Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение
высшего профессионального образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Школа инженерного предпринимательства
Направление подготовки 38.04.02 менеджмент
Кафедра менеджмента

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Роль организационной культуры в управлении информационной безопасностью стартапов

УДК 004.056:005.922.1

Студент

Группа	ФИО	Подпись	Дата
3АМ6Ф	Коробков Е.И.		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
заведующий кафедры	Чистякова Н.О.	к.э.н.		

КОНСУЛЬТАНТЫ:

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Черепанова Н.В.	к.ф.н.		

Нормоконтроль

Должность	ФИО	Ученая степень, звание	Подпись	Дата
ст.преподаватель	Громова Т.В.			

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
менеджмента	Чистякова Н.О.	к.э.н.		

Томск – 2017 г.

Планируемые результаты обучения по ООП 38.04.02 «Менеджмент»

Код результата	Результат обучения (выпускник должен быть готов)
	Общепрофессиональные и профессиональные компетенции
$Р_1$	Способность применять теоретические знания, связанные с основными процессами управления развитием организации, подразделения, группы (команды) сотрудников, проекта и сетей; включающие в себя современные подходы по формированию комплексной стратегии развития предприятия, в том числе в условиях риска и неопределенности
$Р_2$	Способность воспринимать, обрабатывать, анализировать и критически оценивать результаты, полученные отечественными и зарубежными исследователями управления; выявлять и формулировать актуальные научные проблемы в различных областях менеджмента; формировать тематику и программу научного исследования, обосновывать актуальность, теоретическую и практическую значимость избранной темы научного исследования; проводить самостоятельные исследования в соответствии с разработанной программой; представлять результаты проведенного исследования в виде научного отчета, статьи или доклада
$Р_3$	Способность анализировать поведение экономических агентов и рынков в глобальной среде; использовать методы стратегического анализа для управления предприятием, организацией, группой; формировать и реализовывать основные управленческие технологии
$Р_4$	Способность использовать количественные и качественные методы для управления бизнес-процессами и оценки их эффективности; проектировать и управлять системой, частью системы, или процессом удовлетворяющими внутренние и внешние потребности предприятия, организации; идентифицировать, формулировать и решать производственные задачи, включающие в себя материальные, человеческие и экономические параметры
$Р_5$	Способность управлять финансовыми ресурсами предприятия; использовать современный инструментарий для диагностики финансово-хозяйственной деятельности и разработки финансовой стратегии развития предприятия и организации; владеть современными способами оценки эффективности инвестиционных программ, проектов
$Р_6$	Способность к сопровождению бизнес-процессов в разных сферах менеджмента посредством управления психологическим микроклиматом в организациях; к самоактуализации творческого потенциала работников в процессе управления, к осмыслению, прогнозированию развития и решению производственных, трудовых, межличностных конфликтов
$Р_7$	Умение сочетать управленческие, технические, экономические и др. знания для создания конкурентных преимуществ своей организации или подразделения
	Общекультурные компетенции
$Р_8$	Способность применять современные методы и методики преподавания дисциплин; разрабатывать рабочие программы и методическое обеспечение для преподавания экономических и управленческих дисциплин

P_9	Способность понимать необходимость и уметь самостоятельно учиться и повышать квалификацию в течение всего периода профессиональной деятельности, развивать свой общекультурный и профессиональный уровень
P_{10}	Способность эффективно работать индивидуально, в качестве члена команды, в том числе международной, по междисциплинарной тематике, обладая навыками публичных деловых и научных коммуникаций, а также руководить командой, подразделением, предприятием, организацией.
P_{11}	Способность владеть иностранным языком как средством профессионального общения, на уровне, позволяющем работать в интернациональной среде с пониманием культурных, языковых и социально – экономических различий деловой культуры разных стран.
P_{12}	Готовность следовать кодексу профессиональной этики, ответственности и нормам управленческой деятельности

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Школа инженерного предпринимательства
Направление подготовки 38.04.02 Менеджмент
Кафедра менеджмента

УТВЕРЖДАЮ:
Зав. кафедрой
_____Чистякова Н.О.

ЗАДАНИЕ

на выполнение выпускной квалификационной работы

В форме:

магистерской диссертации

Студенту:

Группа	ФИО
3АМ6Ф	Коробкову Евгению Игоревичу

Тема работы:

Роль организационной культуры в управлении информационной безопасностью стартапов	
Утверждена приказом директора (дата, номер)	

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Исходные данные к работе	Справочная, научная, методическая литература, научные статьи, диссертационные исследования, интернет-ресурсы, посвященные объекту исследования – информационной безопасности организации, материалы научно-исследовательской практики.
Перечень подлежащих исследованию, проектированию и разработке вопросов	Анализ основного терминологического аппарата исследования: информационная безопасность, социальные сети, организационная культура, девиация. Обосновать выбор понятия организационной культуры как

	важного фактора информационной безопасности. Рассмотреть условия ее формирования и поддержания. Рассмотреть способы обеспечения информационной безопасности посредством анализа угроз и принятия соответствующих контрмер, моделей управления, разработки политик безопасности и повышения информированности пользователей. Оценить степень влияния руководителей, организационной культуры и политик безопасности на уровень информационной безопасности в организации. Провести качественное или количественное исследование для проверки выдвинутых гипотез
Перечень графического материала	Рисунки и таблицы из текста работы
Консультанты по разделам выпускной квалификационной работы *(с указанием разделов)*	
Раздел	**Консультант**
Социальная ответственность	Черепанова Н.В.
Раздел на английском языке	Солодовникова О.В.
Названия разделов, которые должны быть написаны на русском и иностранном языках:	
Управление информационной безопасностью	Part II. Information Security Management

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	06.02.2017

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Заведующий кафедрой	Чистякова Н.О.	к.э.н., доцент		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
3АМ6Ф	Коробков Е.И.		

Реферат

Выпускная квалификационная работа содержит 90 страниц, 10 таблиц, 1 рисунок, 55 использованных источников, 1 приложение.

Ключевые слова: информационная безопасность, социальные сети, организационная культура, девиация, стартап, качественные методы исследования.

Объектом исследования является: информационная безопасность организации.

Предметом исследования является: организационные меры по повышению информационной безопасности организации.

Цель работы – оценить роль организационной культуры в обеспечении информационной безопасности организаций с точки зрения социальных сетей на примере стартапов региона Нор-Па-де-Кале.

В процессе исследования проводился анализ научной литературы, профессиональных периодических изданий и интернет-ресурсов, международных стандартов и статистической информации. Использовался метод качественного исследования (проводился опрос руководителей стартапов региона Нор-Па-де-Кале с целью выявления степени влияния социальной сети на принятие решений в области информационной безопасности).

В результате исследования было описано влияние социальных сетей и организационной культуры на информационную безопасность организации, проведено исследование стартапов.

Экономическая значимость работы заключается в возможности практического применения рассмотренных управленческих решений для обеспечения информационной безопасности.

Оглавление

Введение

Актуальность выпускной квалификационной работы. В инновационной экономике информация является источником конкурентных преимуществ. Использование социальных сетей сотрудниками способствует инновационной деятельности, создавая потенциальные лазейки в информационной безопасности (ИБ). Человек является слабым звеном в обеспечении информационной безопасности [32]. В этом смысле организационная культура как средство повышения ответственного обращения с информацией играет важнейшую роль наряду с технологическими аспектам соблюдения ИБ.

В данной работе используется многодисциплинарная концептуальная основа: социальный капитал (Дж. Коулман) [12], социальные сети (М. Грановеттер, Р. Берт) [23, 6, 7], культурологический подход к анализу девиаций (Т. Селлин, А. Коэн, Э. Сатерленд) [44, 11, 47], организационная культура (Э. Шейн) [39], теория базовых ценностей (Ш. Шварц) [42] и инновации (Й. Шумпетер, П. Друкер) [41, 18]. Проведено качественное исследование методом интервью по разработанному опроснику с шестью руководителями стартапов, которое позволило получить пригодные для изучения развернутые ответы.

Организационная культура рассматривается как средство развития ответственного поведения сотрудников при взаимодействии с информацией.

Научная новизна исследования состоит в выявлении степени влияния руководителей, организационной культуры и политик безопасности на уровень информационной безопасности в организации. В исследовании ставятся следующие вопросы:

– В какой мере организационные и индивидуальные ценности влияют на поведение сотрудников, связанное с взаимодействием с конфиденциальной информацией?

– Какое влияние оказывают меры ИБ и руководители на организационную культуру и безопасное поведение при обмене информацией?

Теоретическая значимость результатов ВКР. Ожидается, что основной теоретический вклад продолжит исследовательскую работу по информационной безопасности и, в частности, исследование мер, способствующих принятию сотрудниками поведенческих моделей в соответствии с обеспечением информационной безопасности. В этом вопросе подчеркивается важность деятельности операционных менеджеров.

Практическая значимость результатов ВКР. Практический вклад работы заключается в поиске организационных решений, при которых сотрудники могли бы обмениваться информацией через социальные сети в интересах организаций и не ставя под угрозу конкурентоспособность. А также в выявлении ценностей, лежащих в основе безопасного поведения. Этот результат позволяет разработать стратегии для продвижения этих ценностей среди сотрудников.

Предлагаются управленческие решения, которые могут быть использованы менеджерами.

Структура ВКР. Цель и задачи определили структуру ВКР.

Глава 1 посвящена роли организационной культуры и социальных сетей в обеспечении информационной безопасности. Обосновывается выбор понятия организационной культуры как важного фактора ИБ, углубляется понятие концепции ценностей, чтобы учесть условия формирования и поддержания культуры организации. Затем анализируются теории девиации. Наконец, устанавливаются рамки для анализа индивидуальных и коллективных ценностей.

Глава 2 посвящена информационной безопасности, ее внедрению на практике в организации посредством анализа угроз и принятия соответствующих контрмер, моделей управления, разработки политик безопасности и повышения информированности пользователей.

В глава 3 приводятся результаты эмпирическим испытаниям предлагаемой модели и наших исследовательских гипотез путем количественного исследования.

Глава 4 посвящена социальная ответственность компании EuraTechnologies.

Апробация результатов исследования. Результаты диссертационного исследования были использованы для защиты магистерского диплома «Информационная безопасность в стартапах: как социальная сеть влияет на принятие решений в отношении информационной безопасности» в Орлеанском университете (Орлеан, 2017 г.).

1 Роль организационной культуры и социальных сетей в обеспечении информационной безопасности

1.1 Контекст исследования

В экономике знаний, где организации всех форм и типов (компании, государственные структуры, НКО и т.д.) становятся все более взаимосвязанными, информация и ее использование является источником конкурентных преимуществ. Организации используют информацию для создания новых смыслов, знаний и принятия решений [10].

Жизнеспособность организации зависит от ее способности прогнозировать внешние изменения и учитывать их при определении стратегических целей. Организация должна иметь возможность приобретать, распространять и, прежде всего, анализировать информацию, касающуюся текущего состояния и эволюции ее социально-экономической среды. Это требует от организации внедрения и эксплуатации системы сбора, выбора, хранения и анализа информации.

Использование информационных систем упрощает деятельность организаций, но требует вложений в обеспечение безопасности. Трудности при проектировании и внедрении таких систем управления информацией [21], создают пространство для потенциальных проблем, что может обернуться крупной угрозой безопасности для организации.

В период с января по декабрь 2010 года Министерство экономики и финансов Франции стало жертвой компьютерного вторжения. «Троянский конь», внедренный в компьютерные системы, позволил неустановленным лицам осуществлять шпионаж за деятельностью этого министерства.

Государственные службы не являются единственными жертвами такого рода нападений. Группа компаний AREVA также оказалась целью хакерской атаки. Согласно докладу Сената Франции [2, с. 26], «хакеры за последние два года

смогли проникнуть в компьютерную сеть группы и взять под контроль компьютеры». Расходы компании по восстановлению и реконфигурации части информационной системы составили порядка нескольких миллионов евро. Следует также отметить, что потенциальный экономический ущерб, вызванный кражей информации, трудно оценить.

12 марта 2012 года портал «CNN Money» опубликовал статью о рисках, которые несут социальные сети для компаний, и о возможном использовании профессиональной социальной сети LinkedIn в качестве источника информации для хакеров [13]. В течение 2011 года эта сеть подвергалась критике за ее аспекты безопасности, и много статей по этому поводу появилось во время IPO. Эта сеть является важным источником информации для хакеров при планировании атаки на информационные ресурсы организаций с помощью обмана (social engineering). Бывший компьютерный хакер, а ныне консультант по компьютерной безопасности Кевин Митник отмечает, что гораздо легче обмануть кого-то, чтобы заполучить пароль и доступ к системе, чем совершать технические манипуляции и тратить усилия ради той же цели [32].

Французские компании в настоящее время массово становятся жертвами краж информации. Эти атаки направлены, в частности, на сбор информации о менеджерах, заказчиках, поставщиках, технологиях, стратегиях, особенно для экспорта. Хотя нет всеобъемлющих и надежных данных, все говорит о том, что ущерб, понесенный французской экономикой, является значительным: финансовые потери, снижение рыночной доли, снижение занятости и т.д. [2, с. 23].

Поэтому представляется целесообразным принятие организациями активных мер по защите информации. Тем не менее, в исследовании CLUSIF (Французского клуба информационной безопасности), проводимом каждые два года с участием сотен крупных компаний, отмечается, что практическое внедрение конкретных политик информационной безопасности до сих пор не

выполнено: «у 49% компаний до сих пор нет системы сбора и обработки инцидентов информационной безопасности» (CLUSIF, 2016, с. 7).

Кроме того, помимо угроз, непосредственно относящихся к компьютерным системам, также представляется интересным рассмотреть человеческий аспект информационной безопасности. Действительно, человеческий фактор часто представлен как один из основных недостатков систем безопасности, благодаря которым хакеры проникают в информационные системы компаний [1]. В дополнение к техническим аспектам ИБ сильно зависит от поведения сотрудников и их следования установленным процедурам безопасности.

Сотрудники работают с информацией, которая лежит в основе конкурентных преимуществ организации и приносит ей доход. Сотрудники используют связи своих социальных сетей для передачи и получения информации, которая выгодна как для них лично, так и для организации [23, 7].

1.2 Роль социальных сетей

Большое количество исследовательских работ по этой теме рассматривает социальные сети как источник инноваций. В действительности сети являются местами распространения и создания знаний, например, сообществами практики[1]. Организации могут эффективно использовать социальные сети, разрабатывая, в частности, организационные процедуры[2], развивая поглощающую способность[3] и динамические возможности[4].

