МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ АВТОМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра Автоматизированных систем управления

ОТЧЕТ ПО ПРАКТИКЕ

Учебная практика: ознакомительная практика

(наименование практики в соответствии с учебным планом)

Направление подготовки: 09.04.03 Прикладная информатика
профиль: Интеллектуальный анализ и управление в социально-экономических системах

Выполнил:		**Проверил:**	
Студент	*Нерянов П.А..*	Преподаватель	*Муртазина М.Ш., Доцент кафедры АСУ, к.т.н..*
Факультет	*АВТФ*		
Направление (специальность) подготовки	*09.04.03– Прикладная информатика*	Балл: _____	
Группа	*АПМ2-20*	Оценка _____	
Шифр	013455911		

_____ подпись
Дата сдачи: «__»_____20__г.

_____ подпись
Дата защиты: «__»_____20__г.

Новосибирск 2021

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Управления рисками информационной безопасности и выполнение мероприятий по снижению, выявленных рисков до требуемого уровня, является обязательным требованием при проектировании информационной сети компании и обеспечению её безопасности. Во многих кредитных организациях уже давно сложилась практика управления рисками информационной безопасности, основу которой составляют определение актуальных угроз ИБ и планирование мероприятий по их нейтрализации.

Корпоративная сеть является узким звеном предприятия, учитывая глобальную тенденцию к росту числа информационных атак, приводящих к значительным финансовым и материальным потерям. Согласно данным предоставленным главой МВД, только за январь-июнь 2020г. рост IT-преступности в России составил 91,7% по сравнению с аналогичным периодом прошлого года [1].

Обеспечение информационной безопасности является сложной задачей, для решения которой необходима комплексная система, которая призвана не допускать утечек информации, а также препятствовать проникновению третьих лиц в сеть компании. Проектирование такой системы включает организационно-технические, экономические и правовые методы.

1 Теоретико-методологические основы управления рисками информационной безопасности в корпоративной сети компании

1.1 Управление рисками информационной безопасности как область знаний

Риски информационной безопасности в корпоративной сети — это предпосылки к возникновению прямого или косвенного ущерба для компании. Данный ущерб может отразится на работе компании и привести к потере выгоды, что вследствие может привести к банкротству. Всеми процессами при ведении бизнеса необходимо управлять и выделять на это необходимые ресурсы-активы.

Актив - основные ценные ресурсы предприятия. Данные ресурсы являются доходом предприятия. На данный момент разделяют материальные, финансовые, человеческие, информационный активы и процессы.

Материальные активы — это предметы, которые имеют физическое содержание и могут быть использованы для производства или поставки продуктов и услуг. С точки зрения бухгалтерского учета, материальные активы также включают договоры аренды или акции компании. По сути, они являются основными активами организации и могут отличаться от нематериальных активов, таких как деловая репутация, товарные знаки или патенты, которые не имеют физического содержания, но по-прежнему являются ценными концепциями и активами [2].

Финансовые активы — это денежные средства, право требовать по договору денежные средства или другой финансовый актив, право обмена на другой финансовый инструмент, долевой инструмент [3].

Процесс (актив) — это главный актив, он используется для достижения необходимых целей компании объединяя в себе остальные активы организации.

Еще один актив для компании - её репутация. Информационная безопасность неотъемлемая часть имиджа компании. При утечке конфиденциальных данных пользователи перестают доверять компании, и её репутация на рынке стремительно падает. Для примера обычный сбой в работе сервера компании, предоставляющей свои товары онлайн может повлиять на его доступность для потенциальных покупателей. Вследствие этого потенциальные потребители приобретут товар у конкурентов, что повлечет к финансовым потерям. Так же для восстановления правильной работы сервера необходимо привлекать человеческие активы переводя их с другого бизнес-процесса, вызывая дефицит ресурсов уже на нём. Всё это влияет на репутацию компании.

