Учреждение образования

«Белорусский государственный технологический университет»

**Отчеты по практическим работам**

По дисциплине: «Основы защиты информации»

Студентки 2 курса 1 группы ФИТ

Шимчёнок Елизаветы Константиновны

**2022 г.**

**Цель работы:** разработать проект политики информационной безопасности бизнес-компании.

# **Введение**

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных.

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

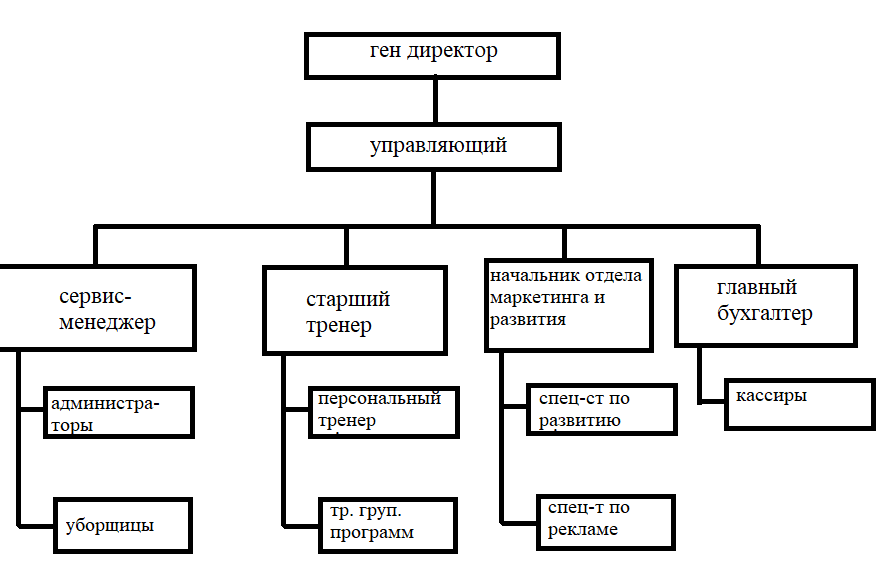
Учитывая важность информации в современном мире, защите от утечек конфиденциальной информации в адрес конкурентов необходимо уделять повышенное внимание. Возможный ущерб невозможно спрогнозировать заранее. Он может выражаться в незначительной сумме, но в некоторых случаях приводит к полной неспособности компании заниматься хозяйственной деятельностью.

Таким образом, можно сделать вывод, что информационные ресурсы в современном обществе являются весьма значимыми, но при этом, очень уязвимыми, благодаря чему информационная безопасность — одно из важнейших условий функционирования любой структуры, будь то государственное учреждение или частное предприятие.

# **Структура организации**

Структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Опишем структуру тренажерного зала «Sport»:



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

# **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).

**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 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**

На основании анализа рисков, а также фактического уровня информационной безопасности рекламного агентства и выбираются средства, обеспечивающие информационную безопасность компании.

Меры по обеспечению информационной безопасности на предприятии можно выделить:

• управление персоналом;

• осуществление физической защиты территории предприятия;

• поддержание работоспособности системы защиты информации;

На программно-техническом уровне реализуются следующие механизмы обеспечения безопасности:

• управление доступом;

• идентификация и аутентификация пользователей;

• протоколирование и аудит;

• удаление остаточной информации;

• шифрование передаваемой информации;

• включение серверных помещений;

• применение сетевых фильтров и бесперебойников электропитания.

Соответственно в компании должны быть разработаны и введены в действие следующие локальные нормативные акты, регулирующие деятельность по обеспечению конфиденциальности и безопасности:

- Политика в области обработки и защиты персональных данных;

- Положение о коммерческой тайне;

- Положение об обработке и защите персональных данных без использования средств автоматизации;

- Перечень конфиденциальной информации, подлежащей защите;

- Положение о мерах по организации защиты информационных систем персональных данных на Предприятии;

- Политика по защите персональных данных;

- Положение об обработке и защите персональных данных Работников.

Исходя из представленной выше информации, можно сделать вывод, что в компании должны быть проведены такие организационные мероприятия, как формулирование перечня мер по обеспечению безопасности и срочному восстановлению данных при сбоях системы; обучение сотрудников автоматизированной информационной системы рекламного агентства правилам и процедурам работы с конфиденциальной информацией; ограничение доступа посторонних лиц в помещение; ограничение круга лиц, имеющих доступ к важным данным в информационные системы рекламного агентства.

Также должен быть проведен ряд административных мероприятий:

 поддержка правильной конфигурации ОС;

 применение инженерно-технических средств защиты информации (телекоммуникационный шкаф, межсетевой экран, дверь и запирающий её механизм минимум 3 класса защиты);

 контроль журналов входа (выхода) субъектов доступа в (из) систему, доступа программ к защищаемым данным;

 контроль целостности защищаемых данных;

 контроль смены паролей;

 применение средств антивирусной защиты (например, покупка и установка Kaspersky Endpoint Security);

 проведение тестирования средств защиты информации.

# **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.