[1] Сообщество практики (community of practice) – группа людей, объединенных общим интересом, профессией или ремеслом, сформировавшаяся естественным образом из-за общих интересов членов в конкретной области или созданная формально с целью получения знаний, связанных с конкретной областью. Именно через процесс обмена информацией и опытом с группой, члены которой учатся друг у друга, участники имеют возможность личного и профессионального развития (Э. Венгер) [55]

[2] Организационные процедуры (organizational routines) являются повторяющимися паттернами взаимозависимых действий, выполняемых несколькими субъектами (Р. Нельсон, С. Винтер) [33]

Создание новых связей социальной сети стимулирует инновационную деятельность, основанную прежде всего на появлении новых идей. Ключевые инновации в науке, технологиях, искусстве и политике возникли из творческих умов людей, бывшими узлами социальных сетей, в которых они распространяли и обсуждали свои идеи.

Однако сети часто рассматриваются лишь с точки зрения полезных аспектов для организаций. Исследование возможных негативных аспектов или других отклонений остается в научной литературе менее проработанным.

Что касается НИОКР (R&D), Э. фон Хиппель [51, с. 4-5] отмечает, что инженеры разных компаний, производящих аналогичные продукты и следующих аналогичным техническим процессам, обмениваются информацией, раскрывая ноу-хау и данные их компаний. Эти инженеры оценивают степень конфиденциальности информации. Если для них приемлемо осуществить обмен, то информация предоставляется контактному лицу. Этот «дар» порождает обязательство взаимной услуги[5].

Техническая информация является объектом неофициального обмена между компаниями, в том числе между конкурентами (С. Шрадер) [40]. Сотрудники участвуют в этом типе обмена для удовлетворения экономических интересов своих компаний. При рассмотрении вопроса о насущности обмена, участники оценивают важность информации, подлежащей обмену, и степень конкуренции между компаниями, характер личных отношений сотрудников уходит на второй план. Транзакция, оцениваемая сотрудником как слишком рискованная, отбрасывается. При этом большую роль играет принцип взаимности

[3] Поглощающая (абсорбционная) способность (absorptive capacity) – способность организации осознавать ценность новой внешней информации, усваивать ее и применять в коммерческих целях (В. Коэн, Д. Левинталь)

[4] Динамические возможности (dynamic capabilities) – совокупность различных способностей организации по адаптированию ресурсной базы с целью достижения устойчивых конкурентных преимуществ (Д. Тис, Г. Пизано, Э. Шуен) [49].

[5] Фон Хиппель ссылается здесь на работу Марселя Мосса «Очерк о даре. Форма и основание обмена в архаических обществах» (1925), чтобы объяснить взаимные (реципрокные) обмены.

(реципрокности) [40, с. 157]. Чем ценнее полученная информация, тем больше получатель «обязан» эмитенту.

Обмен информацией возможен, если:

- получатель не находится в прямой личной конкуренции с эмитентом,
- области применения обмениваемой информации различны (в этом случае бенефициарами могут оказаться обе компании),
- конкурент может получить эту информацию из других источников.

Когда конкуренты переходят к сотрудничеству и неофициально обмениваются информацией, то ценность дополнительной информации, полученной при обмене, должна превысить потерю ценности от разглашения информации конкуренту. По этой логике подразумевается, что, если конкурент получает доступ к информации, ее ценность для владельца снижается. Но если вид информации ближе к идее и «вдохновению», а не к знаниям в товарном виде («sellable truth»), то текущая ценность такой информации невелика, а потери от расширения к ней доступа невысоки. Более того, в случае мотивированности другой стороны на работу и дальнейшее развитие исходной идеи, ее ценность может быстро увеличиваться, принося дивиденды обеим сторонам. Таким образом, вместо того, чтобы рассматривать исключительно первоначальную потерю ценности информации от ее совместного использования, расширение доступа к информации такого рода влечет потенциальный чистый прирост ценности информации. (К. Крейнер и М. Шульц) [29, с. 196-197].

Независимо от того, фокусируются ли ранее рассмотренные работы на установлении новых контактов, улучшении креативных способностей или структуры социальных связей, все они показывают положительные эффекты сетей. Отрицательные эффекты остаются в значительной степени недооцененными или даже игнорируются. Так, Э. фон Хиппель, К. Крейнер и М. Шульц обсуждают преимущества социальных сетей, но не учитывают риски,

которые потенциально могут нести последние. Если негативные эффекты и признаются, то не ищутся причины и средства для их устранения.

Тем не менее, вопрос о негативных эффектах представляется актуальным. Действительно, М. Грановеттер упоминает, что сильные связи предпочтительнее при рискованном обмене. Э. Сазерленд объясняет в теории дифференциальной ассоциации, что девиация – это реализация возможностей, создаваемых связью между акторами и зависящих от ее силы.

В теории конфликта культур Т. Селлина девиантные акты являются результатом отказа от соблюдения норм организации. Таким образом, индивид, непонятый руководством, вынужден действовать девиантным образом, в то время как его цели продолжают совпадать с целями организации и «обычная девиация», то есть несоблюдение норм, становится характерным и позитивным поведением «обычного новатора».

Кроме того, исследования о взаимосвязи между социальным капиталом, социальными сетями и исследовательской деятельностью (R&D), в основном проводятся по выборкам инженеров и сотрудников-исследователей. Однако деятельность, направленная на техническую разработку или исследования, не создает большинства инноваций. Инновации стимулируют участники со всех иерархических уровней организации. По данным ОЭСР [19], около половины инновационных компаний не полагаются на R&D (Share of non-R&D innovators). Возглавляют список [26] самых инновационных работников менеджеры (76% компаний), инженеры (40%), маркетологи (39%), дизайнеры (27%) и в меньшей степени, сотрудники R&D (25%).

Таким образом встает вопрос о поиске решения для очевидного противоречия между, с одной стороны, необходимостью организаций защищать свою информацию, а с другой стороны, необходимостью поощрять сотрудников на установление новых связей и укрепление существующих социальных сетей.

В этом контексте в научной литературе фактор организационной культуры определяется как ключевой в информационной безопасности.

1.3 Организационный подход к формированию культуры информационной безопасности

Чтобы справиться с неопределенностью, в организациях создаются формализованные процедуры, механизмы контроля и санкции. Часть этих стимулирующих и ограничивающих правил являются выражением скрытой или явной политики информационной безопасности, реализованной в организации.

Хотя информационную безопасность можно рассматривать с технологической точки зрения, культурное измерение этой дисциплины еще предстоит изучить. Действительно, сегодня мы сталкиваемся с организационными и социальными аспектами, которые необходимо рассматривать как очень важный предмет для решения проблемы информационной безопасности [15, 5, 52]. Управление информационной безопасностью принимает форму разработки организационных политик и процедур, которые по своей природе подвержены интерпретациям, и должны отвечать как на предвиденные, так и на непредвиденные угрозы.

Фон Солмс объясняет [52], что организации должны учитывать все аспекты информационной безопасности. По его словам, информационная безопасность – это многомерное пространство, которое включает в себя корпоративное управление, организационную структуру, политику, передовые практики, этику, сертификацию, право, страхование, персонал, информированность, технологии, индикаторы и аудит. В международном стандарте ISO/IEC 27002:2005, который представляет свод норм и правил менеджмента информационной безопасности, говорится, что: «Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности

бизнеса, минимизации риска бизнеса, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса».

Множество исследователей сходятся во мнении, что информационная безопасность должна быть частью организационной культуры. Однако, по результатам опроса 874 сертифицированных специалистов в области информационной безопасности (CISSP)[6], составивших 25 наиболее важных проблем информационной безопасности, стоящих сегодня перед организациями, в большинстве организаций это не так [26].

[6] Certified Information Systems Security Professional (CISSP) – независимая сертификация информационной безопасности, проводимая Международным консорциумом по сертификации безопасности информационных систем (ISC)

2 Управление информационной безопасностью

Распространение и широкое использование в организациях информационных систем, подключенных к глобальной и/или локальным сетям, многократно увеличило эффективность работы многих из них, но одновременно подвергло новым угрозам. Хотя некоторые угрозы информационной безопасности организаций носят технический характер или являются результатом стихийных бедствий, многие из них являются антропогенными, будь то ошибки, упущения или злонамеренные действия, совершаемые сотрудниками или внешними акторами, такими как конкуренты, хакеры и т. д.

Эта повышенная уязвимость вынуждает большинство организаций применять контрмеры для предотвращения инцидентов, такие как технические и поведенческие меры контроля. Организации внедряют политики и процедуры безопасности информационных систем, обучение и повышение информированности в области информационной безопасности, а также санкции в отношении нарушений политики ИБ.

Тем не менее, эти меры контроля и меры безопасности эффективны только в той степени, в которой сотрудники хотят им следовать, и это особенно актуально, когда сотрудники находятся за пределами организации. Информационная безопасность является общемировой проблемой, которая касается всех участников рынка независимо от их размера или сектора деятельности.

Организации должны учитывать все аспекты информационной безопасности. Информационная безопасность – это многомерное пространство, которое включает в себя корпоративное управление, организационную структуру, политику, передовые практики, этику, сертификацию, право, страхование, персонал, информированность, технологии, индикаторы и аудит [52]. Информационная безопасность означает больше, чем предотвращение доступа

злоумышленников к конфиденциальным данным. В международном стандарте ISO/IEC 27002:2005, который представляет свод норм и правил менеджмента информационной безопасности, говорится, что: «Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации риска бизнеса, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса» [24].

Вот почему информация:

- не должна быть раскрыты посторонним лицам,
- должна быть защищена от несанкционированной модификации,
- должна быть доступна по запросу пользователей.

Стандарт ISO/IEC 27001:2005 (п. 3.4, с. 2), содержащий спецификации для внедрения Системы менеджмента информационной безопасности (СМИБ), определяет информационную безопасность как «сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность».

Информационная безопасность фокусируется на трех аспектах: конфиденциальности, целостности и доступности (пункты 3.3, 3.8 и 3.2 соответственно).

Конфиденциальность (Confidentiality) означает, что информация доступна только для тех, кто имеет соответствующие полномочия (авторизированные пользователи). Степень конфиденциальности информации зависит от ее стратегического или юридического характера. Для обеспечения конфиденциальности могут быть использованы такие механизмы безопасности как шифрование и управление доступом.

Целостность (Integrity) означает, что информация не будет изменена без предварительного разрешения. Информация должна быть точной, полной и защищенной от изменений.

Доступность (Availability) заключается в обеспечении доступности информационных, системных и других ресурсов пользователям при необходимости. Для обеспечения непрерывности доступных ресурсов используется механизм резервного копирования.

Эти три принципы обычно обозначаются аббревиатурой CIA. Однако Г. Диллон и Дж. Бэкхауз утверждают [14, с. 127-128], что принципов CIA недостаточно для обеспечения безопасности информации. Для этих авторов информационная безопасность относится не только к техническим средам, но также должна применяться к сотрудникам организации. Поэтому авторы предлагают дополнительные принципы, такие как ответственность, доверие и этичность.

В таблице 1 представлено резюме из двадцати двух принципов, предложенных исследователями и специалистами по информационной безопасности [29, с. 256]. Источниками этих требований являются три группы: практические работники, ученые и службы безопасности. При опросе этих групп наиболее часто упоминались шесть

Таблица 1 – Неисчерпывающий перечень основных принципов безопасности (Johnston et al, 2008: 254)

	Практики						Академики						Организации				
Принципы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Конфиденциальность (Confidentiality/privacy)	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
Целостность (Integrity)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Доступность (Availability)	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X
Невозможность отказа от авторства (Non-repudiation)	X	X		X									X		X		
Идентификация (Identification)	X																
Аутентификация (Authentication)	X	X			X			X					X				
Подпись (Signature)	X																
Авторизация (Authorization)	X																
Контроль доступа (Access control)	X					X		X									
Валидация (Validation)	X																
Сертификация (Certification)	X																
Отметка времени (Time-stamping)	X																
Письменное подтверждение (Receipt)	X																
Подтверждение (Confirmation)	X																
Владение (Ownership)	X																
Анонимность (Anonymity)	X																
Аннулирование (Revocation)	X																
Свидетельство (Witnessing)	X																
Полезность (Utility)					X			X									
Распоряжение (Possession)					X												
Контролируемость (Auditability/accountability)						X						X		X			X
Этика (Ethics)									X								
Источники:	1. Boykin (2003), 2. Host (2001), 3. Krauss and Tipton (2002), 4. Byrnes and Proctor (2002), 5. Parker (2002), 6. Hutt (2002)						7. Leiwo *et al.* (1999), 8. Rosenthal (2002), 9. Dhillon and Torkzadeh (2006),10. Summers (2002), 11. Long (1999), 12. Rannenberg *et al.* (1999)						13. CIECA (2003), 14.ITsecurity.com, 15. SAWG (2002), 16. OIT (2002), 17. GASSP(2003)				

Примечание. Курсивом выделены наиболее часто цитируемые принципы информационной безопасности

принципов: конфиденциальность, целостность, доступность, невозможность отказа от авторства, аутентификация и аудит. Фактически, приведенная таблица показывает, что практики информационной безопасности определяют гораздо более исчерпывающий список, чем ученые и организации безопасности. Этот список включает в себя системы доказательств (например: signature, witnessing) и отслеживания (например: timestamp).

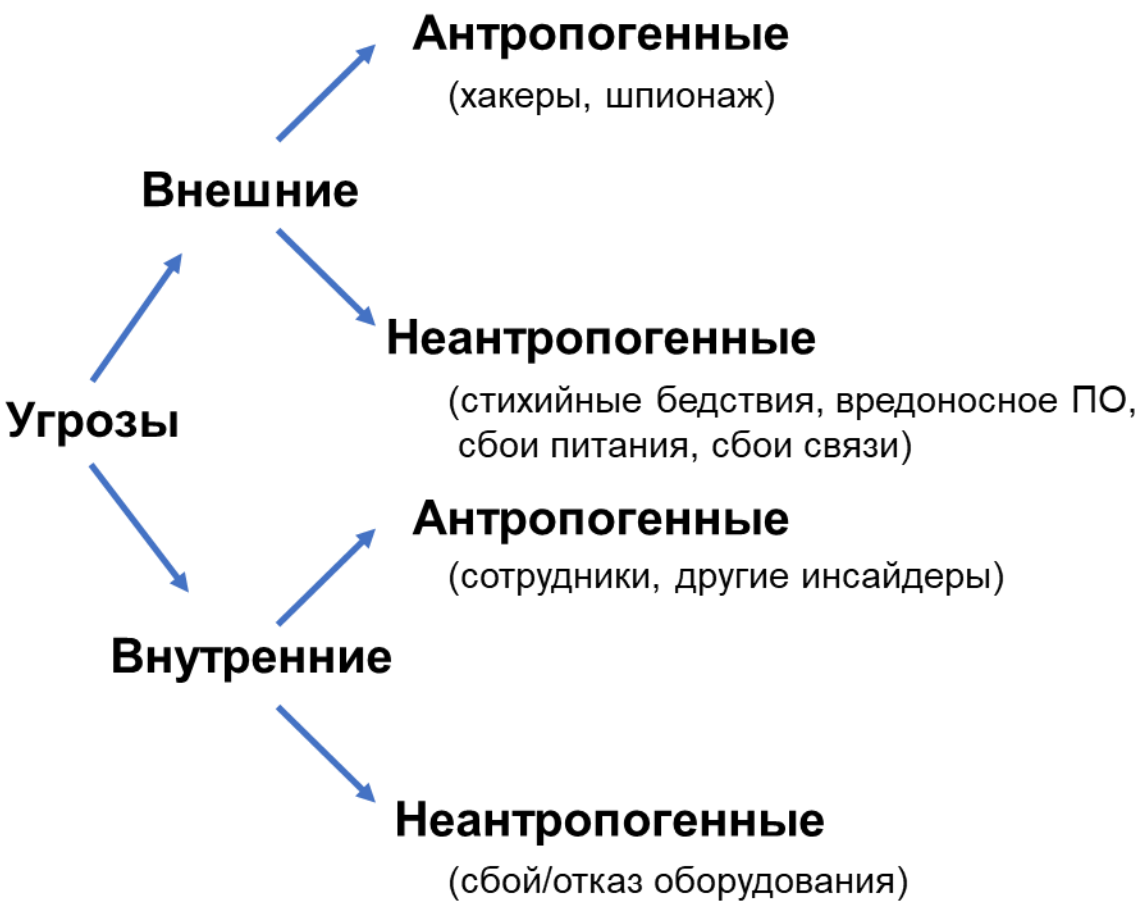
Информационная безопасность организации может быть определена как защита от кражи информации или любой другой атаки на информационные системы, а также защита от сбоев информационных систем, которые могут сделать их недоступными и могут нарушить целостность информации.