Из приведенного примера видно, что бизнес-процессы в организации подвершены большому количеству факторов риска (внутренние и внешние).

У каждой компании существуют более важные активы (основные) и активы, которые менее важны (вспомогательные). Например, если организация занимается управлением финансов (кредитная деятельность, инвестиции и т.д.), то для неё основные активы это финансовые. Для предприятия, специализирующегося на продаже недвижимости, оборудования, ресурсов основные это материальные активы. Если бизнес основан на наукоемкой отрасли или разработки ПО и информационной собственности, то для него важнейшим являются информационные активы.

В каждой компании существуют различные по значимости активы. Например, если в компании произошел риск при использовании основных активов, то это чревато потерей бизнеса. Однако если риск произошел среди вспомогательных активов, то данный ущерб возможно возместить. Именно поэтому ликвидация рисков основных активов является приоритетной задачей глав компании и её сотрудников. В то время как решение рисков второстепенных активов может быть вообще отправлено на аутсорсинг, т.к.

от них зависит в большинстве случаев лишь эффективность управления в организации.

Т.к. не для всех компаний риски информационной безопасности являются основными, то возможны различные способы их управления. Данные способы различаются глубиной и рассчитаны на различное участие информационных активов в производственном процессе компании.

Первый способ рассчитан на компании, в которых информационные активы – вспомогательные активы, а уровень информатизации низок, т.е. оценка информационных рисков для такой компании не является приоритетной задачей. Такой организации при своей работе рекомендуется базовое обеспечение информационной безопасности согласно существующим нормам и стандартам ISO/IEC. Данные нормы и стандарты помогут владельцам компании или лицам, которые занимаются ликвидацией данных рисков на аутсорсинге, т.к. актив является вспомогательным, определить механизмы, которые применимы для данной компании.

Второй способ рассчитан на компании, в которых информационные активы по-прежнему являются вспомогательными активами, однако уровень информатизации высокий, т.е. при их возникновении возможен ущерб основным бизнес-процессам. В таком случае рекомендуется так же использовать базовое обеспечение информационной безопасности согласно существующим нормам и стандартам ISO/IEC и уделить особое внимание наиболее важным участкам.

Третий способ рекомендуется использовать IT-компаниям и рассчитан на глубокий уровень управления. Используется формальный подход и качественные методы.

На практике в компаниях не редки случаи одновременного использования нескольких основных активов с равной степенью важности. Для примера возьмем компанию, в которой два важных основных актива – человеческие и информационные ресурсы. Таким образом, в данной

компании наиболее эффективно будет провести высокоуровневый подход оценки рисков для определения систем и их рисков с критической важностью для функционирования бизнес-процессов компании, и с последующим выявлением риском в системах, определенных на предыдущем этапе. А для остальных рисков воспользоваться базовым обеспечением информационной безопасности согласно существующим нормам и стандартам ISO/IEC.

Понятие риска

Существуют различные точки зрения на понятие риска.

Риск как возможность - имеет в своем основании концепцию существования взаимосвязи между риском и доходностью [4]. Выше риск, следовательно, выше и доход, однако в то же время и вероятность потерпеть убытки. Так как риск является вероятностной величиной, то он имеет два исхода: наличие риска или его отсутствие. Если риск произошел, то существуют три его вариации:

1) отрицательный (убытки),

2) нулевой (безубыточность, бесприбыльность),

3) положительный (прибыль).

Под экономическим риском понимается стоимостное выражение события, ведущего к потерям. Поскольку возможный убыток измеряется в денежном выражении, величина (уровень) риска также выражен в денежных единицах. Можно выделить следующие особенности экономического риска:

- Случайная возможность возникновения убытка;
- Денежное измерение убытка,
- Нежелательность возникновения убытка,
- Наличие возможностей предотвращения убытка или самого события,
- Количественная оценка риска.

Нулевой риск обеспечивает наименьший доход, а наивысшем риске прибыль может иметь наибольшее значение, т.е. высокий риск связан с вероятностью извлечения большего дохода.

