Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Разработка и внедрение политики безопасности страховой компании

Студент: Валдайцев А. Д.

ФИТ 3 курс 5 группа

Преподаватель:

Минск 2023

**Содержание**

[ВВЕДЕНИЕ 3](#_Toc126613529)

[1. Объекты защиты 5](#_Toc126613530)

[1.1. Описание структуры организации 5](#_Toc126613531)

[1.2. Внутренняя структура организации 5](#_Toc126613532)

[1.3. Обзор объектов и субъектов информационных отношений 8](#_Toc126613533)

[1.3.1. Объекты информационных отношений 8](#_Toc126613534)

# ВВЕДЕНИЕ

В современном мире информация в виде отдельного ресурса имеет критическую важность и ключевое значение. Каждый человек тем или иным образом использует информационные ресурсы, базы данных, системы управления и организации информации. В том числе в организациях и учреждениях информация и, в частности, её защита, имеет ключевую роль.

Информация по своей сущности является крайне уязвимой, поэтому в любой организации или учреждении информационная безопасность является важнейшим условием для функционирования. В качестве основного подхода для организации информационной безопасности используется создание политики информационной безопасности, а также её пересмотр, усовершенствование и внедрение на всех уровнях учреждения или организации.

Политикой информационной безопасности организации или учреждения называется совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

Политика информационной безопасности направлена на минимизацию рисков утечки, повреждения, искажения, блокировки доступа и уничтожения данных и информации. Актуальность её разработки заключается в том, что ПИБ является одним из основных условий функционирования любого учреждения, описывает и классифицирует возможные угрозы, уязвимости системы, а также характеризует риски возникновения угроз и возможный ущерб, и документирует алгоритм действий при аварийных ситуациях, что позволяет на основании этого выбрать средства управления информационной системой. В связи с этим можно выделить следующие цели и задачи разработки политики информационной безопасности:

Цели:

* сохранение целостности критически важных данных;
* обеспечение надёжности и безопасности информационных ресурсов;
* обеспечение конфиденциальности, целостности и доступности всех компонентов информационной системы;
* обеспечение непрерывности и безопасности информационных процессов:
* предотвращение или снижение ущерба информационной системы от дестабилизирующих факторов.

Задачи:

* разработка концепции, стандартов, процедур, инструкций и планов мероприятий по защите информации;
* описание структуры организации и характеристика всех возможных объектов и субъектов защиты;
* выявление основных уязвимостей и угроз информационной безопасности и их источников, оценка вероятности их возникновения;
* оценивание рисков на основании вероятности возникновения и возможного ущерба от потенциальных угроз;
* разработка мер, методов и средств обеспечения необходимого уровня защищённости информационной системы.

# 1. Объекты защиты

# Описание структуры организации

В страховой компании для распределения обязанностей и полномочий работников существует организационная структура. Разделение труда и создание организационных структур (отделов, управлений, департаментов) обеспечивает оптимальность, оперативность, экономичность и надёжность функционирования такой организации, как страховая компания.

Общие принципы формирования структуры организации предусматривает предусматривают создание центров управления по двум основным признакам — иерархическому и функциональному.

Иерархическое построение центров управления (вертикальная структура) предусматривает выделение различных уровней управления организацией. Наиболее распространены структуры управления, где верхний уровень представлен главным аппаратом управления организацией, а нижние уровни — службами управления отдельными подразделениями, отделами, управлениями и департаментами.

Функциональное построение центров управления (горизонтальная структура) основано на распределении функций в рамках одного иерархического уровня. В рамках этой системы сотрудник получает указания не от одного, а от ряда вышестоящих сотрудников, и о своей деятельности он информирует не одного человека, а определенное число сотрудников, которые работают в той же области. Однако, он продолжает подчиняться только одному начальнику.

# Внутренняя структура организации

Рассмотрим подробнее внутреннюю структуру страховой компании, её распределение по отделам, управлениям, департаментам и прочим структурным единицам.

Общее собрание акционеров — это высший орган управления страховой компанией, который принимает решения об управлении капиталом и финансированием организации.

Совет директоров — руководители организации, которые выбираются общим собранием акционеров, и образуют основное правление и выбирают председателя правления. Совет директоров производят назначения на руководящие посты, совершают стратегические решения по выбору направления развития компании, но не осуществляют повседневного управления организацией.