Организации и их информационные системы должна быть готовы реагировать на целый ряд угроз. Эти угрозы могут быть вызваны как действиями акторов вне организации, так и ее сотрудников. Согласно докладу Computer Crime and Security Survey [8, с. 20], 43,2% респондентов заявили, что, по крайней мере, часть их потерь была связана со злонамеренными действиями сотрудников.

2.1 Угрозы, уязвимости и контрмеры

Отчеты, подготовленные специализированными организациями, такие как Computer Crime and Security Survey, подготовленный Институтом компьютерной безопасности (CSI), или отчет, подготовленный CLUSIF (Французский клуб информационной безопасности), обычно классифицируют атаки как преднамеренные / непреднамеренные и внутренние / внешние (см. Рисунок 1).

Рисунок 1 – Классификация угроз



Во многих публикациях приводятся более подробные классификации угроз [16, 8]. Ниже некоторые из основных, разбитые на внутренние и внешние по отношению к организации.

Внешние угрозы:

- Компьютерные вирусы, черви и трояны: компьютерные программы, которые могут автоматически реплицироваться, через различные системы и сети;
- Стихийные бедствия: ущерб вызван такими явлениями, как землетрясения, наводнения или пожары;
- Спам (электронная почта): массовая рассылка нежелательных писем;

- Хакерская атака: проникновение информационных систем организации несанкционированным третьим лицом, которые затем могут свободно получать доступ и манипулировать данными (кража, модификация) или нарушать работу систем;
- Хищение информации третьими лицами, получившими доступ посредством обмана и манипулирования внутренними сотрудниками (социальная инженерия), а также из-за халатности внутренних сотрудников, которые позволяют гостям перемещаться без присмотра в помещения организации.

Внутренние угрозы:

- Установка / использование несанкционированного оборудования, периферийных устройств или программного обеспечения: эти аппаратные средства и программное обеспечение могут содержать вирусы или системы копирования информации;
- Мошенническое использование информационной системы пользователями, имеющими санкционированный доступ;
- Кража оборудования / программного обеспечения / информации: кража ценных аппаратных средств, программного обеспечения и информационных активов;
- Ошибка человека: случайное уничтожение или неправильный ввод данных.
- Умышленный ущерб, причиненный недовольным сотрудником с целью осуществления мести;
- Использование ресурсов организации для противоправной или аморальной деятельности;

- Раскрытие конфиденциальной информации внешним организациям или внутренним третьим лицам, которые в ней не нуждались, независимо от носителей (файлов, устной передачи и т. д.).

Некоторые угрозы в организациях связаны с уязвимостями программного обеспечения или оборудования, с конструктивными недостатками информационных систем. Человеческие ошибки в процессе следования политике безопасности: например, может быть забыто блокирование доступа к ресурсам сотруднику, покинувшему организацию.

Таким образом, политики информационной безопасности являются контрмерами нарушений безопасности при условии, что они соблюдаются и применяются.

После выявления угрозы или уязвимости сотрудники должны знать, что предпринять, чтобы обеспечить сохранность информации. В этом контексте важно, чтобы сотрудники знали, степень конфиденциальности информации и приоритеты по ее защите. Они должны уметь определять потребности CIA в своих активах [21].

Организации фактически применяют подход к управлению рисками. Управление рисками является краеугольным камнем для эффективной и целенаправленной работы, проактивных решений возможных инцидентов. Оценка рисков позволяет организациям знать окружающую среду и разрабатывать сценарии борьбы с угрозами [47].

Оценка рисков является обязанностью организации: хотя универсального рецепта для минимизации рисков не существует, специалистам необходимо оценить характер организационной среды, прежде чем рассматривать вопрос о том, следует ли и каким образом проводить внедрение ИТ-решений» [15, с. 73-74].

2.2 Роль организации

Планирование является важным элементом управления для реализации мер безопасности и обоснования их бюджета. Т. Трифонас и др. [49, с. 188] определяют три компонента планирования информационной безопасности:

- Стратегическое планирование: разработка политики,
- Тактическое планирование: соответствие стандартам, проведение анализа рисков, эффективность аудита и т. д.
- Оперативное планирование: внедрение средств безопасности, таких как антивирус и т. д.

Однако, как объясняют Д. Штрауб и Р. Вельке [45, с. 441], «безопасность информации по-прежнему игнорируется руководителями, менеджерами среднего звена и сотрудниками. Результатом этой небрежности является то, что системы безопасности гораздо менее надежны, чем должны быть, и что нарушения безопасности случаются чаще и приносят больший ущерб».

Г. Диллон и Дж. Бэкхауз [14, с. 126-128] разделяют эту точку зрения. Информационная безопасность – это не столько техническая проблема, сколько социальная и организационная. Крайне важно обеспечить разработку надлежащей и эффективной политики безопасности. Действительно, она создает прочную платформу для внедрения методов обеспечения безопасности [51, с. 276]. Эта политика должна включать, по крайней мере, следующие соображения:

- Привлечь команду безопасности и юридический отдел для работы в команде по оценке документа политики на соответствие стандартам;
- Определить потребности организации в защите;
- Содержать требования политики классификации информации;
- Обеспечивать получение всеми сотрудниками информации о лучших методах обеспечения информационной безопасности.

Для Т. Трифонас и др. [49, с. 183] политика информационной безопасности представляет собой сочетание принципов, положений, методов и инструментов, созданных для защиты организации от потенциальных угроз. Существуют:

- Политика организации (в смысле структуры). Эта общая политика применяется к организации в целом. В нем говорится о приверженности руководства информационной безопасности и ее важности для организации. В нем подчеркиваются обязанности каждого в организации и средства для обеспечения безопасности.
- Конкретная политика в отделе информационно-коммуникационных технологий (ИКТ). Эти политики охватывают обязанности Директората информационных систем, роль которого заключается в обеспечении безопасности информационных систем и сетей связи. Он диктует условия выбора программного обеспечения, политики резервного копирования и т. д.
- Политика, предназначенная для сотрудников. Эта политика определяет набор процессов информационной безопасности, которым должны следовать сотрудники (использование Интернета, управление паролями, процедура сообщения о инцидентах безопасности и т. д.)

2.1 Цель политики информационной безопасности

Согласно Дж. Давид [13, с. 506], «безопасность – это не то, что мы делаем или что мы не делаем. Это не то, что мы разрешаем или не позволяем. Безопасность не имеет ничего общего с уровнем безопасности данных и систем. Безопасность – это то, как мы придерживаемся официальных политик безопасности».

Эффективная политика безопасности – это стратегия, в которой люди могут принять то, что от них ожидается при работе с информационными ресурсами. Поэтому эффективная политика безопасности зависит не только от того, что она содержит, но и от того, как участники понимают, что эта политика позволит достичь целей безопасности в организации.

Как добиться этого понимания? Фон Солмс и фон Солмс [51] делают аналогию между разработкой политик безопасности организаций и созданием Библии (Библии в метафорическом смысле). Они заключают, что:

1. Политика должна исходить от самого высокого уровня управления в организации;
2. Общая политика должна быть стабильной с течением времени;
3. Общая политика должна быть сосредоточена на общих концепциях и не должна затрагивать конкретные и технические контексты, которые со временем меняются;
4. Производные политики должна опираться на общую политику. Эти политики определяют специфику технических и бизнес-контекстов;
5. Процедуры должны описывать, как действовать в соответствии с политикой;

Для этого необходимо регулярно обновлять правила и процедуры и регулярно доводить информацию до членов организации.

2.2 Теории действия

Существует немного исследовательских работ, посвященных злонамеренному поведению в организации, такому как несоблюдение политик безопасности. В значительной степени это, по-видимому, связано с трудностями сбора данных, поскольку компании не хотят раскрывать проблемы, возникающие в этом отношении.

Тем не менее, Теория обоснованного действия (ТОД, Theory of reasoned action – TRA) Фишбейна и Айзена [19] и ее расширение – Теория Планируемого Поведения (ТПП, Theory of planned behavior – TCP) Айзена [3] были применены в нескольких исследованиях, связанных с информационной безопасностью. Фишбейн и Айзен объясняют намерение человека принять определенное поведение. Они предполагают, что намерение выполнять различные типы поведения может быть предсказано с большой точностью от отношения к этому поведению, субъективным нормам и воспринимаемому поведенческому контролю. Айзен [3] далее заявляет, что намерения, а также воспринимаемый поведенческий контроль составляют значительную часть различий в фактическом поведении.

Лучшее понимание факторов, которые мотивируют участников соблюдать политику информационной безопасности организации, имеет важное значение для того, чтобы помочь менеджерам выявить пробелы в их усилиях по управлению безопасностью, предоставив им средства для решения проблемы с поведением.

М. Сипонен и др. в [34] попытались представить эмпирические данные о применении поведенческой модели для изучения соблюдения политики безопасности в повседневной практике. Они разработали теоретическую модель, объединяющую теорию мотивации защиты Р. Роджерса (Protection Motivation Theory) [36-37], теорию обоснованного действия Фишбейна и Айзена и теорию диффузии инноваций Е. Роджерса [35], которые затем была подтверждена опросом 971 сотрудника. Результаты показывают, что сотрудники должны быть информированы и чувствовать себя способными действовать в защиту информационных систем компании и что меры, принимаемые руководством, считаются релевантными и адаптированы к реальной деятельности компании. Исследование поведенческих изменений выявило ценность повышения осведомленности и, следовательно, обучения.

2.3 Повышение осведомленности (информированности) о ИБ

Для Национального института стандартов и технологий (NIST 800-50, 2003: 8-9) повышение осведомленности не является обучением. Оно призвано привлечь внимание к безопасности и позволить каждому почувствовать себя вовлеченными и принять соответствующее поведение. Повышение осведомленности направлено на широкую аудиторию, в то время как обучение предоставляется небольшим группам. Участники обучения приобретают практические знания, которые позволяют им быть более эффективными в своей деятельности. Обучение объединяет совокупность знаний, как технических, так и социальных, направленных на подготовку специалистов по информационной безопасности.

Согласно SOGP [44], программа информирования должна способствовать «позитивной культуре безопасности». Различие между осведомленностью и подготовкой или образованием не производится. Речь идет о проведении тренингов по информированию. Эти тренинги должны быть регулярными, поощряться руководством и обращаться ко всем членам организации.

Преимущества повышения уровня информированности пользователей информационных систем:

- ориентация на гетерогенную аудиторию, а не только на специалистов в области информационных систем, что позволяет (1) объяснить цель безопасного поведения, (2) распространить хорошие практики и (3) предоставить помощь, если необходимо;
- специалисты по компьютерной безопасности получают обратную связь и сообщения о возможных инцидентах.

Цель повышения осведомленности определяется как разработка «положительной культуры безопасности» в организациях и эффективность этого процесса достигается только при определенных условиях. Прежде всего,

регулярное обучение требует материальных средств и организации. Поэтому повышение информированности требует, с одной стороны бюджет, а с другой структуру, отвечающую за ее организацию. Это может быть назначенный менеджер, который полагается на внутреннюю команду или внешнюю службу.

Повышение осведомленности должно основываться на простых и понятных как можно большему количеству людей терминах. Оно также должно соответствовать организационной структуре, поэтому ENISA (2006) и SOGP (2011) указывают, что повышение осведомленности должно:

- отвечать потребностям слушателей,
- предлагать реалистичные действия,
- показать, что могут получить слушатели, участвуя в информационной безопасности,
- соответствовать бизнес-стратегии, задачам и стратегическому видению, определяемым руководством.

Как и политики безопасности, повышение осведомленности должно основываться на организационной культуре. Сипонен [34] также считает, что повышение уровня информированности должно способствовать развитию морали и этики, которые отвечают потребностям безопасности, поскольку они являются мощными векторами для изменения поведения.

Участие высшего руководства также является предварительным условием успеха повышения информированности (SOGP). Оно должно обеспечить эффективное продвижение передовых практик и выделить необходимые финансовые, материальные и людские ресурсы. С другой стороны, слишком неформальное обучение, касающееся слишком общих тем, может быть причиной неудачи повышение осведомленности.

При изучении поведения дистанционных сотрудников Furnell (2006) отмечает, что повышение осведомленности оказывает значительное влияние на

восприятие безопасности. Эти результаты интересны тем, что они показывают, как индивид, даже вне организационного контекста, может вести себя в соответствии с ожиданиями организации, если он считает, что это важно. Это эффект нормативного давления. Сотрудник принимает поведение, которое, по его мнению, не исключается из организации при дистанционной работе.

Тем не менее, это не означает, что такие сотрудники усвоили ценности безопасности, продвигаемые организацией. Возможно, их поведение изменится в результате изменения рабочего места, где безопасность будет восприниматься как менее важная. Это подчеркивает роль локальных участников, особенно операционного менеджера. На самом деле, влияние операционного менеджера на осведомленность и поведение сотрудников изучено мало. Однако операционный менеджер имеет локальные полномочия, стратегию и ценности организации. Это потенциально может быть существенным для повышения осведомленности и принятия поведения, соответствующего требованиям безопасности.

2.4 Взаимосвязь между организационной культурой и информационной безопасностью

Безопасность включает сложные социальные конструкции, такие как идентификация, доверие и конфиденциальность, которые различаются в зависимости от контекста. Подход, который учитывает наилучшие интересы всех участников и характеристики информационных систем, сетей и связанных с ними услуг, может быть как эффективным, так и безопасным.

