделяет вопросы, связанные с управлением критичными ИТ активами, а именно, оптимизацией инвестиций и должному руководству приложениями, информацией, инфраструктурой и персоналом.

5.3 Планирование процесса управления рисками, связанными с ИТ инфраструктурой Таллиннского порта

Планирование – ключевой аспект процесса управления рисками. Грамотно спланированный процесс предполагает соразмерность значимости бизнес-процесса для Таллиннского порта тем затратам, которые необходимы для управления рисками, оказывающими влияние на этот бизнес-процесс.

Деятельность по планированию управления рисками эффективнее всего осуществляет рабочая группа или комитет, в состав которой входят топ-менеджмент порта, руководители других подразделений порта и ИТ менеджмент (в частности ИТ менеджер отдела и ИТ архитектор). Если к процессу внедрения методологии управления ИТ рисками решено привлекать консультантов в области управления ИТ, то их участие уже на этапе планирования также является обязательным.
С консультантом по информационной безопасности следует советоваться, по возможности незамедлительно, в случае подозрения на выявлении инцидента

нарушения информационной безопасности или уязвимости безопасности для обеспечении квалифицированного совета или выделения ресурсов.
Подробнее остановимся на том, какой вклад вносит в работу группы каждый ее участник.

- Вопросы формирования стратегических целей процесса управления рисками, бюджета этого процесса и координации усилий разных подразделений очевидным образом относятся к компетенции топ менеджмента Таллиннского порта.
- В рамках совещаний рабочей группы, задача руководителей других подразделений предоставить информацию о внутреннем устройстве бизнес-процессов, необходимую для анализа рисков.
- ИТ менеджмент, принимая участия в совещаниях рабочей группы, берет на себя технические вопросы, связанные с ИТ.

Рис.8 Схема расположения подразделений

Топ - менеджмент	Подразделения маркетинга и Комерции
ИТ отдел	Риск менеджмент

Источник. Автор

На этапе планирования рабочая группа достигает ряда целей:

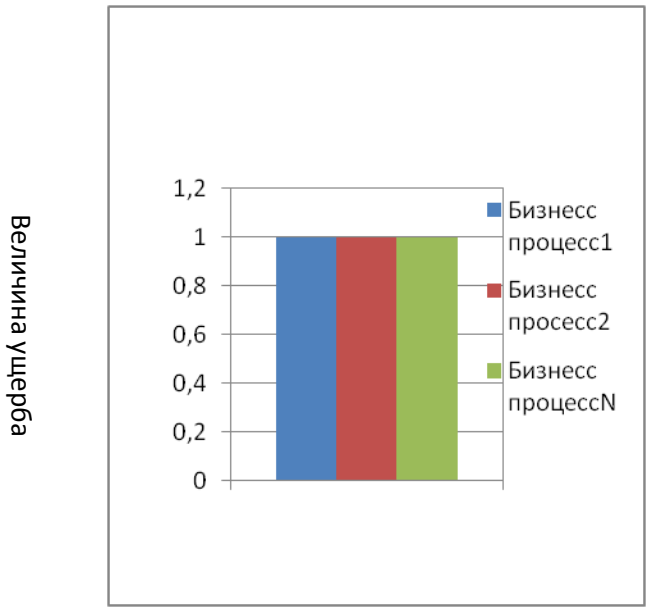
- выявление бизнес-процессов, критичных для Таллиннского порта;
- утверждение карты вероятностей и последствий;
- разработка плана собраний рабочей группы, целью которых является анализ рисков для всех критичных бизнес-процессов;

Рассмотрим каждую из целей этапа планирования отдельно.

5.3.1 Выявление бизнес-процессов, критичных для Таллиннского порта

Каждый процесс, происходящий в Таллиннском порту важен, в особенности он важен с точки зрения сотрудников в нем участвующих. Поэтому, полностью закономерен вопрос: каким же образом выделить бизнес-процессы, критичные в большей степени, чем остальные? Существует несколько типовых подходов к решению этой задачи. Например, можно провести оценку величины ущерба, понесенного Таллиннского порта, для каждого из исследуемых бизнес-процессов, в случае его остановки на срок до одного дня. При этом, величина ущерба рассчитывается в некоторых условных единицах, учитывающих как прямые потери, так и недополученную прибыль, ущерб репутации.

Рис.9 График величины ущерба в бизнес-процессах



Источник. Автор

В своей статье "Риск-менеджмент Программного обеспечения: Принципы и Методы", доктор Боехм описывает риск-менеджмент как, состоящего из следующих действий:

- Оценка степени риска
- Создание списка всех потенциальных опасностей, которые затронут проект