Наблюдательный совет — отдел, контролирующий состояние компании и избираемый общим собранием акционеров.

Генеральным директором может быть председатель правления или президент страховой компании.

Вице-президент — это финансовый директор страховой компании, отвечающий за финансовые вопросы организации.

Число директоров организации может различаться в зависимости от масштаба страховой компании и объёмов указываемых услуг. Например, в организации также могут существовать директора:

* финансовый директор;
* директор по страхованию;
* директор по маркетингу;
* региональный директор;
* директор по имущественному страхованию;
* директор но личному страхованию;
* директор по перестрахованию.

Внутренняя структура управлений страховой компании может состоять из основных и вспомогательных отделов.

Управление личного страхования — отдел, который занимается управляет продуктом по личному страхованию и взаимодействует с отделом рекламы и маркетинга.

Управление имущественного страхования — отдел, проводящий аналогичную работу по имущественному страхованию и страхованию ответственности.

Управление региональной сети — отдел, который работает с филиалами и координирует и контролирует их деятельность.

Отдел рекламы и маркетинга — основной отдел, входящий в управление региональной сети, который занимается рекламой страховых услуг, изучает страховой рынок, составляет прогнозы его развития и взаимодействует со всеми остальными управлениями.

Отдел планирования — составляет краткосрочные, среднесрочные и долгосрочные планы развития страховой компании, анализирует отчетность и по результатам анализа вносит предложения по улучшению финансовых показателей организации.

Бухгалтерия — отдел, который ведет бухгалтерский учет и составляет текущую и годовую отчетность.

Отдел кадров — отдел, который осуществляет кадровое обеспечение страховой компании.

Структура страховой компании представлена на рисунке 1.1.

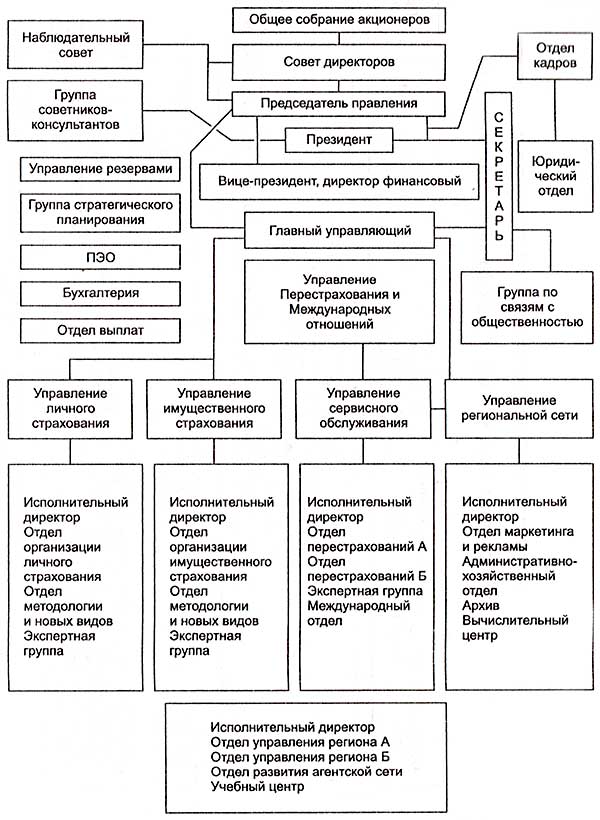


Рисунок 1.1 — Структура страховой компании

# Обзор объектов и субъектов информационных отношений

В данном разделе будут рассмотрены основные объекты и субъекты информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию, например: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

Субъект – активный компонент системы, который может инициировать поток информации, например: пользователь, процесс либо устройство.

# Объекты информационных отношений

Обеспечение безопасности и надёжности объектов информации является одной из основных задач при разработке политики информационной безопасности. В страховой компании можно выделить следующие объекты, требующие обеспечения информационной безопасности:

* технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);
* информационные ресурсы, в том числе содержащие сведения ограниченного распространения и представленные в виде документов в носителях на магнитной, оптической и другой основе, массивах и базах данных;
* программные средства (операционные системы, системы управления базами данных и другое программное обеспечение);
* каналы связи, передающие информацию (кабельные и беспроводные, локальные и глобальные каналы связи).