В «Директивах по проблеме безопасности информационных систем и сетей: формирование культуры обеспечения безопасности» [34] подход ОЭСР к формированию культуры обеспечения информационной безопасности включает девять взаимодополняющих принципов (см. Таблица 2).

Таблица 2 – Формирование культуры обеспечения безопасности ([34], с. 5-8)

Принцип	Определение
1) Осведомленность	Участвующие стороны должны осознавать необходимость обеспечения безопасности информационных систем и сетей и понимать, что они могут сделать для повышения безопасности.
2) Ответственность	За безопасность информационных систем и сетей отвечают все участвующие стороны.
3) Принятие ответных мер	Участвующие стороны должны, в сотрудничестве с другими, предпринимать своевременные действия для предотвращения, выявления и реагирования на инциденты, связанные с нарушениями безопасности.
4) Этика	Участвующие стороны должны учитывать законные интересы других лиц и организаций.
5) Демократия	Обеспечение безопасности информационных систем и сетей не должно вступать в противоречие с основополагающими ценностями демократического общества.
6) Оценка рисков	Участвующие стороны должны проводить оценку рисков.
7) Разработка и реализация систем и сетей с учетом необходимости обеспечения безопасности	Участвующие стороны должны рассматривать безопасность как один из наиболее важных элементов информационных систем и сетей.
8) Руководство обеспечением безопасности	Участвующие стороны должны принять комплексный подход к руководству обеспечением безопасности.
9) Повторная оценка	Участвующие стороны должны анализировать и проводить повторную оценку безопасности информационных систем и сетей, а также вносить соответствующие изменения в политику, практику, меры и процедуры в сфере безопасности.

В определении ОЭСР больше внимания уделяется культурному измерению, занимающему центральное место в деятельности по обеспечению безопасности, которое во многом зависит от уровня восприятия участников: «Руководство обеспечением безопасности должно основываться на оценке рисков. Оно должно быть динамичным, охватывающим все уровни деятельности участвующих сторон и все аспекты их работы. Оно должно включать в себя упреждающее реагирование на появляющиеся угрозы и должно предусматривать принятие мер, направленных на предотвращение и выявление инцидентов и реагирование на них, мер по восстановлению систем после сбоев, непрерывное

техническое обслуживание, анализ и аудит. Политика, практика, меры и процедуры в области обеспечения безопасности информационных систем и сетей должны быть скоординированными и интегрированными с тем, чтобы образовывать логически последовательную систему обеспечения безопасности. Требования к руководству обеспечением безопасности зависят от уровня участия, роли и функций участвующей стороны, существующего риска и требований к системе» [34].

Многие исследователи также предполагают, что информационная безопасность должна быть частью организационной культуры [51, 26] обнаружили, что в большинстве организаций информационная безопасность не является неотъемлемой частью организационной культуры. Для объяснения этого явления можно привести несколько причин, например:

- Отсутствие финансовых вложений – П. Шедден и др. [43] показали, что организации склонны рассматривать расходы на безопасность как оправданные только после того, как произошел инцидент, то есть слишком поздно.
- Недостаточное участие сотрудников – пассивное участие сотрудников в осуществлении мер безопасности, реализация которых часто ложится на плечи единиц.
- Ограниченное внедрение мер безопасности – политики безопасности в большинстве случаев вытекает не из убеждений, а из необходимости соблюдения правил и принуждения через внешние аудиты.

В литературе также показано, что существует три типа отношений между организационной культурой и информационной безопасностью:

1. Информационная безопасность не интегрирована в организационную культуру [27]. В этом случае менеджмент организации не занимается информационной безопасностью. Члены организации мало

осведомлены и не чувствуют ответственности за проблемы безопасности. Организации часто склонны рассматривать расходы на обеспечение безопасности как неоправданные траты [43]. Это та ситуация, когда деятельность по информационной безопасности поддерживается только ИТ-отделом.

2. Информационная безопасность – «субкультура» организационной культуры. Часть сотрудников более осведомлена о требованиях к безопасности, проводится периодическое обучение безопасности. Некоторые отделы организации начинают обращать внимание на безопасность, и вопрос о новых практиках появляется в повестке руководства.
3. Информационная безопасность встроена в организационную культуру. Меры безопасности внедрены во всей организации и с относительно высоким уровнем участия. Кроме того, регулярно обновляются политики безопасности. Члены организации чувствуют ответственность за информацию и мотивированы придерживаться политики безопасности. Практики безопасности становятся бессознательными повседневными действиями [51, 52]. Менеджмент и сотрудники организации разделяют общие ценности информационной безопасности.

Каким образом достигается третий тип отношений? Обзор литературы позволяет выделить несколько переменных, способных развивать организационную культуру, но их влияние, в частности на фактические практики, остается мало изученным.

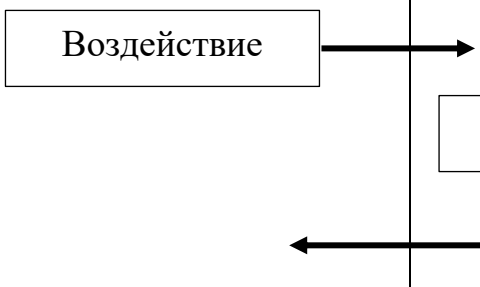
1. Политики безопасности;
2. Участие высшего руководства;
3. Осведомленность;

4. ИТ-отдел / Отдел безопасности;
5. Участие операционного менеджмента.

Некоторые меры безопасности действуют непосредственно на организационном уровне, влияя на «массовое» осознание угроз ИБ, в то время как другие влияют на отдельных лиц. Это повышение индивидуальной осведомленности адаптирует индивидуальную культуру, чтобы привести ее в соответствие с организационной.

В таблице 3 показано, как компоненты безопасности в цикле воздействуют на индивидуальную культуру и через нее меняют организационную.

Таблица 3 – Воздействие компонентов безопасности на индивидуальную и организационную культуру

Компонент	Субъект	Организационная культура
		
Вовлечение и продвижение руководством	Организация	Организационное
Политики безопасности		
ИТ-отдел		
Повышение осведомленности	Индивид	Индивидуальное
Участие операционных менеджеров		
Прошлый опыт		

3 Исследование стартапов региона Нор-Па-де-Кале

3.1 Описание исследования

Практической частью данной работы стало исследование, проведенное в марте 2017 г. во французском регионе Нор-Па-де-Кале. Методологией исследования было выбрано качественное исследование методом интервью по разработанному опроснику с руководителями стартапов, чтобы ответить на вопрос: каким образом социальная сеть стартапа влияет на принятие решений его руководителя в отношении информационной безопасности.

В рамках выбранной проблемы были выдвинуты следующие гипотезы для проверки:

Г1. Социальная сеть стартапа напрямую влияет на решения менеджера в отношении информационной безопасности.

Г2. Навыки менеджера, его знания в области безопасности влияют на принятие решений в отношении информационной безопасности.

Г3. Осознание важности и приверженность ценности защиты данных менеджером стартапа влияют на принятие решений в отношении информационной безопасности.

Г4. Область деятельности стартапа определяет уровень приверженности менеджера обеспечению информационной безопасности.

После определения гипотез был составлен опросник для руководителей стартапов (см. Таблица 4). В таблице 5 приведен оригинал опросника на французском языке.

Таблица 4 – Опросник для проводимого исследования

Тема	Подтема	Примеры вопросов	Цель
Информа-ционная безопасность	Определение / Область	1. **Как вы думаете, что такое «Информационная безопасность»?**	оценить навыки и знания (Г2)
		2. **Какова область информационной безопасности (что вы подразумеваете под информацией)?**	
	Позиция стартапа по внедрению информационной безопасности (по собственному определению ИБ)	1. На каком этапе внедрения информационной безопасности находится Ваш стартап? **Как руководитель, какой приоритет вы присваиваете информационной безопасности в вашем стартапе? Принимаете ли Вы лично участие в процессах информационной безопасности? Если да, то как? Если нет, то почему?**	определить приверженность ценностям (Г3)
		2. **Являются ли требования по информационной безопасности обязательством в области деятельности Вашего стартапа?**	проверить (Г4)
	Потребности в области информационной безопасности	1. **Почему вам важна защита информации?** Соблюдение требований клиентов / соблюдение конфиденциальности	интерпретировать причины принятия решений (Г1-4)
		2. **Были ли случаи, которые привели вас к принятию решений в области информационной безопасности?**	
Способы применения	Принятые решения	Какие меры безопасности реализованы?	оценить степень реализации и факторы, влияющие на этот уровень
		Кто их предложил? Кто занимался реализацией?	
		Почему?	
		Как?	
	Ограничения реализации	Каковы препятствия на пути внедрения подхода информационной безопасности?	выяснить факторы, затрудняющие принятие решений

Таблица 5 – Оригинал опросника (на французском языке)

Thèmes	Sous thèmes	Exemples de questions	Intérêt
La Sécurité de l'information	Définition / Périmètre	1. **Selon vous qu'est-ce que la sécurité de l'Information ?**	évaluer des compétences et connaissances (h2)
		2. **Et elle s'étale à quel périmètre ?**	
	La place de la startup par rapport à sa définition de la sécurité de l'information	1. Votre startup se trouve où par rapport à ce que vous entendez par sécurité de l'information ? **En tant que dirigeant, à quel niveau de priorité placer vous la sécurité de l'information dans votre startup ?** **Et êtes-vous engagé à des procédures de sécurité d'info Si oui comment ? Si non pourquoi ?** 2. **Est-ce que le domaine de votre activité vous oblige à vous positionner à l'égard de la sécurité de l'information ?**	savoir si la startup est engagée dans des procédure de sécurité d'information (h3) et se renseigner (h4)
	Besoins en matière de sécurité d'information	1. **Pourquoi peut-il être nécessaire pour vous de sécuriser vos informations ?** Répondre à des exigences de client / respect de la vie privé 2. **Quels sont les situations qui vous ont amené à mettre en place des décisions de sécurité d'information ?**	interpréter les raisons des prises de décisions pour en conclure les facteurs influençant
Modes d'emploi	Décisions prises	Quelle sont les mesures de sécurités en œuvre ?	évaluer le taux d'implication et les facteurs impactant ce niveau d'implication
		Qui les a proposés ? Qui les a mis en œuvre ?	
		Pourquoi ?	
		Comment ?	
	Limites de la mise en œuvre	Quels sont les obstacles de la mise en œuvre d'une approche de sécurité d'information	clarifier les facteurs qui constituent des freins aux prises de décisions

Вопросы разбиты на темы, такие как определение знаний менеджера о ИБ, позиция стартапа по внедрению информационной безопасности, потребности в области информационной безопасности, принятые решения и ограничения реализации. При этом формулировка вопросов не является жесткой. При проведении интервью вопросы переформулировались в зависимости от ситуации, жестко соблюдалось только покрытие всех тем.

3.2 Описание стартапов

Исследуемой группой стали стартапы в бизнес-инкубаторе и стартап-акселераторе EuraTechnologie, расположенном в городе Лилль в регионе Нор-Па-де-Кале. Были проведены интервью с руководителями шести стартапов, чья сфера деятельности тесно связана с информационными технологиями. Все они предлагают различные продукты или услуги и не являются конкурентами.

3.2.1 Стартап 1 (Jooxter)

Jooxter состоит из примерно пятнадцати сотрудников и существует с 2014 года. Компания работает в области Smart Building Domain Application, предоставляя другим компаниям (B2B) сервис для оптимизации офисных площадей. Используется сеть датчиков, с помощью которых в реальном времени отслеживается перемещение сотрудников в зданиях, соблюдая их анонимность.

В компании нет утвержденной политики безопасности уровня требований банковской сферы. Однако, внедрены меры безопасности, включая контроль прав доступа к информации, анонимизацию передаваемых данных о пользователе или выбор надежных инструментов и технических партнеров (хостинг).

Сотрудники соглашаются с пунктом о конфиденциальности информации в трудовых договорах. Кроме того, компанией принята Хартия уважения частной жизни (конфиденциальности частных данных), не только для «успокоения»

клиентов, но и из здравого смысла (¾ клиентов интересуются защищенностью частных данных). Тем не менее менеджер подчеркнул, что для него одним из препятствий является необходимость убеждения клиентов в том, что нет риска для их частной жизни.

Менеджер стартапа показал высокую осведомленность в вопросах ИБ. Хотя нет утвержденной политики ИБ уровня крупных корпораций, приняты меры по обеспечению безопасности: технического, юридического и организационного характера. Подтверждается вторая гипотеза (Г2) о влиянии знаний менеджера и четвертая (Г4) о влиянии области деятельности (отслеживание перемещений пользователей вызывает их обеспокоенность).

3.2.2 Стартап 2 (Pitchr)

Pitchr, наиболее молодой из опрошенных стартапов, основан в октябре 2016 года. Предлагает своим пользователям онлайн-платформу управления профессиональными сообществами и мобильное приложение, позволяющее находить лучшие профессиональные контакты в нужное время в нужном месте в зависимости от интересов и существующей сети контактов, синхронизируемой с LinkedIn.

В данный момент менеджер концентрируется на продукте, его разработке и продвижении. Тем не менее заявляется высокий приоритет безопасности. Менеджер указывает на причины: «потому что стартап в цифровом бизнесе», укрепление имиджа.

Согласно менеджеру, препятствия, с которыми может столкнуться реализация мер безопасности, – это время и цена, особенно для очень молодого стартапа. Затем следуют сопровождение сотрудников, их обучение и мотивация.

В реализации ИБ менеджер полагается на партнеров, обладающих техническими знаниями. Подтверждается первая гипотеза (Г1) о влиянии сети.

3.2.3 Стартап 3 (Libertrip)

Libertrip, стартап существующий уже 5 лет в качестве производителя программного обеспечения для сектора туризма. Он предоставляет туроператорам SaaS (программное обеспечение как услугу), облегчающий продажи туристических поездок. Компания состоит из десяти человек, в основном инженеров. Это объясняет тот факт, что она хорошо подготовлена перед лицом проблем безопасности.

Менеджер говорит о наличии у него «бэкграунда» ИБ. По его словам, ИБ не является приоритетом, а находится в «ДНК» технологических компаний, является «естественной».

В компании есть проработанные схемы резервного копирования и восстановления данных, шифрования жестких дисков. Случай кражи одного компьютера не создал угрозы для компании: данные на компьютере были зашифрованы, и компания восстановила их из резервной копии. Соблюдается политика сложности и частоты смены паролей (не менее шести раз в год), а также принцип отдельного пароля к каждому сервису. Менеджер знаком с нормами и рекомендациями CNIL (Национальная комиссия по информатике и гражданским свободам Франции).

Со стороны клиентов стартапа не было требований обеспечения безопасности, более того компания сама пытается довести принципы безопасности до клиентов. Менеджер подчеркивает, что, как стартапу, компании легче повысить уровень безопасности, чем крупной компании.

Затраты на обеспечение безопасности являются препятствием, особенно для небольших компаний. Но руководитель подчеркивает необходимость этой инвестиции, даже если ROSI (Return On Security Investment) виден не сразу.