Риск как опасность или угроза - возможность наступления событий с негативными последствиями, т.е. возможность реализации предполагаемой опасности [4]. Нет уверенности в том, что это событие произойдет, но его возникновение повлечет неблагоприятный исход: возникновение потерь (недополучение доходов), помешает получить заданный результат, снизит качество или надежность этого результата и т.п.

Под риском понимается возможная опасность потерь, вытекающая из специфики тех или иных явлений природы и видов деятельности человека.

Риски информационной безопасности рассматриваются именно в рамках данной формулировки. Таким образом цель управления будет заключаться в распределении ресурсов для минимизации вероятности возникновения неблагоприятных событий.

Риск как неопределенность - наличие неопределенных факторов, при которых возникает возможность возникновения непредусмотренных событий, приводящих к отличию действительного исхода от планируемого [4].

Неопределенность носит объективный характер, обусловленный наличием факторов недетерминированной природы, благодаря которым конечный результат принимаемого решения не может быть однозначно определен. В этом случае результат фактически может быть определен как вероятностный выбор из пространства исходов.

Любая целенаправленная деятельность человека, направлена в будущее, т.е. всегда существует временной разрыв между начальными усилиями, сопровождающимися затратами ресурсов и конечным результатом. Отсюда следует, что конечный результат заведомо не детерминирован.

Неопределенность - атрибут и фактор принятия решений [5]. Неопределенность показывает факторы недетерминированной природы, их наличие и влияние, которое они оказывают на результат принятия решения;

Существуют следующие причины неопределенности:

1. Незнание − неполнота знаний и представлений об ситуации,

2. Случайность. Спланировать каждый случай невозможно,

3. Противодействие − технические аварии и сбои, действия нарушителей др.

Наиболее рациональным подходом к определению риска является понимание его как совокупности вероятности события и тяжести его возможных последствий/размера ущерба. Именно такой подход принят в стандартах управления рисками информационной безопасности [6].

Факторы риска

Факторы риска – потенциально опасные участки системы: ценные ресурсы предприятия или факторы и события, при которых возможен ущерб системе.

Подходы, описанные выше при своем исполнении, оперируют факторами риска, на основе которых принимается решение какую применить контрмеру для ликвидации риска. Для рисков информационной безопасности выделяют 7 факторов риска:

- Основные ценные ресурсы предприятия (Активы),

- Ущерб - затраты на восстановление системы в работоспособное состояние после возможного инцидента информационной безопасности, а также на восстановление искаженной, утерянной информации или же нейтрализации последствий утечки конфиденциальной информации [7],

- Угроза - потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба [8],

- Уязвимость - присущие объекту информатизации свойства, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные особенностями процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным

обеспечением и аппаратной платформой, а также условиями эксплуатации [9],

- Механизм контроля – эффективное управление участниками бизнес-процесса управлении рисками,

- Материальные и финансовые потери,

- Банковские операции.

Оценка рисками информационной безопасности и методы анализа применяются согласно выбранной в компании методологии. Данный процесс состоит из двух этапов: анализ рисков и оценка рисков.

При анализе рисков следуют следующей последовательности:

Для начала члены компании определяют основной(-ые) активы компании и определяют их ценность. Далее выявляют потенциальные угрозы для данных активов, вероятность их возникновения и убытки. Заключающей фазой этапа является определения вероятности уязвимости организации.

При оценке рисков члены компании под руководством начальства отвечают на следующий вопрос: Какой уровень риска (материальные и финансовые потери) является приемлемым для организации.

По результатам ответа на данный вопрос (оценки рисков), получают риски, из-за которых текущий уровень риска не соответствует (соответствует) требованиям компании.

Процесс оценки рисков заключается в следующем:

На начальном этапе выбирается способ обработки риска и механизмы контроля. Далее происходит оценка эффективности выбранных способов и методов. В конце составляется план обработки рисков, в котором учитывается стоимость контрмер и сроки их реализации.