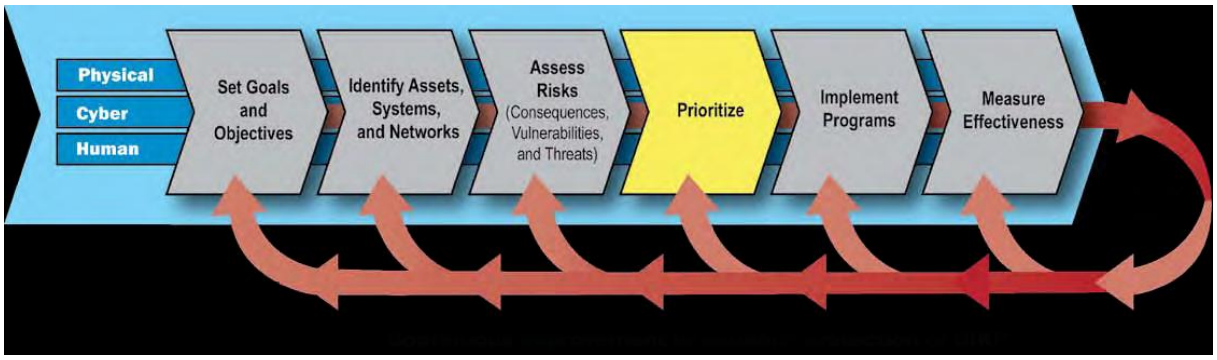
(Boehm B.W. (1991), Software risk management)

Все бизнес-процессы, для которых величина ущерба больше некоторой заранее определенной величины, объявляются критическими.

5.3.2 Приоритетные ИТ риски процессов Таллиннского порта

Необходимо четка выделить приоритетные ИТ риски Таллиннского порта и работать уже по ним.

Рис. 10 График приоритетных ИТ рисков в бизнес-процессах



Источник. (National InfrastructureProtection Plan 2009)

В классах безопасности целостность описывается как:

Т - Целостность

- **Т3** – В информации должно быть реальное значение
- **Т2** – Информация должна быть распознаваема
- **Т1** - Информация , в которой делается изменения должна быть распознаваема

- **T0** – Информация, ее изменения не важно к распознаванию

В классах безопасности доступность описывается как:

K – критически по времени

- **K3** – Получение информации важно в течении секунды
- **K2** - Получение информации важно в течении часа
- **K1** - Получение информации важно в течении дня
- **K0** - Получение информации неограниченно во времени

- **R** – взвешивание в последствии результатов
  - **R3** – Неполучение информации ведет к невыполнению функциональности
  - **R2** - Неполучение информации ведет к нарушению выполнения функциональности
  - **R1** - Неполучение информации ведет к возможности нарушения выполнения функциональности
  - **R0**- Неполучение информации не ведет к возможности нарушения выполнения функциональности

В классах безопасности секретность описывается как:

S - Секретность

- **S3** - Информация по закону засекречена
- **S2** – Доступ к информации разрешен только владельцу
- **S1** - Доступ к информации разрешен только для решения определенной задачи
- **S0** – К доступу информации нет ограничения (Riigi Infosüsteemide Arenduskeskus 2010)

Приотизируем ИТ риски и запишем в карту классов:

1. Тарифы Таллиннского порта S0 K1 R1 T1

2. Регистер клиентов S1 K1 R1 T1

Полная карта классов проиндиксированных ИТ приложений находиться в приложении 1 данной магистерской работы.

5.3.3 План мероприятий по анализу рисков

Календарный план сессий анализа для выделенных критических процессов является основанием для выделения бюджета для этого типа работ.

Как правило, участие рабочей группы в полном составе на этапе анализа не целесообразно, поэтому к работе в рамках каждого собрания, привлекаются лишь те руководители других подразделений, которые отвечают за рассматриваемую группу бизнес-процессов и сотрудники IT-подразделения.

Для записи инцидентов нарушения информационной безопасности и других связанных с безопасностью событий следует создавать журналы аудита и хранить их в течении согласованного периода времени.
Необходимо, чтобы записи аудита включали:

- ID пользователей
- Даты время входа и выхода
- Идентификатор терминала
- Записи успешных и отклоненных попыток доступа к системе

5.4 Стратегия реагирования

5.4.1 Анализ бизнес-процессов и аудит рисков

Анализ бизнес-процессов и аудит рисков – следующий шаг на пути внедрения методологии управления ИТ рисками Таллиннского порта. Этот процесс логично разделить на ряд последовательных этапов:

- формализация бизнес-процессов;
- выявление ИТ ативов, задействованных на каждом шаге;
- выявление “узких мест” и проблемных участков ИТ инфраструктуры;
- формализация и ранжирование рисков.

Чаще всего бизнес-процессы Таллиннского порта описаны достаточно абстрактно, не достаточна для анализа рисков, поэтому первым шагом является их формализация. Для каждого этапа бизнес-процесса ИТ подразделение определяет, какие элементы ИТ инфраструктуры в нем задействованы и какова вероятность их сбоя.

Согласно методу Octave, выявленные таким образом ИТ риски записываются в реестр и ранжируются. Приблизительный формат реестра ИТ рисков приведен в таблице. Ранг каждого риска определяется на основании карты вероятностей и последствий.

Среди бизнес процессов можно выделить:

Бизнесс -процесс1 - синхронизация данных
Бизнесс -процесс2 - контроль доступа к программам
Бизнесс -процесс3 - сканирование антивирусником ИТ отдела

Рис.11 Карта вероятности

	Категория 1		Категория 2	
	Риск 1	Риск 2	Риск 3	Риск 4
Бизнесс - процесс1				
Бизнесс - процесс2				
Бизнесс - процесс3				
Суммарный риск				

Источник. Автор

Необходимо подчеркнуть, что анализируя риски, нужно принимать во внимание не только работу систем в штатном режиме, но и пиковую нагрузку на них. Например, IT-система, обычно функционирующая без сбоев, может выйти из строя во время предновогоднего пика нагрузки во время перехода на евро.