Подтверждается третья гипотеза (Г3) о приверженности менеджера ценности безопасности. Он несколько раз упоминает о том, что в цифровом

бизнесе нужно быть безупречным и не пренебрегать безопасностью. Тем не менее, этого недостаточно для подтверждения или опровержения четвертой гипотезы о влиянии области деятельности на принятие решений.

3.2.4 Стартап 4 (Mail Billy)

Данный стартап представляет собой платформу по переводу и созданию многоязычного контента для компаний (B2B). Перевод писем и написание маркетинговых текстов гарантируется в течении одного часа. Компания основана в январе 2017 года.

Менеджер имеет большой опыт в переводе и написании текстов, в том числе в работе с конфиденциальными текстами. Устоявшийся способ работы в этом бизнесе подразумевает пересылку множества электронных писем с документами в приложении. Что ставит конфиденциальные данные под угрозу и создает высокую вероятность ошибок человеческого фактора. Повышение безопасности и автоматизация работы были стимулами создания платформы. Руководитель пригласила на работу разработчика, который взял на себя ответственность за все технические аспекты компании.

По ее словам, информация, безопасность которой должна быть обеспечена, – это документы для перевода, предоставленные клиентами. Во время вопроса о том, требует ли защиты внутренняя информация компании, разработчик вмешался в интервью, как только менеджер заявила, что «Мы совсем не защищены». Этот факт полностью опровергает вторую гипотезу о влиянии навыков и знаний.

Тем не менее, руководитель принимает меры обеспечения безопасности. Например, просит клиента удалить или зашифровать в своем документе любую конфиденциальную информацию.

Разработчик применяет собственные инициативы в отношении безопасности, и таким образом выступает в роли менеджера ИБ. Так, он

реализовал шифрование паролей и сведений, хранящихся в базе данных. Для возраста и размера стартапа, и особенно того факта, что платформа была построена в режиме MVP («Минимально жизнеспособного продукта»), эта ситуация представляет собой допустимый уровень минимальной защищенности.

Таким образом, подтверждается первая гипотеза (Г1) о влиянии сети.

3.2.5 Стартап 5 (Languages.ai)

Это стартап из шести сотрудников, специализирующийся на разработке расширения браузера (плагина), помогающего пользователям улучшить знание иностранных языков. С помощью расширения пользователи могут искать перевод слов и отмечать слова для изучения. В случае встречи отмеченного слова на любой веб-странице оно выделяется в тексте и пользователю предлагается протестировать свои знания или напомнить значение слова.

Менеджер настаивает на том, что в их области деятельности, помимо исходного кода и алгоритмов, разработанных в стартапе, другая информация не требует обеспечения защиты. Так, даже внутренняя информация стратегического или финансового характера на данном этапе не представляет достаточной важности, чтобы обеспечивать уровень ее защиты как конфиденциальной информации.

Будучи руководителем очень небольшой структуры в области деятльности менее требовательной к безопасности, менеджер компании не считает информационную безопасность приоритетом или предметом, который нужно рассматривать ежедневно, и не видит изменения этой ситуации в будущем.

Тем не менее, реализованной мерой является защита исходного кода программы.

Препятствием для реализации ИБ, по мнению, руководителя, являются вопросы времени, денег и приоритетов.

Это интервью позволяет сделать вывод о том, что сфера деятельности стартапа является очень важным фактором, оказывающим явное влияние на принятие менеджером решений в отношении ИБ.

В этом случае менеджер не видит конкретных причин для поддержания уровня безопасности, но он отметил, что безопасность никогда не была требованием со стороны ее клиентов или партнеров.

Подтверждается четвертая (Г4) о влиянии области деятельности.

3.2.6 Стартап 6 (Moffi)

Компания Moffi – небольшой стартап, состоящий из 8 человек, включая разработчика, ответственного за информационную безопасность. Это усиливает вовлеченность стартапа в организацию ИБ. Стартап предлагает платформу совместного использования рабочего пространства, позволяющую владельцам коворкингов, бизнес-центров и офисов компаний, не занятых на 100%, сдавать в аренду рабочие места на любой срок с помощью онлайн системы бронирования и оплаты.

Директор связывает безопасность информации с имиджем компании и гарантирует первостепенность ее обеспечения в своей компании. По шкале от 1 до 10 менеджер дает уровень приоритета информационной безопасности между 8 и 9.

По его убеждению, любой веб-сайт должен быть безопасным, независимо от области деятельности. Тем не менее, это не опровергает гипотезу, выдвинутую в связи с влиянием области деятельности. Все зависит от интерпретации области деятельности. В этом случае директор подразумевает, что обслуживание и создание веб-сайтов всегда требует обеспечения безопасности.

Менеджер называет в своем случае два типа важной информации, требующей защиты. Первый тип – это банковская информация, связанная с транзакциями и платежами на платформе, чья безопасность обеспечивается в первую очередь системой обработки платежей банка, а не стартапом. Вторым

типом являются пользовательские данные, защита которых обеспечивается стартапом.

Сотрудником, ответственным за информационную безопасность, является один из разработчиков, имеющий опыт в области ИБ. Таким образом он посвящает этому вопросу не все рабочее время. Это распространенная практика в стартапах, где сотрудники, учитывая размер компании, могут быть задействованы одновременно в различных аспектах.

Это интервью подтверждает две гипотезы: четвертую гипотезу (Г4) о влиянии области деятельности и первую гипотезу (Г1) о влиянии сети. Менеджер подтверждает необходимость обеспечения безопасности в компании, которая работает в Интернете, а ответственный за ИБ, берет на себя инициативу и встречается с менеджером, чтобы уточнить вопросы и рекомендовать возможные решения.

В таблицах 6 и 7 приведены краткие ответы респондентов, разбитые по темам и стартапам.

Таблица 6 – Результаты интервью

Тема	Стартап 1	Стартап 2	Стартап 3
Понимание менеджментом информации / ИБ	Различает три типа информации: зарезервированную для менеджмента (конфиденциальную), внутреннюю информацию различных отделов, публичную информацию, доступную для всех.	Область ИБ: все данные, относящиеся к жизни компании, являются ли они структурными или экономическими данными. Для менеджера ИБ распространяется на все аспекты бизнеса стартапа и касается доступности данных и обмена данными между различными внутренними и внешними заинтересованными сторонами. Он также проводит различие между компьютерной безопасностью и информационной безопасностью.	Проблемы безопасности: вторжение, резервное копирование и восстановление данных. Наиболее важная информация: исходные коды программ и платформа. Нормы и рекомендации CNIL (Национальная комиссия по информатике и гражданским свободам Франции)
Позиция стартапа по внедрению информационной безопасности (в понимании менеджмента)	Нет до мельчайших деталей проработанной политики. Нет радикальных мер безопасности. Но есть обязательство со стороны стартапа по обеспечению сохранности данных и уровень безопасности достаточен для этого типа данных: «Мы не банк и не работаем для банковских организаций, где безопасность имеет критическое значение».	Приложение минимально защищено. Менеджер задается вопросом о безопасности, несмотря на то, что стартапу 7 месяцев. ИБ имеет 2-й или 3-й приоритет, хотя на данный момент стартап не занимается конкретно процедурами безопасности. Главный приоритет: продукт, который работает и нравится пользователям, создание пользовательской базы	ИБ не является приоритетом, но она находится в «ДНК» стартапа. Стартап, состоящий из сотрудников, осведомленных о ИБ. У менеджера есть «бэкграунд» ИБ. «Мы знаем, что значит потерять данные». «Как стартап мы можем быть более активны в попытках повысить уровень безопасности».
Причина / мотив для обеспечения информационной безопасности	Чтобы заверить клиентов (3/4 регулярно спрашивают). Уважение к частной жизни является важным для стартапа. Из принципа, по гуманным сооб-	Потому что стартап в цифровом бизнесе Не допустить кражи данных о клиентах Укрепить имидж	Принцип восстановления, возможность быстро заново запустить систему в случае ЧС. Это «естественно» для технологической компании.

	ражениям и на основе здравого смысла		Предотвращение кражи данных. Позволяет спокойно сосредоточится на бизнесе. Для поддержания имиджа бренда. Соответствие нормам.
Меры безопасности, реализованные / подлежащие реализации	Передаваемые данные о пользователях анонимизированы. Доверие к техническим партнерам по оказанию услуг хостинга и обеспечению безопасности размещенных данных. Внутреннее управление правами доступа к конфиденциальной информации. Использование надежных облачных сервисов и корпоративных инструментов для эффективного и безопасного обмена. предоставляемых третьими лицами. Утверждена Хартия уважения частной жизни (конфиденциальности частных данных), не только для «успокоения» клиентов, но и из здравого смысла. Пункт о конфиденциальности информации в трудовых договорах сотрудников.	Облачные сервисы для резервного копирования определенных документов Инфраструктура надежных технологических партнеров. Юридически оформленные общие положения пользования и внутренние инструменты Приложение, размещенное на доверенном веб-узле Данные зашифрованы	Резервное копирование исходного кода. Унификация используемого компьютерного оборудования. Шифрование жестких дисков. Политика сложности и частоты смены паролей. Использование PaaS (платформа как услуга) Amazon AWS и Heroku позволяет снять задачу обеспечения безопасности серверной инфраструктуры
Препятствия / трудности	Убеждение клиентов, что нет риска для их личной жизни	Менеджер концентрируется в данный момент на продукте («сначала должен быть хороший продукт и пользователи») Цена обеспечения ИБ (аутсорсинг, рабочая сила, время)	Нет мгновенной окупаемости инвестиции (как страхование). Стоимость и затраты на квалифицированные кадры, техническое обслуживание. И прежде всего: невежество. От-

		Сопровождение сотрудников и их вовлеченности	сутствие культуры безопасности и отсутствие обучения и приобретения навыков.
Сфера деятельности	Smart Building Domain Application в B2B для оптимизации офисных площадей. Использование датчика, позволяющее в реальном времени отслеживать перемещение сотрудников в зданиях, соблюдая их анонимность. Цель клиентов и характер данных, связанных с бизнесом, не очень чувствительны к обеспечению ИБ. «Нет критичного риска».	Онлайн-платформа управления профессиональными сообществами. Мобильное приложение, позволяющее находить лучшие профессиональные контакты в нужное время в нужном месте в зависимости от интересов и существующей сети контактов)	Онлайн сервис для организации путешествий. Туроператоры могут предложить готовые поездки, а туристы выбрать предложенный или спланировать собственный маршрут с возможностью сделать все бронирования онлайн

Таблица 7 – Результаты интервью (продолжение)

Тема	Стартап 4	Стартап 5	Стартап 6
Понимание менеджментом информации / ИБ	Информация – это любой документ, предоставленный клиентами для переводов. Менеджер чувствует ответственность за обеспечение конфиденциальности информации своих клиентов и стремится обеспечить минимально необходимую безопасность в процессе обмена информацией между клиентами, стартапом и языковыми экспертами, которые выполняют переводы.	Информация – это данные пользователя, а также код компании и алгоритмы, отличающие от конкурентов. Но внутренние данные типа (стратегия / финансы менее важны на текущей стадии). Информационная безопасность состоит в защите кода и обеспечении защищенности конфиденциальных данных от доступа извне.	Наиболее важная банковская информация. Личные данные клиента. База данных платформы и обмен данными между пользователями и платформой
Позиция стартапа по внедрению информационной безопасности (в понимании менеджмента)	«Мы совсем не защищены»	Информационная безопасность вовсе не является приоритетом или предметом, рассматриваемым ежедневно.	Безопасность пользовательских данных имеет первоочередное значение для стартапа. Как и безопасность платежей, но она обеспечивается в первую очередь системой обработки платежей банка, а не стартапом. Делается все возможное для ИБ
Причина / мотив для обеспечения информационной безопасности	Сохранять конфиденциальность информации о клиенте Клиенты иногда относятся к сектору, чувствительному к ИБ: государственному службы, крупные компании и т. д. Определенные внутренние политики клиентов, требующие подписания соглашения о неразглашении (NDA) с поставщиками услуг	Защита данных и минимизация рисков внешних атак и внутренних утечек.	Предотвращение ущерба из-за кражи пользовательских данных. Попытка взлома может происходить в любое время. Уже были попытки атак. Имидж компании.

Меры безопасности, реализованные / подлежащие реализации	Главный разработчик занимается обеспечением безопасности и самостоятельно принимает решения. Платформа существует в режиме MVP (минимально жизнеспособного продукта). В процессе разработки функциональные возможности платформы, автоматизирующие процессы и ограничивающие необходимость ручного вмешательства в базу данных. Клиентам напоминается о необходимости удалить конфиденциальную информацию из документов, отправляемых для перевода. Зашифрованные пароли	Необходимый минимум. Управления правами доступа к пользовательской информации. Контроль обмена конфиденциальными данными. Шифрование ключей в исходном коде программы. Обновление ключей доступа к базе данных, чтобы гарантировать, что ни один человек не имеет права доступа к нему.	Разработчик, наделенный ответственностью обеспечения ИБ и имеющий опыт в этой области. 4 сервера для резерва, в т.ч. в случае атак. Аутсорсинг обеспечения безопасности банковских данных. Процесс и система для выявления причин ошибок. Управление правами доступа к серверам по определенным IP-адресам.
Препятствия / трудности	Нет контроля со стороны менеджмента (недостаточно технических компетенций). Обеспечением безопасности в данный момент занимается один сотрудник	Время. Деньги. Тот факт, что это не является основой бизнеса, и это не приоритет.	Баланс между безопасностью и изменениями. Жесткие меры безопасности могут быть в ущерб простоте использования продукта и оттолкнуть клиента
Сфера деятельности	Перевод и создание многоязычного контента B2B.	Расширение браузера для изучения или повторения слов в иностранных языках.	Платформа совместного использования рабочего пространства, позволяющая владельцам коворкингов, бизнес-центров и офисов компаний, не занятых на 100%, сдавать в аренду рабочие места на любой срок с помощью онлайн системы бронирования и оплаты.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА «СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту

Группа	ФИО
3АМ6Ф	Коробкову Евгению Игоревичу

Институт	Школа инженерного предпринимательства	**Кафедра**	менеджмента
Уровень образования	магистратура	**Направление/ специальность**	Менеджмент 38.04.02

Исходные данные к разделу «Социальная ответственность»	
1. Описание рабочего места (рабочей зоны, технологического процесса, используемого оборудования) на предмет возникновения: *- вредных проявлений факторов производственной среды (метеоусловия, вредные вещества, освещение, шумы, вибрация, электромагнитные поля, ионизирующие излучения)* *- опасных проявлений факторов производственной среды (механической природы, термического характера, электрической, пожарной природы)* *- негативного воздействия на окружающую природную среду (атмосферу, гидросферу, литосферу)* *- чрезвычайных ситуаций (техногенного, стихийного, экологического и социального характера)*	Рабочее место находится в офисе компании EuraTechnologies SEML 165, avenue de Bretagne 59000 Lille, France Вредные и опасные проявления факторов производственной среды, а также чрезвычайные ситуации социального характера на рабочем месте отсутствуют.
2. Список законодательных и нормативных документов по теме	- международный стандарт ISO 26000:2010 (ИСО 26000) «Руководство по социальной ответственности» - серия международных стандартов систем экологического менеджмента ISO 14000 - GRI (Global Reporting Initiative) – всемирная инициатива добровольной отчетности - SA 8000 (Social Accountability 8000) – стандарт для оценки социальных аспектов систем менеджмента - данные, представленные на официальном сайте - внутренняя документация предприятия - методические указания для выполнения раздела «Социальная ответственность»
Перечень вопросов, подлежащих исследованию, проектированию и разработке	
1. Анализ факторов внутренней социальной ответственности:	- принципы корпоративной культуры исследуемой организации; - системы организации труда и его безопасности; - развитие человеческих ресурсов через обучающие программы и программы подготовки и повышения квалификации;
2. Анализ факторов внешней социальной ответственности:	- мероприятия, связанные с экологией и

	природопользованием; - содействие охране окружающей среды; - взаимодействие с местным сообществом и местной властью; - спонсорство и корпоративная благотворительность; - взаимодействие с экологическими организациями; - взаимодействие с научным сообществом; - взаимодействие с общественными организациями.
3. Правовые и организационные вопросы обеспечения социальной ответственности: *- анализ правовых норм трудового законодательства;* *- анализ специальных (характерные для исследуемой области деятельности) правовых и нормативных законодательных актов;* *- анализ внутренних нормативных документов и регламентов организации в области исследуемой деятельности.*	- анализ правовых норм трудового законодательства; - анализ специальных правовых и нормативных законодательных актов; - анализ внутренних нормативных документов и регламентов организации в области исследуемой деятельности
Перечень графического материала:	
При необходимости представить эскизные графические материалы к расчетному заданию (обязательно для специалистов и магистров)	- отчетные таблицы и графики, - фотоматериалы с сайта организации

Дата выдачи задания для раздела по линейному графику	06.10.2017

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Черепанова Н.В.	к.ф.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
ЗАМ6Ф	Коробков Е.И.		

