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](#_Toc126602841)

# 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.

# Объекты защиты