Проверка информационной безопасности может быть выполнена внутренним аудитом, независимым менеджером или сторонней организацией, специализирующейся на таких проверках, при чем специалисты привлекаемые к проверкам, должны обладать соответствующими опытом и навыками. Внутренний аудит в Таллиннском порту проводится согласно действующим международным стандартам (ISO 9001:2008) и (ISO 14001:2004). Результаты аудита сохраняется, как правило в электронном регистре. (Tallinna Sadam AS (2010), Kvaliteedikäsiraamat)

5.4.2 Разработка стратегии реагирования

Следующий этап – формирование рабочей группой стратегии реагирования на выявленные и проранжированные риски.
Возможны четыре основных варианта такой стратегии:

- предотвращение
- реагирование

- передача
- принятие

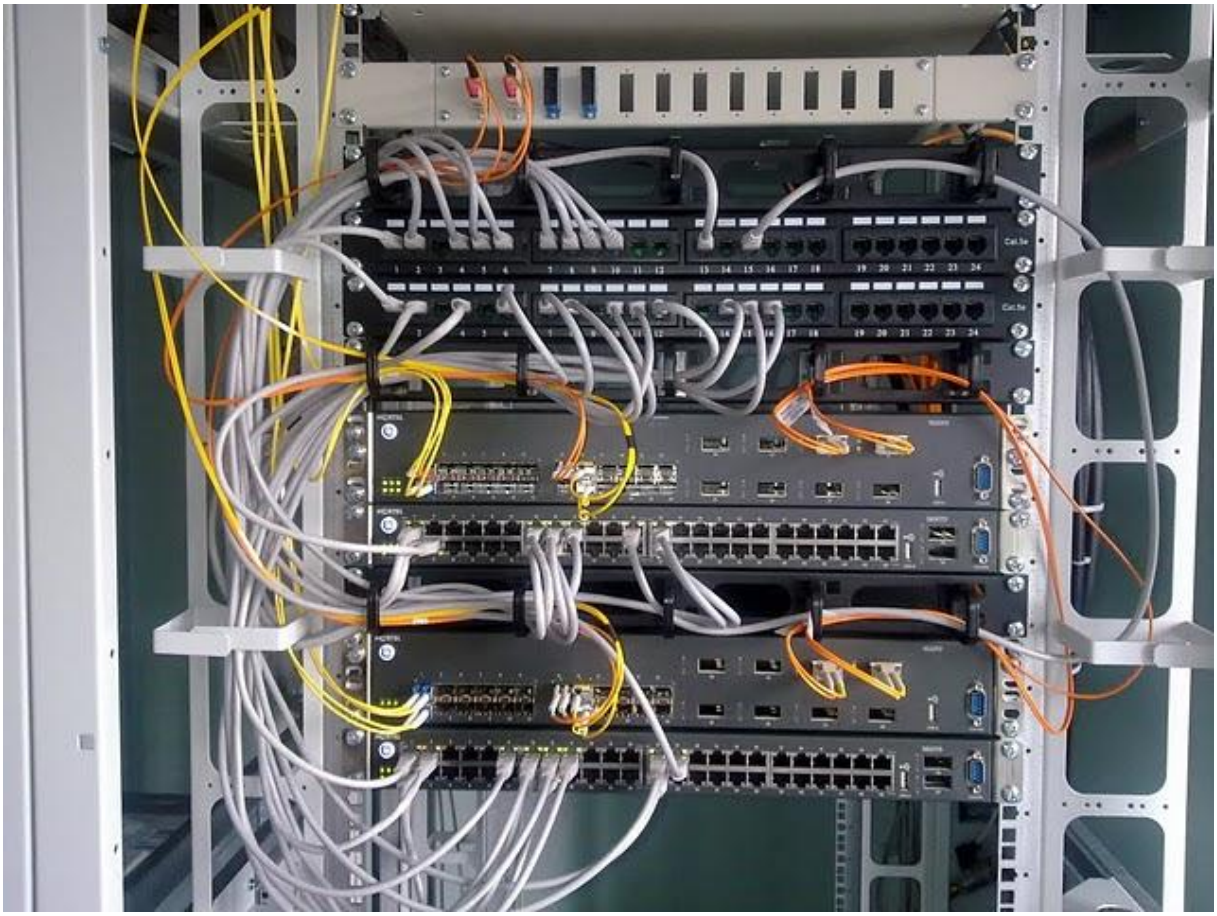


Рис.12 Запасной сервер Таллиннского порта

Предотвращение предполагает разработку сценария действий, направленных на исключение угрозы, связанной с риском.

- Угроза (THREAT) — потенциально возможное происшествие, неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на бизнес-процессы Таллиннского порта, IT-системы, а также на информационные активы компании. Иначе говоря, угроза — это нечто плохое, что когда-нибудь может произойти.

