Цель: разработать проект политики информационной безопасности бизнес-компании.

**Введение**

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Большинство крупных компаний в Беларуси не всегда готовы защитить свою безопасность в сфере информационного взаимодействия с другими организациями. Утечки информации, неосторожное поведение сотрудников, диффамация – все это подрывает конкурентоспособность компании. При разработке системы защиты необходимо опираться и на белорусские, и на международные стандарты. Это позволит и взаимодействовать с белорусскими государственными органами в соответствующем правовом поле, и успешно сотрудничать с зарубежными партнерами.

Прежде всего политика необходима для того, чтобы донести до бизнеса цели и задачи информационной безопасности компании. Бизнес должен понимать, что агент безопасности – это не только инструмент для расследования фактов утечек данных, но и помощник в минимизации рисков компании, а, следовательно, ­­­­­­­­– в повышении прибыльности компании.

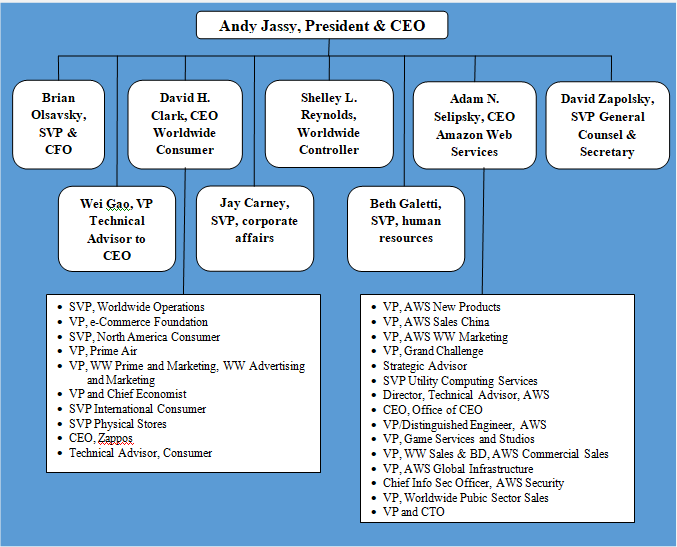
**Описание структуры компании**

**Организационная структура компании** — это руководство для пользования, которое объясняет, как организация выстроена и как она работает. Организационная структура описывает, как в компании принимаются решения, и кто является ее лидером.

Почему необходимо разрабатывать организационную структуру предприятия?

* Организационная структура дает четкое понимание того, в каком направлении движется компания. Ясная структура — это инструмент, с помощью которого можно придерживаться порядка в принятии решений и преодолевать различные разногласия.
* Организационная структура связывает участников. Благодаря ей люди, присоединяющиеся к группе, имеют отличительные черты. В то же время и сама группа обладает определенными особенностями.
* Организационная структура формируется неизбежно. Любая организация по определению подразумевает какую-то структуру.

Организационная структура Amazon:



1. Иерархическая корпоративная структура. Иерархическая структура в Amazon сложилась из-за огромных размеров бизнеса. В крупнейшем интернет-ритейлере в мире по объему выручки работает более 1,3 миллиона человек по всему миру.

2. Гибридные проектные группы. Корпоративная структура Amazon объединяет гибридные проектные группы при разработке новых продуктов и услуг. Специалисты из различных отделов привлекаются в соответствии с их навыками и компетенциями, необходимыми для проекта. Эти сотрудники могут быть привлечены на неполный рабочий день для отчетности как перед руководителями своих отделов, так и перед руководителями проектов, или они могут участвовать в проекте на полный рабочий день, отчитываясь перед менеджером проекта только на время проекта.

3. Гибкость бизнеса. Важно отметить, что, несмотря на свой большой размер, в отличие от многих других компаний с иерархической организационной структурой, Amazon остается очень гибкой, чтобы адаптироваться к частым изменениям на внешнем рынке. Более того, гигант онлайн-ритейла приводит к изменениям во внешней бизнес-среде; это привело к прорывным инновациям в электронной коммерции, и в настоящее время это приведет к прорывным инновациям в глобальной логистической отрасли. Успешная организация гибридных проектных групп играет важную роль в поддержании гибкости бизнеса.

Организационная структура Amazon объединяет множество небольших команд, которые занимаются различными аспектами бизнеса. Основателю Amazon и бывшему генеральному директору Джеффу Безосу приписывают введение ”правила двух пицц". Согласно этому правилу, встречи должны проводиться в командах, достаточно маленьких, чтобы всех можно было накормить всего двумя пиццами. “Правило двух пицц” действует и по сей день под руководством нового генерального директора Энди Джасси.

4. Стабильность в высшем руководстве. Стабильность - одна из ключевых особенностей Amazon. В частности, крупнейшая по выручке интернет-компания испытывает “очень небольшую текучесть кадров среди своих наиболее важных влиятельных игроков, причем многие из них работают в компании годами, если не десятилетиями”. Это довольно необычно для современных компаний, где изменения в команде высшего руководства стали частым явлением.