Оценка рисков

При оценке рисков необходимо продумать последовательность всех шагов и необходимую для них детализацию выполнения. В классических методиках предусмотрено определение и оценка активов, определение

уязвимостей, разработка модели угроз и модели нападения. Формализованные результаты необходимо оценить, классифицировать и графически отобразить.

При оценке рисков определяется его вероятность для нахождения величины ущерба. Есть два метода для определения вероятности риска: прогнозированием (на основе обнаруженных уязвимостей и потенциальных нападающих) или на основе существующей статистики (классификация уязвимостей).

CVSS (common vulnerability scoring system) – одна из систем классификации уязвимостей, которая позволяет определить основные характеристики уязвимости и получить числовую оценку, и преобразовать её в качественное представление (например, низкое, среднее, высокое и критическое), чтобы помочь организациям правильно оценить и определить приоритеты своих процессов управления уязвимостями [10].

Ущерб определяется для каждого актива с обнаруженной уязвимостью. Величина ущерба не во всех случаях является денежной или процентной величиной. Так как в большинстве случаев полученные результаты в таком виде представить невозможно из-за методов оценки рисков.

Процесс анализа рисков является не тривиальной задачей. Для успешности данного процесса необходимо учесть множество факторов, поэтому использование одних лишь методических рекомендаций будет недостаточно для получения требуемого результата. Таким образом помимо методических рекомендаций необходимо выбрать инструментарий с поддержкой необходимых методов и стандартов, а также соблюсти регламент управления рисками. Данный процесс помимо информационных ресурсов неразрывно связан и с человеческими активами, т.е. различными структурными подразделениями компании и привлечением в процесс менеджеров компании, которые обеспечат управление структурных подразделений.

1.2. Модели и методы мониторинга информационной безопасности в корпоративной сети компании

1.2.1 Процессная модель управления рисками

Стандарт BS 7799-3[11] и наследуемый от него ISO 27001[12] определяют существующие 4-х фазные процессные модели управления рисками. Определяют 4 фазы процессной модели: планирование, реализация, проверка, действия.

1 фаза – Планирование. Во время исполнения данной фазы происходит выбор методики управления рисками и производится оценка рисков и требуемого уровня рисков.

2 фаза – Реализация. Выполняется обработка рисков, обнаруженная на предыдущей фазе, и применяются необходимые механизмы устранения для обнаруженных рисков (игнорирование, минимизация, ликвидация, экстрадирование).

3 фаза – Проверка. Производится аудирование существующих механизмов контроля, который проходит в 3 этапа: разработка регламента проведения аудита, сбор информации, составление отчета уровня безопасности.

4 фаза – Действия. По результатам проведенного аудита, в случае необходимости, производятся действия, связанные с переоценкой рисков, а также изменением выбранных методов оценки и управления рисками.