Угрозы информационным активам в Таллиннском порту :

T01. Утечка информации о клиентах к конкурентам через незащищенный канал связи

Программы Personal, Client

T02. Поставка программного обеспечения и данных - вирусы или испорченные данные.

Возникали проблемы у диспетчеров, программы SCAP.

T03. Случайное или злоумышленное причинение вреда информации в базах данных через интернет

Нежелательные злонамеренные действия через интернет страницы к базам данных компании.

T04. Угрозы нарушения работоспособности системы, программного обеспечения

Рабочий сервер WDC и программы SCAP, DISB, DISP.

T05. Угрозы целостности данных, программ, аппаратуры

Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов. Программа Disb.

T06. Угрозы доступности данных

Возникают в том случае, когда пользователь не получает доступа к законно выделенным ему активам. Эта угроза реализуется захватом всех активов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации.

T07. Угрозы канала связи

Эта угроза может исходить от удаленного нарушителя на почтовый сервер Таллиннского порта.

Поскольку данные угрозы могут быть реализованы через осуществление несанкционированного доступа, то для защиты информационной системы используются следующие методы:

1. Идентификация и аутентификация пользователей системы.
2. Авторизация и разграничение доступа пользователей к ресурсам инфосистемы.
3. Регистрация и оперативное оповещение о событиях, происходящих в системе.
4. Криптографическое закрытие хранимых и передаваемых по каналам связи данных.
5. Контроль целостности данных.
6. Выявление и нейтрализация действий компьютерных вирусов.
7. Выявление уязвимостей системы.
8. Изоляция компьютерных сетей.
9. Обнаружение атак и оперативное реагирование.

Определенная угроза занесена автором в приложении 3.

- Уязвимость (vulnerability) информационной системы — тот или иной ее недостаток, из-за которого становится возможным нежелательное воздействие на нее со стороны злоумышленников, неквалифицированного персонала или вредоносного кода (например, вирусов или программ-шпионов).

Идентифицируем уязвимости, присутствующие в инфраструктуре Таллиннского порта. Для этого необходимо обратить внимание на все программные и аппаратные средства, которые могут являтся точкой проникновения.

V01. Продукты Microsoft

WSUS сервер. С его помощью осуществляется управление обновлениями для операционных систем и интернет браузеров – самых уязвимых по статистике

компонентов инфраструктуры. Поддерживая приложения Office и почтовый сервер Exchange.

V02. SQL, Oracle сервер

Есть угроза потерей конфиденциальности информации, хранящейся в базе данных.

V03. DNS сервер

Особых проблем не нет. В случае попыток организации сетевого шторма маршрутизатор от Cisco должен подстраховать. Этот тип атак хорошо изучен и эффективно блокируется.

V04. Корпоративная сеть

Защищена. Взломщику, например, получить системные привилегии на каком-либо компьютере сети, не получится.

Определенная автором уязвимость занесена в приложении 3.

Реагирование предполагает понижение вероятности и последствий наступления риска. Например, в случае выхода из строя одного из серверов системы, сценарий реагирования может включать временный перевод пользователей на резервный сервер.

Передача риска подразумевает переложение негативных последствий и ответственности за реагирование на риск на третью сторону. Передача риска предполагает передачу ответственности за его управление другой стороне, риск при этом не устраняется. Принятие риска, не предполагает проведения никаких предупредительных мероприятий, оставляя ИТ подразделению право действовать по собственному усмотрению в случае наступления риска.

Как стратегии предотвращения, так и стратегии реагирования предполагают разработку специальных сценариев, которые, как правило, описывают:

- последовательность действий ИТ персонала, направленных на предотвращение угрозы, либо на ликвидацию последствий
- последовательность действий сотрудников других подразделений, в период, когда ИТ сервис недоступен, и после его восстановления.

В рамках сессий по разработке стратегии реагирования, для каждого сценария и каждого действия в его рамках необходимо определить ответственного, а также предусмотреть механизмы контроля за его действиями.

5.4.3 Ответственность ИТ подразделения. Схема

Стратегия реагирования ИТ подразделения подготавливается на основе анализа возможных угроз каждого из элементов ИТ инфраструктуры, находящегося в зоне риска. В число таких угроз входят:

- человеческий фактор (нарушение процедур эксплуатации);
- выход оборудования из строя;
- сетевые атаки;
- отключение электричества;

В рамках выбранной рабочей группой стратегии реагирования, в зону ответственности ИТ подразделения Таллиннского порта входит:

- разработка сценариев действий для каждой выявленной угрозы;
- определение ИТ специалистов, ответственных за каждый сценарий;
- разработка механизмов тестирования сценариев;
- определение механизмов мониторинга угроз.

5.4.4 ИТ риски Таллиннского порта. Мониторинг и управление

Очевидно, работы по мониторингу рисков предполагают, что признаки наступления риска четко определены, а статистика всякого рода сбоев ведется.