4 Социальная ответственность компании EuraTechnologies

В мире бизнеса основная «ответственность» корпораций исторически заключалась в том, чтобы зарабатывать деньги и повышать акционерную стоимость. Другими словами, корпоративная ответственность являлась синонимом финансовой ответственности перед акционерами. Однако за последние два десятилетия движение, определяющее более широкие корпоративные обязанности – для окружающей среды, местных сообществ, условий труда и устойчивого развития – набрало силу и укрепилось. Эта новая движущая сила известна как корпоративная социальная ответственность (КСО).

Корпоративная социальная ответственность – это концепция прозрачной бизнес-практики, основанной на этических ценностях, соблюдении правовых требований и уважении к людям, сообществам и окружающей среде. Таким образом, помимо получения прибыли компании несут ответственность за совокупность их воздействия на людей и на планету. Здесь в понятие «люди» вкладываются все стейкхолдеры (заинтересованные стороны) компании: ее сотрудники, клиенты, деловые партнеры, инвесторы, поставщики, государство и сообщество. Все чаще заинтересованные стороны ожидают, что компании должны быть более экологически и социально ответственными в осуществлении своего бизнеса.

Реализуя социальные программы, корпорации сокращают свои текущие прибыли, но в долгосрочной перспективе формируют благоприятную социальную среду для своих работников и территорий своей деятельности, добиваясь в конечном итоге стабильности своей прибыли.

Так как магистерская диссертация посвящена исследованию не отдельно взятой компании, а технологических стартапов, для анализа эффективности программ корпоративной социальной ответственности была выбрана компания EuraTechnologies SEML – крупнейший стартап-акселератор Франции, расположенный в городе Лилль.

4.1 Деятельность компании

EuraTechnologies – это бизнес-инкубатор и стартап-акселератор, объединяющий под своей крышей около 200 ИТ-компаний. Этот бизнес-парк дает начинающим кампаниям возможность взаимодействовать с представителями исследовательского и научного сообщества, университетами и другими экономическими субъектами в области ИКТ (стартапы, малые и средние предприятия, крупные французские и зарубежные компании).

EuraTechnologies работает с большой сетью партнеров: университетов, лабораторий, успешных предпринимателей, инвесторов и бизнес-тренеров. С более чем 200 французскими и зарубежными компаниями-резидентами, EuraTechnologies стремится создать полную экосистему для местных и мировых предпринимателей городе Лилль, столице региона Нор-Па-де-Кале.

EuraTechnologies находится в районе Буа-Бланс в Лилле. Центральным зданием является Ле Блан-Лафон, бывший прядильный завод, построенный в 1900 году, а сам кластер простирается на площади более 100 гектаров и имеет целью превращение в эко-район, объединяющий офисы, лаборатории, предприятия с общественными пространствами, жилой зоной и зеленые насаждениями.

Кроме резидентов, пространства бизнес-парка также предоставляются внешним участникам, в частности, для организации мероприятий, конференций, форумов и ярмарок, связанных с инновациями и новыми технологиями (аудитории, конференц-залы, переговорные и т.д.). Основной же задачей остается поддержка руководителей проектов, связанных с новыми технологиями. Таким образом, EuraTechnologies объединяет бизнес-инкубатор, позволяя предпринимателям созреть и запустить свои проекты, а затем перейти на этап стартапа. В настоящее время в акселераторе, открытом с 2009 года, работает около 200 компаний, что составляет порядка 4 000 рабочих мест.

В миссии EuraTechnologies перечислены следующие задачи:

- Поддерживать компании в их технологическом, коммерческом и стратегическом развитии
- Способствовать появлению проектов ИКТ и новых талантов
- Предложить инструменты и среду, которые отвечает потребностям компаний

EuraTechnologies содействуют экономическому и социальному развитию посредством передачи технологий и инноваций и работают над последовательным технополитическим подходом, объединяя миры исследований, высшего образования и экономики.

В управляющей компании EuraTechnologies SEML работают около 50 сотрудников. Председателем совета директоров компании является Пьер Сантиньон.

4.2 Определение стейкхолдеров

Таблица 8 – Стейкхолдеры EuraTechnologies SEML

Прямые стейкхолдеры	Влияние
Сотрудники	Предоставление полного социального пакета, возможности повышения квалификации и переобучения в рамках осуществляемой деятельности, предоставление разнообразных льгот и корпоративных скидок в компаниях-партнерах, обеспечение лучших кадров жильем и др.
Клиенты (компании-резиденты)	Предоставление качественных и квалифицированных услуг, гарантия полного соответствия уровню социальной и этической ответственности компании
Косвенные стейкхолдеры	
Население региона Нор-Па-де-Кале	Реализация проектов на развитие социальной сферы города: развитие территорий, организация культурно-досуговых мероприятий, участие в благотворительных проектах и т.д.
Экологические организации	Совместная реализация образовательных проектов в сфере экологии, совместная работа в проектировке и создании эко-района
НКО и фонды	Благотворительные пожертвования на развитие и конкретные мероприятия, участие в

	мероприятиях и акциях, помощь в предоставлении материально-технического оснащения и др.

Корпоративная социальная ответственность компании EuraTechnologies сводится к трем направлениям:

– общество;

– экология;

– охрана труда.

С первых лет создания EuraTechnologies неизменно придерживается политики высокой социальной ответственности не только перед своими сотрудниками, но и перед населением региона Нор-Па-де-Кале. Деятельность EuraTechnologies, входящего в десятку лучших стартап-акселераторов Европы, способствует развитию экономики региона Нор-Па-де-Кале, созданию новых рабочих мест, обеспечению устойчивого развития. Помимо этого, реализуется широкий перечень образовательных и просветительских проектов, направленных на популяризацию технологий, науки и инноваций.

Одним из основных направлений развития является создание эко-района, отвечающего концепции устойчивого развития, жестким стандартам потребления энергии (класс энергоэффективности A+++) и окруженного зеленой зоной с «голубой рамкой» – эко-ландшафтной сети, состоящей из рек и смежных или зависимых водно-болотных угодий.

Человеческий и социальный капитал являются высшей ценностью компании. Рабочие места соответствуют нормам безопасности труда.

4.3 Определение структуры программ КСО

Структура программ КСО составляет портрет КСО организации и составляется в соответствии с целями компании и выбранными стейкхолдерами, на которых эти программы будут направлены (см. Таблица 5).

Таблица 9 – Структура программ КСО

Наименование мероприятия	Элемент	Стейкхолдеры	Сроки	Ожидаемый результат от реализации мероприятия
1. Образовательные мероприятия	Проведение лекций, мастер-классов, презентаций	Компании-резиденты, Население региона Нор-Па-де-Кале, Общественные организации, Сотрудники	ежегодно	Популяризация технологий, науки и инноваций, продвижение бренда
	Профессиональные конференции		ежегодно	
	Мероприятия для детей (введение в программирование, робототехника, техническое творчество)		ежегодно	
2. Благотворительность	Предоставление площадки для благотворительных организаций	Население региона Нор-Па-де-Кале, НКО и фонды	ежегодно	Привлечение внимания к существующим проблемам и поиск совместного пути их решения
	Организация мобильного донорского центра Красного креста		ежегодно	
	Организация сэконд-хенд ярмарок		ежегодно	
3. Спорт и культура	Организация благотворительного забега	Население региона Нор-Па-де-Кале, Компании-резиденты	ежегодно	Участие в культурно-досуговой деятельности региона и ее разнообразие
	Проведение концертов и творческих вечеров	Сотрудники Население	ежегодно	
4. Экологически ориентированное поведение	Облагораживание территорий	Население Экологические организации	ежегодно	Облагораживание территорий региона Нор-Па-де-Кале и города Лилль
	Проведение походов выходного дня	Сотрудники, Компании-резиденты	ежегодно	Продвижение знаний о регионе и здорового образа жизни
5. Охрана труда и промышленная безопасность	Соответствие требованиям международных стандартов OHSAS 18001, ИСО 9001 и осуществлять постоянное совершенствование системы менеджмента	Сотрудники, Компании-резиденты	ежегодно	Своевременная реакция на любые изменения в стандартах и сертификации

Согласно анализируемой документации, компания добросовестно исполняет свои обязательства перед сотрудниками, населением и другими стейкхолдерами.

4.4 Определение затрат на программы КСО

С учетом мероприятий, разработанных в предыдущем пункте, необходимо спланировать бюджет на программы КСО (см. Таблица 6).

Таблица 10 – Затраты на мероприятия КСО

№	Мероприятие	Единица измерения	Цена	Стоимость реализации
1	Проведение лекций, мастер-классов, презентаций	кол-во мероприятий	30 000 EUR	40 000 EUR
2	Профессиональные конференции	кол-во конференций	50 000 EUR	65 000 EUR
3	Мероприятия для детей (введение в программирование, робототехника, техническое творчество)	кол-во участников мероприятия: 20–80	15 000 EUR	15 000 EUR
4	Предоставление площадки для благотворительных организаций	-	Бесплатно	Бесплатно
5	Организация мобильного донорского центра Красного креста	-	Бесплатно	Бесплатно
6	Организация сэконд-хенд ярмарок	-	Бесплатно	Бесплатно
7	Организация благотворительного забега	спонсорский взнос	3 000 EUR	3 000 EUR
8	Проведение концертов и творческих вечеров	кол-во концертов	12 000 EUR	12 000 EUR
9	Облагораживание территорий	размер взноса	10 000 000 EUR	800 000 EUR
10	Проведение походов выходного дня	-	500 EUR	500 EUR
11	Соответствие требованиям международных стандартов OHSAS 18001, ИСО 9001 и осуществлять постоянное совершенствование системы менеджмента	кол-во обученных специалистов	40 000 EUR	45 000 EUR
Итого затраты на КСО				**950 500** EUR

4.5 Оценка эффективности программ и выработка рекомендаций

На основании данных представленных выше, информации о деятельности организации, ее отчетности, можно сделать следующие выводы:

1. Компания EuraTechnologies добросовестно организует свою деятельность согласно утвержденным принципам. Деятельность компании транспарента, много информации в открытом доступе. Руководство компании уважает интересы общества и сотрудников. Программа КСО соответствует стратегии организации.

2. Деление на внешнюю и внутреннюю КСО в данной компании весьма условно: соблюдается баланс интересов и уделяется внимание всем сферам.

3. Программы КСО отвечают интересам всех стейкхолдеров.

4. Реализуя мероприятия КСО, компания создает себе позитивный имидж, осуществляет свою деятельность осознано и ответственно. Организация находится в курсе социально-значимых проблем современного мира и имеет возможность принимать участие в решении этих проблем. В дополнение к этому внутри предприятия складывается благоприятный климат и этическое поведение становится частью жизни не только EuraTechnologies, но и каждого сотрудника.5. Затраты на КСО в целом адекватны полученным результатам. Почти все мероприятия можно оценить с точки зрения эффективности инвестирования, за исключением тех, где нельзя отследить количественный результат.

6. EuraTechnologies можно считать социально-ответственной организацией. Она имеет не просто прописанную программу КСО, а целый комплекс мер по каждому направлению: экология, охрана труда и безопасность, общество. В дополнение к этому можно рекомендовать компании:

- учесть социально-этический аспект в формулировки цели;
- уделить внимания мероприятиям, направленным на потребителя;

– оптимизировать расходы, заменив капиталоемкие проекты на проекты со средним бюджетом, которые обладают примерным социально-значимым эффектом.

Заключение

Информационная безопасность представляет собой крайне важный аспект современной организации. Недостаточное обеспечение информационной безопасности наносит мировой экономике колоссальный ущерб. Для стартапов вопрос информационной безопасности является краеугольным камнем для продолжения и развития своего бизнеса.

Результаты показывают, что организационные меры информационной безопасности ограничивают распространение стратегической информации и делают сотрудников ответственными в их практике обмена информацией. В организационной культуре выделяется роль операционного менеджера. Влияние последнего является важным как в доведении до сведения сотрудников организационных мер безопасности, так в распространении среди сотрудников организационных ценностей.

Дана оценку влиянию ценностей индивидуума и организационной культуры на практику информационной безопасности. Также результаты вносят долю в критический взгляд на теорию социальных сетей, широко признанную в научном сообществе.

Обоснован выбор понятия организационной культуры как важного фактора информационной безопасности. Рассмотрены условия ее формирования и поддержания.

Рассмотрены способы обеспечения информационной безопасности посредством анализа угроз и принятия соответствующих контрмер, моделей управления, разработки политик безопасности и повышения информированности пользователей.

Оценить степень влияния руководителей, организационной культуры и политик безопасности на уровень информационной безопасности в организации.

