Учреждение образования

«Белорусский государственный технологический университет»

**Практическое занятие №2**

**«Разработка политики информационной безопасности бизнес-компании»**

Выполнил:

Студент 2 курса 1 группы ФИТ

Палазник Арсений Викторович

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.

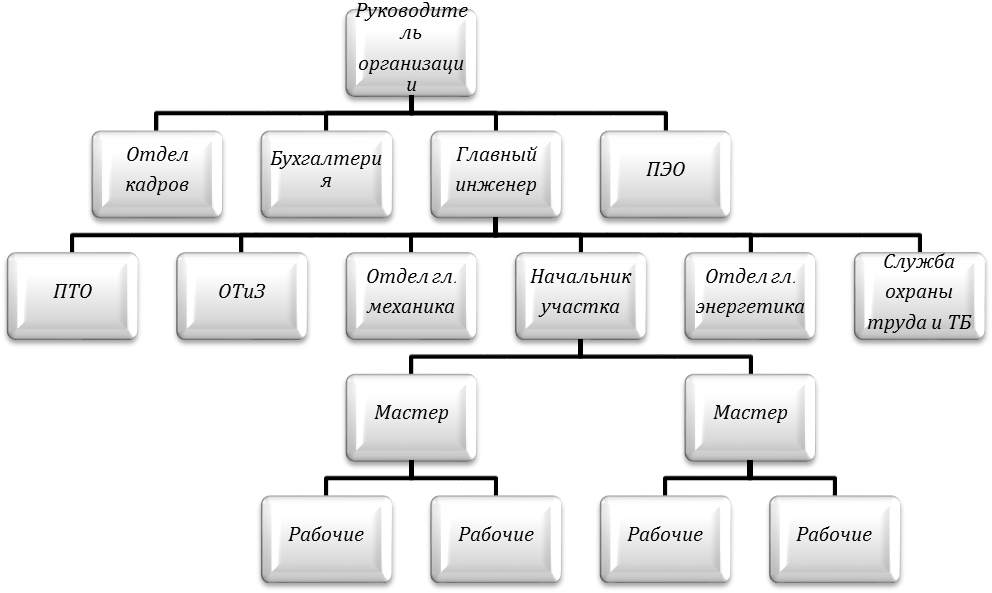
**Описание структуры компании**

**Организационная структура компании** — документ, схематически отражающий состав и иерархию подразделений предприятия.

**Почему необходимо разрабатывать организационную структуру предприятия?**

* Четкое понимание порядка принятия решений и взаимодействия между подразделениями и отдельными работниками
* Увязка всех рабочих процессов и их участников
* Группировку структурных единиц по определенным характеристикам
* Отсутствие дублирования каких-либо функциональных обязанностей
* Распределение полномочий и обязанностей между работниками, имеющими определенные профессиональные знания, навыки и опыт
* Формирование перечня необходимых сотрудников, уровня их квалификации, должностных обязанностей

Организационная структура строительной организации верхнего уровня



Исходя из анализа организационной структуры, представленной выше, можно сделать вывод, что структура относится к функциональному типу.

**Функциональная структура**

Распределение основных направлений и вертикалей по выполняемым функциям. Чаще всего, структура выстраивается с разбивкой по таким блокам: производство, продажа, маркетинг, бухгалтерский и налоговый учет, финансовый менеджмент и пр.

Преимущества:

* Высокая степень специализации.
* Понятная схема подчинения работников, которая выстраивается по направлениям.
* Четкое понимание ответственности за определенные блоки работ.
* Высокая эффективность и скорость.
* Отсутствие необходимости в дублировании работы.

Недостатки:

* Коммуникация сталкивается с несколькими барьерами.
* В центре внимания находятся люди, а не организация.
* Решения, принятые единственным человеком, могут не всегда идти на пользу организации.
* По мере роста компании становится труднее осуществлять контроль над действиями внутри нее.
* Отсутствие командной работы между различными отделами или единицами.
* Поскольку все функции отделены, сотрудники могут не знать о том, что творится у коллег.