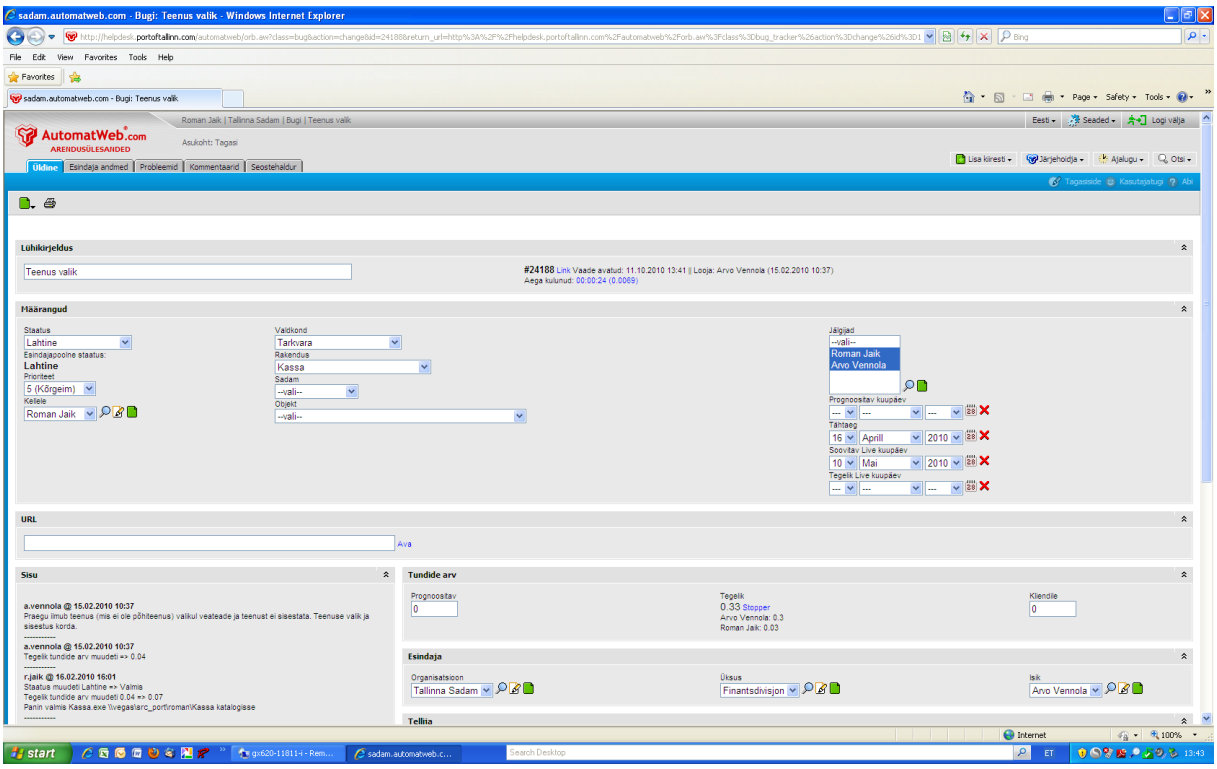


Рис 13. Система Help-Desk

Есть большое количество программных средств, позволяющих в автоматическом режиме собирать подобную статистику, анализировать ее. Хороших результатов можно добиться, применяя в комплексе, как системы класса HelpDesk и системы мониторинга состояния оборудования.

Сама программа HelpDesk внедрена в порту и прошлом году и позволяет оперативно передавать информацию. Руководство строго следит за сроками выполнений заданий. Периодически необходимо проводить выборочное тестирование наиболее значимых стратегий реагирования.

Само стратегия и планирование по уменьшению ИТ рисков, включает в себя

Id риски, которые могут быть как распознаны, так и нет.

Уровень риска может быть низкий, средний, высокий. Преобразование, включает в себя принятие, минимизирование, избежание.

Полную таблицу уменьшения рисков смотри таблицу в приложении 4.

Следующий цикл анализа рисков позволяет определить, какие мероприятия эффективны для минимизации и предотвращения рисков, а какие нет. На основе анализа эффективности можно корректировать понимание риска, его оценки и требуемых действий. Кроме того, анализ эффективности предоставит возможность увидеть минимизацию параметров уязвимости и ущерб для всех рисков, что в целом усилит режим IT-безопасности.

Возможное выявление новых внешних угроз, автоматизация новых бизнес-процессов приводит к неизбежному изменению требований к существующим ключевым ИТ сервисам. Регулярное обновление планов и процедур по обеспечению непрерывности ключевых ИТ услуг позволят ИТ подразделению гибко приспосабливаться к изменяющемуся бизнесу организации.
Для обеспечения уверенности в том, что пользователи выполняют только те действия на которые они были авторизированны, необходимо определить процедуры мониторинга использования средств обработки информации.
При мониторинге следует обращать внимание на

а) авторизованный доступ, включая следующие детали:

- пользовательский ID
- дата и время основных событий
- типы событий
- файлы, к которым был осуществлен доступ
- использованные программы

б) все привилегированные действия, такие как:

- запуск и останов системы
- подсоединение или отсоединение системы ввода/ вывода

в) попытки неавторизованного доступа, такие как:

- неудавшиеся попытки
- предупреждение от собственных систем обнаружения вторжения

5.4.5 Схема процесса управления ИТ рисками

Схема процесса управления IT-рисками подчеркивает цикличность процесса и обязательность контроля эффективности со стороны руководства порта.