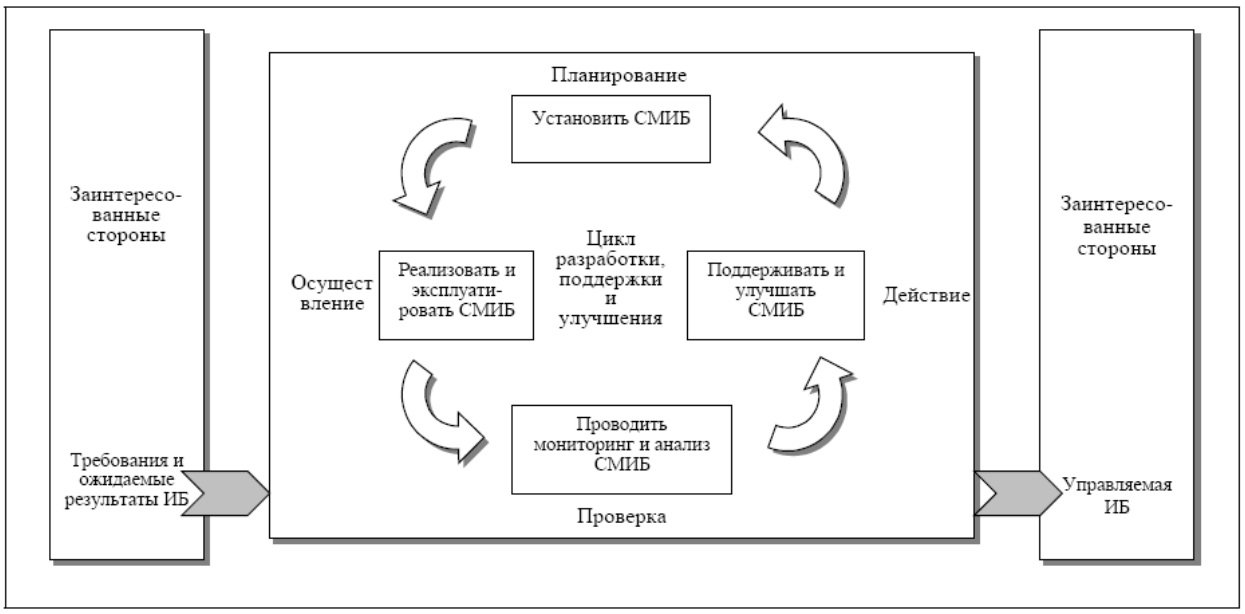

Рисунок 1 – 4-х фазная процессная модель управления рисками

1.2.2 Методы управления рисками

Существует большое множество методов управления рисками, как количественные, так и качественные, поэтому методы управления рисками можно разделить следующим образом:

1) качественные методы,

2) количественные методы,

3) сочетание качественных и количественных методов (смешанные методы).

На данный момент не существует явных причин, при которых строго регламентирован выбор того или иного метода управления. Приведем некоторые из наиболее известных методов управления рисками, которые хорошо себя зарекомендовали.

OCTAVE – Оценка критичных угроз, активов и уязвимостей (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [13]. Данный метод рассчитан на организации различных сфер и объёмов производства, и состоит из 3-х этапов, не включающих планирование. Во время планирования разрабатывается график семинаров и назначение ролей.

Первый этап состоит из оценки активов, анализа законодательных требований, определения угроз и вероятности возникновения риска.

Второй этап заключается в анализе обнаруженных уязвимостей на прошлом этапе при оценке активов компании.

На третьем этапе производится оценка и обработка рисков, разработка контрмер по их устранению, а также вычисление ущерба, как величины потерь организации за календарный год.

Другой метод оценки рисков - CRAMM (CCTA Risk Analysis and Management Method)[14]. Основа данного метода — это оценка рисков посредством проведения опросов. Данный метод востребован большим количеством компаний из-за удобного программного обеспечения для управления. Данное ПО содержит постоянно обновляющуюся базу знаний рисков и контрмер, а также возможность определить величину риска.

Различие с предыдущим методом заключается в подготовительном этапе и последовательности действий. Подготовительный этап в данном случае заключается в определении целесообразности проведения оценки рисков и уже при необходимости проводится глубокая оценка рисков. В противном же случае используются способы, уже содержащиеся в базе знаний инструментария CRAMM.

Первый этап заключается в оценке активов и определяются связи между различными активами.

Второй этапе заключается в оценке рисков и его вероятности. Риски определяются для связки: Ресурс-Угроза-Уязвимость. Контрмеры к рискам на данном этапе не производятся.

Заканчивается анализ определением контрмер к обнаруженным рискам на основе базы знаний CRAMM. Полученный результат сравнивается с требуемым уровнем рисков.