Провести качественное или количественное исследование для проверки выдвинутых гипотез

Список используемых источников

1. Митник К., Саймон В. Искусство обмана: пер. с англ. – М.: Изд-во Компания АйТи, 2004. – 360 с.
2. Сенат Франции – Информ. отчет № 681 (2011–2012) [Электронный ресурс]: La cyberdéfense: un enjeu mondial, une priorité nationale / Bockel J.-M. URL: http://www.senat.fr/notice-rapport/2011/r11-681-notice.html (дата обращения: 28.11.2017).
3. Ajzen I. The theory of planned behavior //Organizational behavior and human decision processes. – 1991. – Vol. 50. – №. 2. – P. 179-211.
4. Arundel A., Bordoy C., Kanerva M. Neglected innovators: How do innovative firms that do not perform R&D innovate? : Results of an analysis of the Innobarometer 2007 survey No. 215 [Электронный ресурс]. URL: http://pub.maastrichtuniversity.nl/83134293-81ce-4d4f-9cf1-d4943ef03189 (дата обращения: 28.11.2017).
5. Björck F. Institutional theory: A new perspective for research into IS/IT security in organisations // System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on. – IEEE, 2004. – 5 pp.
6. Burt R. Neighbor networks: competitive advantage local and personal. – Oxford: Oxford University Press, 2011. – 389 p.
7. Burt R. Structural holes: the social structure of competition. – Cambridge: Harvard University Press, 1992. – 313 p.
8. CLUSIF. Menaces informatiques et pratiques de sécurité en France, Rapport 2016 [Электронный ресурс]. URL: https://clusif.fr/content/uploads/2016/06/CLUSIF_2016_Rapport-MIPS_vF.pdf (дата обращения: 28.11.2017).
9. CSI Computer Crime and Security Survey. 2011-2012 // CSI Computer Security Institute. – 2011.

10. Choo C. The knowing organization: how organizations use information to construct meaning, create knowledge, and make decisions. – New York: Oxford University Press, 2006. – 2nd ed. – 354 p.
11. Cohen A. Delinquent boys: the culture of the gang. – Glencoe: Free Press, 1955. – 202 p.
12. Coleman J. Social capital in the creation of human capital // American journal of sociology. – 1988. – Vol. 94. – Supplement: Organizations and Institutions: Sociological and Economic Approaches to the Analysis of Social Structure. – P. S95-S120.
13. Cowley S. LinkedIn is a hacker's dream tool [Электронный ресурс]. URL: http://money.cnn.com/2012/03/12/technology/linkedin-hackers/index.htm (дата обращения: 28.11.2017).
14. David J. Policy enforcement in the workplace // Computers & Security. – 2002. – Vol. 21. – №. 6. – P. 506-513.
15. Dhillon G., Backhouse J. Current directions in IS security research: towards socio-organizational perspectives // Information Systems Journal. – 2001. – Vol. 11. – №. 2. – P. 127-153.
16. Dhillon G., Backhouse J. Risks in the use of information technology within organizations // International Journal of Information Management. – 1996. – Vol. 16. – №. 1. – P. 65-74.
17. Doherty N. F., Fulford H. Do information security policies reduce the incidence of security breaches: an exploratory analysis // IGI Global. – 2005.
18. Drucker P. Innovation and entrepreneurship: practice and principles. – New York: Harper & Row, 1985. – 277 p.
19. European Innovation Scoreboard 2007: Comparative analysis of innovation performance. [Электронный ресурс]. URL: https://publications.europa.eu/en/publication-detail/-/publication/71bca3b1-ec59-4172-ac6c-e294acd15bd9 (дата обращения: 28.11.2017).

20. Fishbein M. A., Ajzen I. Belief, attitude, intention and behavior: An introduction to theory and research. – 1975.
21. Fui-Hoon Nah F., Lee-Shang Lau J., Kuang J. Critical factors for successful implementation of enterprise systems // Business process management journal. – 2001. – Vol. 7. – №. 3. – P. 285-296.
22. Garbars K. Implementing an effective IT security program // SANS Institute. Retrieved January. – 2002. – Vol. 11. – P. 2004.
23. Granovetter M. The strength of weak ties // American journal of sociology. – 1973. – Vol. 78. – № 6. – P. 1360-1380.
24. Granovetter M. The strength of weak ties: A network theory revisited // Sociological theory. – 1983. – P. 201-233.
25. ISO/IEC 27002:2005. Code of Practice for Information Security Management. ISO. – 2005.
26. Innobarometer 2007: Analytical Report, Innovation transfer, Flash EB Series No. 215 – The Gallup Organization, 2008 [Электронный ресурс]. URL: http://ec.europa.eu/commfrontoffice/publicopinion/flash/fl_215_en.pdf (дата обращения: 28.11.2017).
27. Knapp K. J. et al. Information security: management's effect on culture and policy // Information Management & Computer Security. – 2006. – Vol. 14. – №. 1. – P. 24-36.
28. Knapp K. J. et al. Top Ranked Information Security Issues // International Information Systems Security Certification Consortium (ISC). – 2004.
29. Kreiner K., Schultz M. Informal collaboration in R & D. The formation of networks across organizations // Organization studies. – 1993. – Vol. 14. – №. 2. – P. 189-209.
30. Ma Q., Johnston A., Pearson J. Information security management objectives and practices: a parsimonious framework // Information Management & Computer Security. – 2008. – Vol. 16. – №. 3. – P. 251-270.
31. Mauss M. Essai sur le don forme et raison de l'échange dans les sociétés archaïques // L’Année sociologique. – 1923. – Vol. 1. – P. 30-186.

32. Mitnick K., Kasperavičius A. CSEPS course workbook. – NY: Mitnick Security Publishing, 2004
33. Nelson R., Winter S. An Evolutionary Theory of Economic Change. – Cambridge: Belknap Press, 1982. – 437 p.
34. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Summary in Russian), 2002 // OECD iLibrary [Электронный ресурс]. URL: http://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-for-the-security-of-information-systems-and-networks/summary/russian_9789264059177-sum-ru (дата обращения: 06.12.2017).
35. Pahnila S., Siponen M., Mahmood A. Employees' behavior towards IS security policy compliance // System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on. – IEEE, 2007. – P. 156b-156b.
36. Rogers E. M. Diffusion of innovations. – Simon and Schuster, 2010.
37. Rogers R. W. A protection motivation theory of fear appeals and attitude change1 //The journal of psychology. – 1975. – Vol. 91. – №. 1. – P. 93-114.
38. Rogers R., Prentice-Dunn S. Protection motivation theory and preventive health: Beyond the health belief model // Health education research. – 1986. – Vol. 1. – №. 3. – P. 153-161.
39. Schein E. Organizational culture and leadership. – San Francisco: Jossey-Bass Publishers, 1985. – 358 p.
40. Schrader S. Informal technology transfer between firms: Cooperation through information trading // Research policy. – 1991. – Vol. 20. – №. 2. – P. 153-170.
41. Schumpeter J. Capitalism, Socialism and Democracy. – New York: Harper & Row, 1942. – 381 p.
42. Schwartz S. Are there universal aspects in the structure and contents of human values? // Journal of social issues. – 1994. – Vol. 50. – №. 4. – P. 19-45.
43. Sellin T. Culture conflict and crime // American Journal of sociology. – 1938. – Vol. 44. – № 1. – P. 97-103.

44. Shedden P., Ruighaver T., Ahmad A. Risk Management Standards and the Perception of Ease of Use. – 2006.
45. Standard of Good Practice for Information Security. – ISF, 2011.
46. Straub D. W., Welke R. J. Coping with systems risk: security planning models for management decision making // MIS quarterly. – 1998. – P. 441-469.
47. Sutherland E., Cressey D. Principles of criminology. – Philadelphia: Lippincott, 1966. – 7th ed. – 721 p.
48. Swanson M., Guttman B. Generally accepted principles and practices for securing information technology systems. – National Institute of Standards and Technology, Technology Administration, US Department of Commerce, 1996. – P. 800-14.
49. Teece D., Pisano G., Shuen A. Dynamic Capabilities and Strategic Management // Strategic Management Journal. – 1997. – Vol. 18. – № 7. – P. 509–533.
50. Tryfonas T., Kiountouzis E., Poulymenakou A. Embedding security practices in contemporary information systems development approaches // Information Management & Computer Security. – 2001. – Vol. 9. – №. 4. – P. 183-197.
51. Von Hippel E. Cooperation between rivals: informal know-how trading // Research policy. – 1987. – Vol. 16. – №. 6. – P. 291-302.
52. Von Solms R., Von Solms B. From policies to culture // Computers & security. – 2004. – Vol. 23. – №. 4. – P. 275-279.
53. Von Solms R., Vroom C. Towards information security behavioural compliance // Computers & Security. – 2004. – Vol. 23. – №. 3. – P. 191-198.
54. Warkentin M., Straub D., Malimage K. Featured talk: Measuring secure behavior: A research commentary //Annual Symposium of Information Assurance & Secure Knowledge Management, Albany, NY. – 2012.
55. Wenger E. Communities of Practice: Learning, Meaning, and Identity. – Cambridge: Cambridge University Press, 1998. 340 c.
56. Wilson M., Hash J. SP 800-50. Building an Information Technology Security Awareness and Training Program. – 2003.

Приложение А

(обязательное)

Part II. Information Security Management

Студент:

Группа	ФИО	Подпись	Дата
3АМ6Ф	Коробков Евгений Игоревич		

Консультант кафедры менеджмента

Должность	ФИО	Ученая степень, звание	Подпись	Дата
заведующий кафедрой	Чистякова Наталья Олеговна	к.э.н.		

Консультант – лингвист кафедры ИЯСГТ :

Должность	ФИО	Ученая степень, звание	Подпись	Дата
заведующий кафедрой	Солодовникова Ольга Владимировна	к.ф.н.		

Part II. Information Security Management

The widespread use of information systems connected to the global and / or local networks in organizations has multiplied the efficiency of many of them, but simultaneously exposed them to the new threats. Although some threats to the information security of organizations are of a technical nature or result from natural disasters, many of them are anthropogenic, whether they are mistakes, omissions or malicious acts committed by employees or external actors such as competitors, hackers, etc.

This increased vulnerability forces most organizations to apply countermeasures to prevent incidents, such as technical and behavioral control measures. Organizations implement policies and procedures for the security of information systems, training and awareness-raising in the field of information security, as well as sanctions for violations of IS policy.

However, these control measures and security measures are effective only to the extent that employees want to follow them, and this is especially true when employees are outside the organization. Information security is a worldwide problem that concerns all market participants regardless of their size or sector of activity.

Von Solms explains that organizations must take into account all aspects of information security. According to him, information security is a multidimensional space that includes corporate governance, organizational structure, policies, best practices, ethics, certification, law, insurance, personnel, information, technology, indicators and audit. Information security means more than preventing malicious users from accessing sensitive data. The international standard ISO / IEC 27002: 2005, which provides a set of rules and regulations for information security management, states that: "Information security protects information from a wide range of threats in order to ensure business continuity, minimize business risk, maximize return on investment, as well as the realization of potential business opportunities".

That's why the information:

- should not be disclosed to unauthorized persons;
- must be protected from unauthorized modification;
- must be available at the request of users.

ISO / IEC 27001: 2005 (clause 3.4, page 2), containing specifications for the implementation of the Information Security Management System (ISMS), defines information security as "maintaining confidentiality, integrity and accessibility of information; in addition, other properties, such as authenticity, impossibility of refusal of authorship, reliability can be included".

Information security focuses on three aspects: confidentiality, integrity and accessibility (paragraphs 3.3, 3.8 and 3.2 respectively).

Confidentiality means that information is only available to those who have the appropriate rights (authorized users). The degree of confidentiality of information depends on its strategic or legal nature. To ensure confidentiality, security mechanisms such as encryption and access control can be used.

Integrity means that the information will not be changed without prior permission. Information should be accurate, complete and protected from change.

Availability is ensuring that information and other resources are accessible by users. To ensure the continuity of available resources, a backup mechanism is used.

These three principles are usually denoted by the abbreviation CIA. However, Dhillon and Backhouse (2000, pp. 127-128) argue that the CIA principles are not sufficient to ensure the security of information. For these authors, information security refers not only to technical environments, but also applies to employees of the organization. Therefore, the authors offer additional principles, such as responsibility, trust and ethics.

Table #1 provides a summary of the twenty-two principles proposed by researchers and information security specialists (Johnston et al. 2008, 256). The sources of these

requirements are three groups: practitioners, scientists and security services. In the survey of these groups, six principles: confidentiality, integrity, accessibility, non-repudiation, authentication and audit. In fact, the table below shows that information security practices define a much more exhaustive list than scientists and security organizations. This list includes evidence systems (for example: signature, witnessing) and tracking (for example: timestamp).

Table 1 – Non-exhaustive list of basic safety principles (Johnston et al, 2008: 254)

	Practitioners						Academics						Organizations				
Principle	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Confidentiality/privacy	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
Integrity	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Availability	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X
Non-repudiation	X	X		X									X		X		
Identification	X																
Authentication	X	X			X			X					X				
Signature	X																
Authorization	X																
Access control	X					X		X									
Validation	X																
Certification	X																
Time-stamping	X																
Receipt	X																
Confirmation	X																
Ownership	X																
Anonymity	X																
Revocation	X																
Witnessing	X																
Utility					X			X									
Possession					X												
Auditability/accountability						X						X		X			X
Ethics									X								

References:

1. Boykin (2003), 2. Host (2001), 3. Krauss and Tipton (2002), 4. Byrnes and Proctor (2002), 5. Parker (2002), 6. Hutt (2002)

7. Leiwo *et al.* (1999), 8. Rosenthal (2002), 9. Dhillon and Torkzadeh (2006),10. Summers (2002), 11. Long (1999), 12. Rannenberg *et al.* (1999)

13. CIECA (2003), 14.ITsecurity.com, 15. SAWG (2002), 16. OIT (2002), 17. GASSP(2003)

Note. Italicized most frequently cited principles of information security

The information security of an organization can be defined as protection from theft of information or any other attack on information systems, as well as protection from failures of information systems that can make them inaccessible and can violate the integrity of information.

Organizations and their information systems must be prepared to respond to a variety of threats. These threats can be caused both by actions of actors outside the organization and by its employees. On this issue, Anderson and Moore (2008: 11) note that the traditional view of security professionals is rather dichotomous when it comes to users of the information system. On the one hand, there are "good guys", that is, members of the organization, and on the other – "bad guys", that is, people outside the organization who want to harm it. But according to the report of Computer Crime and Security Survey (2011: 20), 43.2% of respondents said that at least some of their losses were associated with malicious actions of employees.

2.1 Threats, vulnerabilities and countermeasures

Reports prepared by specialized organizations, such as the Computer Crime and Security Survey, prepared by the Computer Security Institute (CSI) or the CLUSIF reports (French Information Security Club), usually classify attacks as intentional / unintentional and internal / external.

Many publications provide more detailed threat classifications for Hinde (2002), Whitman (2003), Doherty & Fulford (2005), CSI (2009, 2011). Below are some of the main ones, broken down into internal and external to the organization.