- Планирование
    - Карта вероятностей и последствиий
    - Список ответсвенных за процесс

- Идентификация
    - Список ответсвенных за каждый из рисков
    - Реест рисков
    - процедуры мониторинга и контроля

- Разработка стратегии реагирования
    - Реест рисков
    - Стратегию реагирования
    - Процедуры мониторинга и контроля

- Приоатизирование ИТ рисков
    - Таблица ИТ рисков
    - Стратегию реагирования
    - Процедуры мониторинга и контроля

- Внедрение
    - Реест рисков
    - Стратегию реагирования
    - Процедуры мониторинга и контроля

- Мониторинг и контроль
    - Инициатива руководства
    - Культура управления рисками
    - Стандарты

Природа ИТ рисков динамична, поэтому управление ими должно носить непрерывный характер. Такой подход поможет Таллиннскому порту соответствовать постоянно меняющимся условиями, в которых ему приходится работать.

Основным результатом (выходом) процесса оценки рисков является перечень всех потенциальных рисков с их количественными и качественными оценками ущерба и возможности реализации. Необходимо определить перечень особо опасных рисков, к минимизации которых следует приступить немедленно и минимизация которых повысит уровень безопасности Таллиннского порта. То есть речь идет лишь о понимании, сколько риска готов взять на себя Таллиннский порт и какому риску она подвергается в действительности. Таблица уменьшения риска находиться в приложении 4.

Одним из важных этапов построения системы IT-безопасности является создание эффективного механизма управления рисками, что позволит принимать обоснованные решения в данном направлении.

Использованная литература

Boehm B.W. (1991), Software risk management: Principles and practices, IEEE Software, Jan. 32-41.

National Institute of Standards and Technology (Risk Management Guide for Information Technology Systems Gary Stonebumer,Alice Goguen, and Alexis Feringa 2002),
URL http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Octave, (2003).
URL http://www.cert.org/octave/approach_intro.pdf

COBIT,(2010). IT Governance Institute,
URL http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

ISKE,(2010). Riigi Infosüsteemide Arenduskeskus. Infosüsteemide kolmeastmelise etalonturbe süsteem. (versioon 5. 2009),
URL http://www.ria.ee/public/ISKE/iske_kataloogid_5_01.pdf

Tallinna Sadam AS (2010),
URL http://www.ts.ee

Riigi Infosüsteemide Arenduskeskus (2010). Turvanõuete klassifitseerimisvajadusest,
URL http://www.ria.ee/?404, (September 1, 2010)

Практические правила управления безопасностью,ISO/IEC 17799:2000,
URL http://ostapbenderx.narod.ru/Index/22/2262.htm, (November 1, 2010)

National InfrastructureProtection Plan(2009),
URL http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Riigi Infosüsteemid (2010). Küberjulgeolek kui osa riigi-, sise-, välis- ja Majandusjulgeolekust,
URL http://www.riso.ee/et/files/4.2_%20Kyberstrateegia_H.Tiirmaa-Klaar.pdf

P.Leis (2010), Cobit: Учебные материалы, Таллиннский Университет,
URL http://www.tlu.ee/?LangID=1&CatID=5030&ArtID=910&action=article

ISO 27000,(2010). Комплект Стандартов ISO 27000,

URL http://iso27000.ru/standarty/iso-27000

ISO/IEC 27002,(2010). Стандарт ISO/IEC 27002,

URL http://ru.wikipedia.org/wiki/ISO/IEC_27002

BS25999,(2010). Стандарт по обеспечению непрерывности ведения бизнеса BS25999,

URL http://www.leta.ru/services/information-security-management/business-continuity-BS25999.html

Tallinna Sadam AS (2010), Kvaliteedikäsiraamat – Siseauditid.

Выводы

Целью представленной работы является разработка методики ИТ рисков в Таллиннском порту.

Были изучены следующие темы:

- Понятия и термины ИТ риска, детально проанализированы классы безопасности
- Сделан обзор методической литературы
- Проанализированы ИТ процессы Таллиннского порта

Выполнены следующие задачи:

1. Составлена карта классов для всех ИТ приложений
2. Составлена матрица ИТ рисков
3. Составлена таблица идентификация ИТ рисков
4. Составлена таблица по уменьшению ИТ рисков
5. Разработана методическое пособие по управлению ИТ рисками

Данная работа состоит из введения, 5 основных частей, вывода, использованной литературы и приложений. Магистерская работа написана на русском языке.

Kokkuvõtte

Käesoleva töö eesmärgiks on sadamate IT riskide metoodika väljatöötamine.
Käsitletakse järgmisi teemasid:

- IT riski mõiste ja terminid, turvaklasside üksikasjalik analüüs;
- metoodilise kirjanduse, metodoloogia ja standardite ülevaade.