Метод FRAP (Facilitated Risk Analysis Process) является качественным методом. В методе FRAP используются следующие этапы при оценке рисков:

- Определение защищаемых активов (автоматизированный анализ сети),

- Идентификация угроз,

- На основе идентифицированных угроз производится возможная оценка нанесенного ущерба (по следующим уровням: - Низкий; -Средний; - Высокий),

- Определение контрмер согласно выявленным угрозам,

- Документирование.

Таким образом, основным достоинством данного метода является использование минимальных трудозатрат. К минусам такого подхода можно отнести отсутствие глубокой декомпозиции при анализе угроз, а также отсутствие возможности оценки рисков в денежном эквиваленте.

Многие методы основное свое внимание уделяют построению комплексного процесса управления рисками, а вопросы непосредственной оценки рисков рассматривается весьма поверхностно. Метод FAIR (Factor Analysis of Information Risk) разработан для устранения этого недостатка. Он не является самостоятельным методом по управлению рисками, но может использоваться в дополнение ко многим другим методам. FAIR анализ подразумевает следующую последовательность операций: 1) Сбор данных по каждому фактору; 2) Экспертная оценка; 3) Анализ сценарий для каждого фактора (использование калиброванных значений PERT); 4) Использование инструментов стохастического моделирование (метод Монте-Карло) [15, с. 93]. Основу при факторном анализе информационных рисков составляет декомпозиция рисков на частоту появления инцидента и вероятность потерь от его наступления. А также последующую декомпозицию каждого события. Так как автор данной метода рекомендует использовать его в сочетании с другим методом, основанным на качественно оценке. Главным минусов данного метода является её несамостоятельность и узкая направленность.

Однако, данный метод позволяет проводить глубокую декомпозицию при анализе угроз.

Другой метод, представленная корпорацией Microsoft в 2006г. является методом, который использует как качественную, так и количественную оценку угроз. Аналитика рисков, согласно методу Microsoft, позволяет проводить оценку потенциальных рисков, связанных с инсайдерской деятельностью в организации, без настройки каких-либо политик риска, связанных с инсайдерской деятельностью. Эта оценка может помочь организации определить потенциальные области повышенного риска пользователей и определить тип и область политики управления рисками, которые можно настроить [16].

Данный метод включает в себя следующих 4 этапа:

1) Оценка рисков,

2) Поддержка принятия решений,

3) Реализация контроля,

4) Оценка эффективности программы.

Такой подход к управлению рисками информационной безопасности позволяет использовать непрерывный цикл реализации процесса и охватить все аспекты том числе и эффективность процесса управления рисками. Конечно, у такого подхода тоже имеются свои минусы, такие как высокая трудоемкость процесса и дополнительные затраты т.к. не подразумевает использование типовых рисковых сценарий.

Выбор метода, который необходимо использовать на предприятии является не тривиальной задачей. При выборе метода нужно учитывать такие аспекты как необходимость детального изучения рисков информационной безопасности и необходимые трудозатраты для реализации процесса. Таким образом, для различных организаций будет правильной свой метой, однако разрабатываемый компанией метод должен соответствовать потребностям

организации, обеспечивать повторное использование ранних результатов и быть прозрачной для всех заинтересованных сторон в компании.

Оценка рисков зачастую является циклическим процессом. Допустим выявив некоторый риск, и затем проведя необходимые процедуры для минимизации его влияния на бизнес-процесс необходимо снова провести оценку влияния данного риска, для оценки эффективности проведенным контрмер. Так же при оценке рисков необходимо использовать базу данных для хранения информации обо всех этапах оценки (документация, используемые стандарты, реестры ресурсов, текущие перечни уязвимостей и др.) и алгоритм для работы с данными.

Инструментарии, которые предлагают такие возможности существует многое количество. Например RA2[17], который поддерживает метод CRAMM и стандарты ISO 27001 или vsRisk[18], Callio Secura 17799[19], которые в своей работе запрограммированы на следование стандартов BS 7799-3. Помимо зарубежных существуют и отечественные системы для автоматизации управления рисками. Один из них это РискДетектор[20].