**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;

Основными угрозами информационной безопасности является:

- незаконное копирование данных и распространение их;

- несанкционированный доступ к информационным ресурсам;

- редактирование личной информации посетителей и работников

Создание эффективной стратегии информационной безопасности требует применения различных инструментов и технологий. В большинстве стратегий используется определенная комбинация технологий:

- Система обнаружения вторжений (IDS) – это инструменты для мониторинга входящего трафика и обнаружения угроз.

- Система предотвращения вторжений (IPS) – эти решения реагируют на трафик, который идентифицируется как подозрительный или вредоносный, блокируя запросы или завершая сеансы пользователя.

- Брандмауэры –позволяют фильтровать трафик и передавать данные о трафике в системы мониторинга и обнаружения.

- Блокчейн-кибербезопасность – это технология, которая опирается на неизменяемые транзакционные события. В блокчейн-технологиях распределенные сети пользователей проверяют подлинность транзакций и обеспечивают поддержание целостности.

- Поведенческая аналитика пользователей (UBA) – решения UBA собирают информацию о действиях пользователей и соотносят их поведение с базовым уровнем. Затем решения используют этот базовый уровень в качестве сравнения с новыми моделями поведения для выявления несоответствий. Затем решение помечает эти несоответствия как потенциальные угрозы.

- Управление положением облачной безопасности (CSPM) – это набор практик и технологий, которые вы можете использовать для оценки безопасности ваших облачных ресурсов. Эти технологии позволяют сканировать конфигурации, сравнивать средства защиты с эталонными показателями и обеспечивать единообразное применение политик безопасности

**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 СЗПДн действуют следующие стандартные подсистемы:

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

Функционал подсистем СЗПДн учитывает класс ИСПДн.

**Пользователи информационной системы персональных данных (ИСПДн)**

На основании проводимой Политики произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности по обработке. Каждая группа пользователей, получает доступ и информированность в соответствие с компетентностью.

**Требования к персоналу по обеспечению защиты ПДн**

Все сотрудники, являющиеся пользователями ИСПДн, знают и выполняют установленные правила доступа к защищаемым объектам, соблюдают режим безопасности.

При вступлении в должность нового сотрудника организовано его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн. Проводится обучение навыкам санкционированного использования ИСПДн.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами, третьим лицам. При работе с ПДн обеспечивается перекрывание просмотра ПДн третьими лицами.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн. По выявленным событиям организуется немедленное реагирование на угрозы безопасности ПДн.

**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. Общий обзор

Политика чистого рабочего стола может быть инструментом импорта для обеспечения того, чтобы все конфиденциальные / конфиденциальные материалы удалялись из рабочей области конечного пользователя и блокировались, когда элементы не используются или сотрудник покидает свое рабочее место. Это одна из лучших стратегий, которую следует использовать при попытке снизить риск нарушений безопасности на рабочем месте. Такая политика также может повысить осведомленность сотрудников о защите конфиденциальной информации.

2. Цель

Целью этой политики является установление минимальных требований для поддержания “чистого рабочего стола”, где конфиденциальная / важная информация о наших сотрудниках, нашей интеллектуальной собственности, наших клиентах и наших поставщиках находится в безопасности в закрытых помещениях и за пределами сайта. Политика чистого рабочего стола не только соответствует стандарту ISO 27001/17799, но и является частью стандартного базового контроля конфиденциальности.

3. Сфера применения

Эта политика применяется ко всем сотрудникам и аффилированным лицам стоматологической компании.

4. Политика

4.1 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.

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

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

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

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

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

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

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

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

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

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

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

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

Все принтеры и факсимильные аппараты должны быть очищены от бумаги сразу после их печати; это помогает гарантировать, что конфиденциальные документы не будут оставлены в лотках принтера для получения не тем человеком.

5. Соблюдение Политики

5.1 Измерение Соответствия требованиям

Команда Infosec будет проверять соответствие этой политике с помощью различных методов (например, проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите и т.п.), включая, но не ограничиваясь этим, периодические обходы, видеомониторинг, отчеты о бизнес-инструментах, внутренние и внешние аудиты и обратную связь с владельцем политики.

5.2 Исключения

Любое исключение из политики должно быть заранее одобрено командой Infosec.

5.3 Несоблюдение требований

Сотрудник, уличенный в нарушении этой политики, может быть привлечен к дисциплинарной ответственности, вплоть до увольнения с работы.

**Выводы**

Важно помнить, что, прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

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