Täidetud on järgmine ülesanne:
- Analüüsida erinevaid riskianalüüsi standardeid meetodeid ja valida välja sobiv riskianalüüsi meetod, mis sobiks AS Tallinna Sadam infosüsteemile
- Kõigi IT protsesside analüüs
Töö tulemusteks on:

1. sadama turvaklasside kaardi loomine
2. riskimaatriksi tabeli loomine
3. IT riskide määratlemise tabeli loomine
4. IT riski vähendamise tabeli loomine
5. metoodilise õppevahendi valmistamine

Antud töö koosneb sissejuhatusest, 5 põhiosast, kokkuvõttest, kasutatud kirjanduse nimekirjast ja lisast. Töö on kirjutatud vene keeles.

Приложение 1. Карта классов ИТ приложений

1. Sadamatasude arvestuse süsteemi info	
1.1. Klientidele väljastatud sadamatasude ja laevadele osutatavate teenuste tasude arved.	S1 K1 R1 T1
2. Dokumentide register	
2.1. Lepingute register	S1 K1 R1 T1
2.2. Kirjade register	S1 K1 R1 T1
2.3. Korralduste register	S1 K1 R1 T1
2.4. Käskkirjade register	S1 K1 R1 T1
2.5. Aktide register	S1 K1 R1 T1
2.6. Protokollide ja ISO-ga seotud dokumentide register.	S1 K1 R1 T1
2.7. Sadamatasude tariifid	S0 K1 R1 T1
2.8. Operaatorfirmade koostöölepingute info ja kaubatasude tariifid	S1 K1 R1 T1
3. Kaubatasu arvestuse süsteemi info	
3.1. Operaatorfirmade veoste töötlemise registrite info	S1 K1 R1 T1
3.2. Klientidele väljastatud kaubatasude arved	S1 K1 R1 T1
3.3. Punkerdamislaevade omanikele väljastatud arved	S1 K1 R1 T1
4. Personaliarvestuse süsteemi info	
4.1. Töötajate isikuandmed	S1 K1 R0 T1
4.2. Töötajate pildid	S1 K1 R0 T0
4.3. Töötajate töölepingute info	S1 K1 R0 T1
4.4. Ettevõtte struktuur	S1 K1 R0 T1

4.5. Ettevõtte koosseisu info	S1 K1 R0 T1
4.6. Töötajate palgamäärad	S1 K1 R0 T1
4.7. Puhkuste register	S1 K1 R0 T1
4.8. Distsiplinaarkaristuste register	S1 K1 R0 T1
4.9. Materiaalse vastutuse lepingute register	S1 K1 R0 T1
4.10. Töötajate tööaja arvestuse süsteemi info	S1 K1 R0 T1
5. Juhtimisinfosüsteemi info	
5.1. Sadama põhitegevust toetavate süsteemide info	S1 K1 R1 T1
5.2. Kauba- ja sadamatasude arvestuse süsteemide info	S1 K1 R1 T1
6. Registrite haldamise süsteemi info	
6.1. Laevade register	S0 K1 R1 T1
6.2. Klientide register	S0 K1 R1 T1
6.3. Sadamate register	S0 K1 R1 T1
6.4. Veoste register	S0 K1 R1 T1
6.5. Riikide register	S0 K1 R1 T1
6.6. Teenuste register	S0 K1 R1 T1
6.7. Arvutiprogrammide kasutajate register	S1 K0 R0 T0
7. Laevade sadamakülastuste info	
7.1. Laeva tehnilised andmed ja lipuriik (laevade registri abil)	S0 K1 R1 T1
7.2. Saabumise (väljumise) number	S0 K1 R1 T1
7.3. Laeva saabumise (väljumise) aeg	S0 K1 R1 T1
7.4. Laeva agent (klientide registri abil)	S0 K1 R1 T1
7.5. Operaatorfirma (klientide registri abil)	S0 K1 R1 T1
7.6. Lasti nimetus (veoste registri abil)	S1 K1 R1 T1
7.7. Lossitud või lastitud kogus	S0 K1 R1 T1
7.8. Reisijate arv	S0 K1 R1 T1
7.9. Saabuva laeva lähtesadam	S1 K1 R1 T1
7.10. Väljuva laeva sihtsadam	S1 K1 R1 T1
7.11. Laevade paigutuse ja kaide kasutamise info	S0 K0 R0 T0

7.12. Punkerdamislaevade sadamakülastuste ja laadimisoperatsioonide	S0 K1 R1 T1
8. Laadimisoperatsioonide planeerimise ja arvestuse süsteemi info	
8.1. Sadamatesse saabuvate laevade info	S1 K1 R1 T1
8.2. Laevade laadimis- ja lossimisinfo	S1 K1 R1 T1
8.3. Vagunite laadimis-, lossimisinfo	S1 K1 R1 T1
8.4. Ohtlike kaupade info	S1 K1 R1 T1
8.5. Operaatorfirmade igakuised veoste töötlemise plaanid jms tootmisinfo	S1 K1 R1 T1
9. Sadama riist- ja tarkvara registri info	S0 K0 R0 T1
10. Sadama tootmisinfo koostööpartneritele	
10.1. Sadamatesse saabuvate laevade info	S1 K0 R1 T1
10.2. Sadamates olevate laevade info	S1 K0 R1 T1
10.3. Laevade register	S0 K0 R1 T1
10.4. Veoste register	S0 K0 R1 T1
11. Majandusarvestuse tarkvara Concorde XAL	
11.1. Moodul: Pearaamat	
11.1.1. Kontoplaan ja pearaamatu kanded	S1 K1 R1 T1
11.1.2. Dimensioonid	S1 K1 R1 T1
11.1.3. Tulu ja kulukontode eelarve	S1 K1 R1 T1
11.1.4. Alaeelarved ja kulujuhid	S1 K1 R1 T1
11.2. Moodul: Müük / Klient	
11.2.1. Klientide register	S1 K1 R1 T1
11.2.2. Kliendiga seotud lepingud	S1 K1 R1 T1
11.2.3. Kliendile väljastatud arved	S1 K1 R1 T1
11.2.4. Raha laekumised kliendilt	S1 K1 R1 T1
11.3. Moodul: Hange / Hankijad	
11.3.1. Hankijate register	S1 K1 R1 T1
11.3.2. Hankijatelt saadud arved	S1 K1 R1 T1
11.3.3. Hankijatele tehtud maksed	S1 K1 R1 T1