Использование систем для автоматизации управления рисками позволяет проводить многократный циклический процесс переоценки рисков. Так же появляется возможность комфортной работы со всеми данными по оценки рисков бизнес-процессов, а более продвинутые инструментарии могут содержать и дополнительные средства для работы (разработка реестров ресурсов, документирование СУИБ и др.).

ЗАКЛЮЧЕНИЕ

Процесс анализа рисков является не тривиальной задачей. Для успешности данного процесса необходимо учесть множество факторов, поэтому использование одних лишь методических рекомендаций будет недостаточно для получения требуемого результата. Таким образом помимо методических рекомендаций необходимо выбрать инструментарий с поддержкой необходимых методов и стандартов, а также соблюсти регламент управления рисками. Данный процесс помимо информационных ресурсов неразрывно связан и с человеческими активами, т.е. различными структурными подразделениями компании и привлечением в процесс менеджеров компании, которые обеспечат управление структурных подразделений.

СПлжИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Состояние преступности в России за январь-июнь 2020 года: статистический сборник. М.: ГИАЦ МВД РФ, 2020.
2. Sutherland J., Canwell D. Tangible asset. – 2004.
3. Исакова С. А. Финансовые активы и финансовые обязательства в условиях перехода на МСФО (НСФО 2) //Международный бухгалтерский учет. – 2012. – №. 24.
4. Акимов В. А., Воронов С. П., Радаев Н. Н. Концепции риска и концепции анализа риска //Стратегия гражданской защиты: проблемы и исследования. – 2013. – Т. 3. – №. 2.
5. Диев В. С. Неопределенность как атрибут и фактор принятия решении. – 2010.
6. BS 7799-3:2006 – Information security management systems – Guidelines for information security risk management и ГОСТ Р ИСО/МЭК 27005–2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
7. Галатенко В.А. Основы информационной безопасности. М., 2004. 264 с.
8. Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.]. М.: Радио и связь. 2001.
9. Муханова А., Ревнивых А. В., Федотов А. М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах //Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2013. – Т. 11. – №. 2.
10. FIRST [Electronic resource]. – URL: https://www.first.org/cvss/ (accessed 11.06.2021)
11. BS 7799-3: 2006. Information security management systems – Part 3. Guidelines for information security risk management (Руководство по управлению рисками ИБ)
12. ISO/IEC 27001 — Information security management. [Electronic resource]. – URL: https://www.iso.org/isoiec-27001-information-security.html (accessed 11.06.2021)
13. Alberts C. J., Dorofee A. J. Managing information security risks: the OCTAVE approach. – Addison-Wesley Professional, 2003.
14. Mullerova J., Orincak M. RM/RA CRAMM-Quantitative Risk Assessment Method for Prevention of Criminality //Security Dimensions. ISSN. – 2017. – Т. 23537000. – С. 131-144.
15. Freund J., Jones J. Measuring and managing information risk: a FAIR approach. – Butterworth-Heinemann, 2014.
16. Управление внутренними рисками [Электронный ресурс]. – URL: https://docs.microsoft.com/ru-ru/microsoft-365/compliance/insider-risk-management (доступ 26.04.2021).

17. EUROPIAN UNION AGENCY FOR CUBERSECURITY. [Electronic resource]. – URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ra2.html (accessed 12.06.2021).

18. IT Governance vsRisk. [Electronic resource]. – URL: https://store.softline.ru/itgovernance/it-governance-vs-risk/ (accessed 12.06.2021).

19. Искусство управления информационными рисками. Callio Secura 17799 [Electronic resource]. – URL: http://xn----7sbab7afcqes2bn.xn--p1ai/content/callio-secura-17799 (accessed 12.06.2021).

20. РискДетектор. Система автоматизации управления рисками, аудита, мониторинга, контроля фундаментальности безопасности, обеспечения качества критериев и нормативной базы. [Electronic resource]. – URL: http://www.srisks.ru/ (accessed 12.06.2021).