External threats:

- Computer viruses, worms and Trojans: computer programs that can be automatically replicated, through various systems and networks;

- Natural disasters: damage is caused by such phenomena as earthquakes, floods or fires;
- Spam (e-mail): mass mailing of unsolicited emails;
- Hacker attack: penetration of the organization's information systems by an unauthorized third party, who can then freely access and manipulate data (theft, modification) or disrupt systems;
- Theft of information by third parties who have been accessed through fraud and manipulation of internal employees (social engineering), and also because of the negligence of internal employees, which allow guests to move unattended to the premises of the organization.

Internal threats:

- Installation / use of unauthorized equipment, peripherals or software: these hardware and software may contain viruses or copying systems;
- Fraudulent use of the information system by users with authorized access;
- Theft of equipment / software / information: theft of valuable hardware, software and information assets;
- Human error: accidental destruction or incorrect data entry.
- Deliberate damage caused by a disgruntled employee for the purpose of carrying out revenge;
- Use of organization resources for illegal or immoral activities;
- Disclosure of confidential information to external organizations or internal third parties that did not need it, regardless of media (files, oral transmission, etc.).

Some threats in organizations are related to software or hardware vulnerabilities, with design flaws in information systems. Human errors in the pursuit of security policy: for example, it may be forgotten to block access to resources to the employee who left the organization.

Thus, information security policies are countermeasures to security violations, provided that they are respected and applied.

After identifying a threat or vulnerability, employees need to know what to do to ensure the safety of information. In this context, it is important that employees know the degree of confidentiality of information and priorities for its protection. They should be able to determine the needs of the CIA in their assets (Garbars, 2002; Lévêque 2006 & Anderson 2003).

Organizations actually apply the risk management approach (Siegel et al., 2002). Risk management is "the cornerstone for effective and focused work, proactive solutions to possible incidents" (Henry, 2007b: 321). Risk assessment allows organizations to know the environment and develop scenarios for combating threats (Swanson & Guttman, 1996).

Risk assessment is the responsibility of the organization: although there is no universal prescription for minimizing risks, specialists need to assess the nature of the organizational environment before considering whether and how to implement IT solutions "(Dhillon & Backhouse, 1996: 73-74).

2.2 Role of the organization

Planning is an important element of management for implementing security measures and justifying their budget. Tryfonas et al. (2001: 188) defines three components of information security planning:

- Strategic planning is the development of policies,
- Tactical planning is the compliance with standards, conducting risk analysis, audit effectiveness, etc.
- Operational planning is the implementation of security tools, such as antivirus, and so on.

However, as Straub & Welke (1998: 441) explains, "the security of information is still ignored by executives, middle managers and employees. The result of this negligence is that security systems are much less reliable than they should be, and that security breaches happen more often and cause more damage".

Dhillon and Backhouse (2001: 126-128) share this view. Information security is not so much a technical problem as social and organizational. It is essential to ensure the development of an appropriate and effective security policy. Indeed, it creates a solid platform for implementing security practices (Von Solms and Solms, 2004: 276). This policy should include at least the following considerations (Verdon, 2006: 49):

- Involve the security team and the legal department to work in the team to assess the policy document for compliance;
- Identify the organization's protection needs;
- Maintain the requirements of the information classification policy;
- Ensure that all employees receive information about the best methods of ensuring information security.

For Tryfonas et al. (2001: 183), the information security policy is a combination of principles, regulations, methods and tools designed to protect an organization from potential threats:

- Organization policy (in terms of structure). This general policy applies to the organization as a whole. It refers to the commitment of the information security management and its importance to the organization. It highlights the responsibilities of everyone in the organization and the means to ensure security.
- Specific policy in the Information and Communication Technologies (ICT) department. These policies cover the duties of the Directorate of Information Systems, whose role is to ensure the security of information systems and

communication networks. It dictates the terms of the software choice, the backup policy, and so on.

- A policy designed for employees. This policy defines a set of information security processes that employees should follow (Internet use, password management, security incident reporting procedure, etc.)

2.3 Policy Objectives

According to David (2002: 506), "security is not what we do or what we do not do. This is not what we allow or do not allow. Security has nothing to do with the level of security of data and systems. Security is how we stick to official security policies."

An effective security policy is a strategy in which people can accept what is expected of them when working with information resources. Therefore, an effective security policy depends not only on what it contains, but also on how participants understand that this policy will achieve the security objectives in the organization.

How to achieve this understanding? Von Solms and von Solms (2004: 4) makes an analogy between the development of the organization's security policies and the creation of the Bible (the Bible metaphorically). They conclude that:

1. The policy should come from the highest level of management in the organization;
2. The overall policy should be stable over time;
3. The general policy should focus on general concepts and should not affect the specific and technical contexts that change over time;
4. Derived policies should be based on a common policy. These policies determine the specifics of technical and business contexts;
5. Procedures should describe how to act in accordance with the policy;

For this, it is necessary to regularly update the rules and procedures and regularly bring information to the members of the organization.

2.4 Theory of action

There are few research papers on malicious behavior in the organization, such as non-compliance with security policies. To a large extent, this seems to be due to the difficulties of data collection, as companies do not want to disclose the problems that arise in this regard.

Nevertheless, we can note that the Theory of Reasonable Action (TRA) (Fishbein and Ajzen, 1975) and its extension, Theory of Planned Behavior (TPB) (Ajzen, 1985) were applied in several studies related to information security. Fishbein and Ajzen explain intention to follow certain behavior. They assume that the intention to perform different types of behavior can be predicted with great accuracy from the attitude toward this behavior, subjective norms and perceived behavioral control. Ajzen (1991) further states that intentions, as well as perceived behavioral control, form a significant part of the differences in actual behavior.

A better understanding of the factors that motivate participants to comply with the organization's information security policy is important to help managers identify gaps in their security management efforts by providing them with the means to solve the behavior problem.

Siponen et al. (2007) attempted to provide empirical evidence on the application of the behavioral model to studying compliance with safety policy in everyday practice. They developed a theoretical model combining the theory of defense motivation (Protection Motivation Theory, Rodgers, 1975), the theory of sound action (Fishbein and Ajzen, 1975, 1980) and the theory of diffusion of innovations (Rodgers, 1962), which was subsequently confirmed by a survey of 971 employees. The results show that employees should be informed and feel able to act in defense of the company's information systems

and that the actions taken by the management are considered relevant and adapted to the company's actual operations. The study of behavioral changes has revealed the value of raising awareness and, consequently, of learning.

2.5 Raising awareness of information security

For the National Institute of Standards and Technology (NIST 800-50, 2003: 8-9), raising awareness is not training. It is designed to draw attention to security and allow everyone to feel involved and adopt appropriate behavior. Awareness raising is aimed at a wide audience, while training is provided to small groups. Learners acquire practical knowledge that allows them to be more effective in their activities. Training combines the totality of knowledge, both technical and social, aimed at training specialists in information security.

According to SOGP (Standard of Good Practices, 2011: CF 2.2), the information program should promote a "positive safety culture". The difference between awareness and training or education is not made. It is about holding awareness-raising trainings. These trainings should be regular, encouraged by management and addressed to all members of the organization.

Advantages of increasing the level of information system users' awareness:

- targeting a heterogeneous audience, not just information systems specialists, which allows (1) to explain the goal of safe behavior, (2) to spread good practices and (3) to provide assistance, if necessary;
- computer security specialists receive feedback and reports on possible incidents.

The goal of raising awareness is defined as the development of a "positive safety culture" in organizations and the effectiveness of this process is achieved only under certain conditions. First of all, regular training requires material means and organization. Therefore, raising awareness requires, on the one hand, the budget, and on the other the

structure responsible for its organization. It can be a designated manager that relies on an internal command or an external service.

Awareness-raising should be based on simple terms that are understandable to as many people as possible (ENISA 2006, Goucher 2008). It must also conform to the organizational structure, so ENISA (2006) and SOGP (2011: SG 1.1.3) indicate that awareness-raising should:

- Meet the needs of listeners,
- Propose realistic actions,
- Show what listeners can get by participating in information security,
- Meet the business strategy, objectives and strategic vision defined by management.

Like security policies, awareness-raising should be based on organizational culture (Casmir and Yngstrom, 2005). Siponen (2000) also believes that awareness-raising should promote morality and ethics that respond to security needs, as they are powerful vectors for behavior change.

Participation of senior management is also a prerequisite for the success of awareness-raising (SOGP, 2011: CF 2.2, Maeyer, 2007). It must ensure the effective promotion of best practices and allocate the necessary financial, material and human resources. On the other hand, Maeyer (2007), shows that too informal training on too general topics may be the cause of the failure of awareness.

When studying the behavior of remote employees, Furnell (2006) notes that awareness raising has a significant impact on the perception of safety. These results are interesting in that they show how an individual, even outside the organizational context, can behave in accordance with the expectations of the organization, if he believes that this is important. This is the effect of normative pressure. The employee accepts behavior, which, in his opinion, is not excluded from the organization during remote work.

However, this does not mean that such employees have learned the security values promoted by the organization. Perhaps their behavior will change as a result of changing the workplace, where security is perceived as less important. This emphasizes the role of local participants, especially the operations manager. In fact, the influence of the operational manager on the awareness and behavior of employees has been little studied. However, the operational manager has local authority, strategy and values of the organization. This can potentially be significant for raising awareness and adopting behavior that meets safety requirements.

2.6 The relationship between organizational culture and information security

Security includes complex social constructs, such as identification, trust and confidentiality, which vary depending on the context. An approach that takes into account the best interests of all participants and the characteristics of information systems, networks and related services can be both effective and safe.

The OECD's approach to the formation of a culture of information security includes nine mutually complementary principles (see Table 2).

Table 2 – Formation of a culture of security (OECD 2002, pp. 5-8)

Principle	Definition
1) Awareness	Participating parties should be aware of the need to ensure the security of information systems and networks and understand what they can do to improve security.
2) Responsibility	The security of information systems and networks is the responsibility of all parties involved.

3) Taking Response	Participating parties should, in cooperation with others, take timely action to prevent, identify and respond to incidents involving security breaches.
4) Ethics	The parties involved must take into account the legitimate interests of other individuals and organizations.
5) Democracy	Ensuring the security of information systems and networks should not conflict with the fundamental values of a democratic society.
6) Risk assessment	Participating parties should conduct risk assessment.
7) Development and implementation of systems and networks taking into account the need for security	Participating parties should consider security as one of the most important elements of information systems and networks.
8) Security management	Participating parties should adopt an integrated approach to security management.
9) Reassessment	Participating parties should review and reassess the security of information systems and networks, and make appropriate changes to security policies, practices, measures and procedures.

The OECD definition focuses more on the cultural dimension that is central to security activities, which largely depends on the level of perception of participants: "Security management should be based on risk assessment. It must be dynamic, covering all levels

of activity of the parties involved and all aspects of their work. It should include a proactive response to emerging threats and should include measures to prevent and detect incidents and respond to them, measures to restore systems after disruptions, continuous maintenance, analysis and audit. Policies, practices, measures and procedures for the security of information systems and networks should be coordinated and integrated so as to form a coherent security system. The requirements for security management depend on the level of participation, the role and functions of the participating party, the existing risk and the requirements for the system".

Many researchers also suggest that information security should be part of the organizational culture (Von Solms 2000, Schlienger and Teufel 2002, 2003). Knapp et al. (2006) found that in most organizations, information security is not an integral part of the organizational culture. To explain this phenomenon, there are several reasons, for example:

- Lack of financial investments – Shedden et al. (2006) showed that organizations tend to view security spending as justified after an incident occurred, that is too late.
- Insufficient staff participation – some researchers have pointed to the passive participation of employees in implementing security measures, the implementation of which often falls on the shoulders of units (Chia et al, 2002, Koh et al, 2005).
- Limited implementation of security measures: the Maynard & Ruighaver (2006) study shows that the implementation of a security policy in most cases does not result from beliefs but from the need for compliance and enforcement through external audits.

The literature also shows that there are three types of relationship between organizational culture and information security.

1. Information security is not integrated into the organizational culture (Chia et al, 2002, Knapp, Marshall, Rainer et al, 2004, Koh et al, 2005). In this case, the organization management does not deal with information security. Members of the organization are poorly informed and do not feel responsible for security problems. Organizations are often inclined to view spending on security as unjustified spending (Shedden et al, 2006). This is the situation where information security activities are supported only by the IT department.
2. Information security – the "subculture" of organizational culture. Part of the staff is more aware of the requirements for security, periodic security training is conducted. Some departments of the organization begin to pay attention to safety, and the issue of new practices appears in the agenda of the leadership.
3. Information security is built into the organizational culture. Security measures are implemented throughout the organization and with a relatively high level of participation. In addition, security policies are regularly updated. Members of the organization feel responsible for the information and are motivated to adhere to the security policy. Security practices become unconscious everyday activities (Von Solms, 2000, Vroom and Von Solms, 2004, Thomson and Von Solms, 2005, Thomson et al, 2006). Management and employees of the organization share common values of information security.

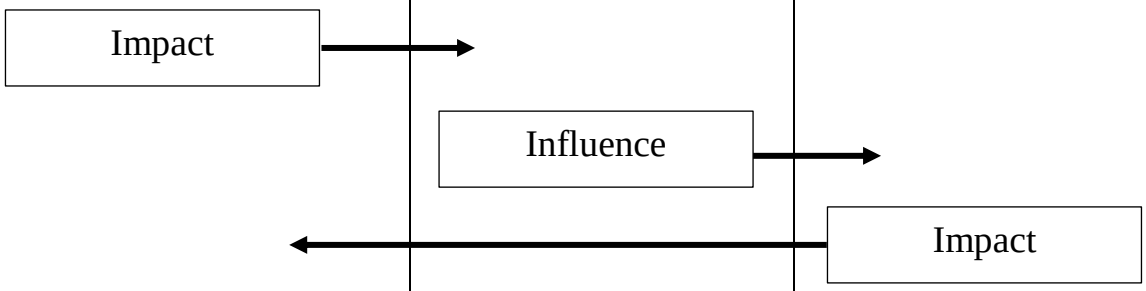
How is the third type of relationship achieved? The review of the literature makes it possible to identify several variables capable of developing the organizational culture, but their influence, in particular on actual practices, remains poorly understood.

1. Security policies;
2. Participation of top management;
3. Awareness;
4. IT department / Security department;
5. Participation of operational management.

Some security measures operate directly at the organizational level, affecting the "mass" awareness of IS threats, while others affect individuals. This increase in individual awareness adapts the individual culture to bring it in line with the organizational culture.

Table 3 shows how the security components in the cycle affect the individual culture and through it change the organizational culture.

Table 3 – Impact of safety components on individual and organizational culture

Component	Subject	Organizational culture
		
Involvement and promotion by management	Organization	Organizational
Security Policies		
IT department		
Raise awareness	Individual	Individual
Participation of operational managers		
Experience		