**Оценка рисков**

**Анализ информационных рисков** — это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков. При этом риск — это вероятный ущерб, который зависит от защищенности системы. Итак, из определения следует, что на выходе алгоритма анализа риска можно получить либо количественную оценку рисков (риск измеряется в деньгах), либо — качественную (уровни риска; обычно: высокий, средний, низкий).

На сегодня не существует единой методики количественного расчета величин рисков, измеряемой в стоимостной оценки.

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

* антропогенные,
* техногенные,
* естественные (природные).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Главпочтамта могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* противозаконный сбор и использование информации;
* использование информационного оружия.

К программным угрозам относятся:

* использование ошибок и «дыр» в ПО;
* компьютерные вирусы и вредоносные программы;

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи;

**Общие положения**

Безопасность объектов информатизации достигается противодействием всем видам угроз, внешним и внутренним, умышленным и непреднамеренным, минимизацией ущерба от возможной реализации угрозы безопасности персональных данных, исключением несанкционированного, в том числе случайного, доступа к объектам защиты. Персональные данные подлежат защите в контролируемой зоне и при передаче по каналам связи за ее границы.

**Область действия**

Требования Политики распространяются на всех сотрудников, а также прочих лиц, привлекаемых к исполнению работ связанных с обработкой персональных данных.

**Система защиты персональных данных (СЗПДн)**

Система (подсистема) защиты персональных данных строится на основании регулярных внутренних проверок состава персональных данных (ПДн), соответствия уровня защиты составу ПДн, выявления угроз безопасности. Для достижения необходимого уровня безопасности выполняются плановые обучающие, административные и технические мероприятия. В составе СЗПД действуют следующие стандартные подсистемы:

* управления доступом, регистрации и учета;
* обеспечения целостности и доступности;
* антивирусной защиты;
* межсетевого экранирования;
* анализа защищенности;
* обнаружения вторжений;
* криптографической защиты.

**Разработка мер защиты**

Проведение мероприятий, направленных на постоянное повышение осведомленности работников в области ИБ, должна являться одной из задач. Необходимо проведение периодического практического тестирования готовности работников к выполнению своих должностных обязанностей по защите информации. Конкретные требования по обеспечению ИБ должны быть внесены в должностные регламенты всех работников, в зависимости от их должностных обязанностей. Подбор, и порядок вступления в договорные и трудовые отношения и их расторжения, а также ежедневное выполнение работником его должностных обязанностей, должны соответствовать требованиям НПА (нормативного правового акта) РБ. Порядок допуска сотрудника к работе с информацией ограниченного доступа, порядок работы с такой информацией и порядок прекращения допуска к такой информации, должен соответствовать НПА РБ. В «Политику повышения осведомленности в области ИБ и кадровую политику» входят такие процедуры и процессы, как:

1) Требования до приема на работу

2) Требования при выполнении должностных обязанностей

3) Требования при прекращении выполнения должностных обязанностей

1. Политика безопасности

1.1 Сотрудники обязаны обеспечивать сохранность всей конфиденциальной/конфиденциальной информации в печатном или электронном виде на своем рабочем месте в конце рабочего дня и когда ожидается, что они будут отсутствовать в течение длительного периода.

1.2 Рабочие станции компьютеров должны быть заблокированы, когда рабочее пространство не занято.

1.3 Компьютерные рабочие станции должны быть полностью выключены в конце рабочего дня.

1.4 Любая ограниченная или конфиденциальная информация должна быть удалена со стола и заперта в ящике, когда стол свободен и в конце рабочего дня.

1.5 Картотечные шкафы, содержащие ограниченную или конфиденциальную информацию, должны храниться закрытыми и запертыми, когда они не используются или когда их не посещают.

1.6 Ключи, используемые для доступа к закрытой или конфиденциальной информации, нельзя оставлять на столе без присмотра.

1.7 Ноутбуки должны быть либо заблокированы с помощью фиксирующего кабеля, либо заперты в ящике стола.

1.8 Пароли нельзя оставлять на стикерах, размещенных на компьютере или под ним, а также оставлять записанными в доступном месте.

1.9 Распечатки, содержащие ограниченную или конфиденциальную информацию, должны быть немедленно удалены из принтера.

1.10 При утилизации Ограниченные и/ или конфиденциальные документы должны быть уничтожены в официальных контейнерах для измельчения или помещены в закрытые контейнеры для конфиденциальной утилизации.

1.11 Доски, содержащие ограниченную и/или конфиденциальную информацию, должны быть удалены.

1.12 Блокируйте портативные вычислительные устройства, такие как ноутбуки и планшеты.

1.13 Относитесь к устройствам хранения данных, таким как CDROM, DVD или USB-накопители, как к конфиденциальным и храните их в запертом ящике

**Выводы**

Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот.

Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Опыт показывает, что для достижения удачных решений по защите информации кампаний необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.