11.3.4. Muude maksete register	S1 K1 R1 T1
11.4. Moodul: Ladu	
11.4.1. Müüdavate teenuste register	S1 K1 R1 T1
11.4.2. Müügikäibed objektide lõikes	S1 K1 R1 T1
11.4.3. Müügieelarve	S1 K1 R1 T1
11.5. Moodul: Põhivara	
11.5.1. Põhivarade klassifikaator	S1 K1 R1 T1
11.5.2. Põhivarade register	S1 K1 R1 T1
11.5.3. Põhivarade liikumine	S1 K1 R1 T1
11.5.4. Põhivaradega seotud rendilepingud	S1 K1 R1 T1
11.6. Moodul: Palk	
11.6.1. Sadama tegevkoosseisus olevate ja töölepingu lõpetanud töötajate isikuandmed	S1 K1 R1 T1
11.6.2. Töölepingute info	S1 K1 R1 T1
11.6.3. Palgamäärad	S1 K1 R1 T1
11.6.4. Tööaja tabeli info	S1 K1 R1 T1
11.6.5. Puudumiste info	S1 K1 R1 T1
11.6.6. Palgaarvestused	S1 K1 R1 T1
11.6.7. Tasuliikide register jms info	S1 K1 R1 T1

Приложение 2. Матрица ИТ рисков

		Продукты Microsoft	SQL, Oracle сервер	DNS сервер	Корпоративная сеть
		V01	V02	V03	V04
Утечка информации о клиентах к конкурентам через незащищенный канал связи	T01	-	**R**	-	-
Поставка программного обеспечения и данных - вирусы или испорченные данные.	T02	-	-	**R**	-

Случайное или злоумышленное причинение вреда к информации в базах данных и интернету	T03	-	-	-	**R**
Угрозы нарушения работоспособности системы, программного обеспечения	T04	**R**	-	**R**	-
Угрозы целостности данных, программ, аппаратуры	T05	-	**R**	-	-
Угрозы доступности данных	T06	-	**R**	**R**	-
Угрозы канала связи	T07	-	-	-	**R**

Приложение 3. Идентификация ИТ рисков

Риск id	Величина ущерба id	Величина уязвимости id	Распознанные риски	Вероятность	Воздействие	Уровень риска	Индикатор риска
R01	T01	V02	да	2	существенное	средний	-
R02	T02	V03	да	2	существенное	средний	-
R03	T03	V04	да	2	крупное	высокий	NB!
R04	T04	V01	да	2	крупное	высокий	NB!
R05	T04	V03	да	1	незначительное	низкий	-
R06	T05	V02	да	2	крупное	высокий	NB!
R07	T06	V02	да	2	крупное	высокий	NB!
R08	T06	V03	да	1	незначительное	низкий	-
R09	T07	V04	да	1	незначительное	низкий	-

Приложение 4. Уменьшение ИТ рисков

Риск id	Распознанные риски	Уровень риска	Преобразование риска	Пояснение	Собственник риска
R01	да	средний	избегать		Отдел персонала
R02	да	средний	принятие		ИТ отдел
R03	да	высокий	минимизирование		ИТ отдел
R04	да	высокий	минимизирование		ИТ отдел
R05	да	низкий	принятие		ИТ отдел
R06	да	высокий	минимизирование		ИТ отдел
R07	да	высокий	минимизирование		Отдел бухгалтерии
R08	да	низкий	принятие		Отдел бухгалтерии
R09	да	низкий	принятие		ИТ отдел

Риск id	Ответственный за риски	Планируемая дата	Владелец ответсвенного за риск	Статус риска	Статус дня
R01	ИТ одел	01.02.2011	Таллиннский порт		
R02	ИТ одел	01.02.2011	Таллиннский порт		
R03	ИТ одел	01.02.2011	Таллиннский порт		
R04	ИТ одел	01.02.2011	Таллиннский порт		
R05	ИТ одел	01.02.2011	Таллиннский порт		
R06	ИТ одел	01.02.2011	Таллиннский порт		
R07	ИТ одел	01.02.2011	Таллиннский порт		
R08	ИТ одел	01.02.2011	Таллиннский порт		
R09	ИТ одел	01.02.2011	Таллиннский порт		