Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Разработка и внедрение политики безопасности страховой компании

Студент: Валдайцев А. Д.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Содержание**

[ВВЕДЕНИЕ 3](#_Toc127041387)

[1. Объекты защиты 5](#_Toc127041388)

[1.1. Описание структуры организации 5](#_Toc127041389)

[1.2. Внутренняя структура организации 5](#_Toc127041390)

[1.3. Обзор объектов и субъектов информационных отношений 8](#_Toc127041391)

[1.3.1. Объекты информационных отношений 8](#_Toc127041392)

[1.3.2. Субъекты информационных отношений 8](#_Toc127041393)

[2. Основные угрозы и их источники 9](#_Toc127041394)

[2.1. Внутренние угрозы 9](#_Toc127041395)

[2.2. Внешние угрозы 10](#_Toc127041396)

[2.3. Естественные угрозы 10](#_Toc127041397)

[2.4. Искусственные угрозы 11](#_Toc127041398)

[2.5. Непреднамеренные угрозы 11](#_Toc127041399)

[2.6. Преднамеренные угрозы 12](#_Toc127041400)

# 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

# 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.

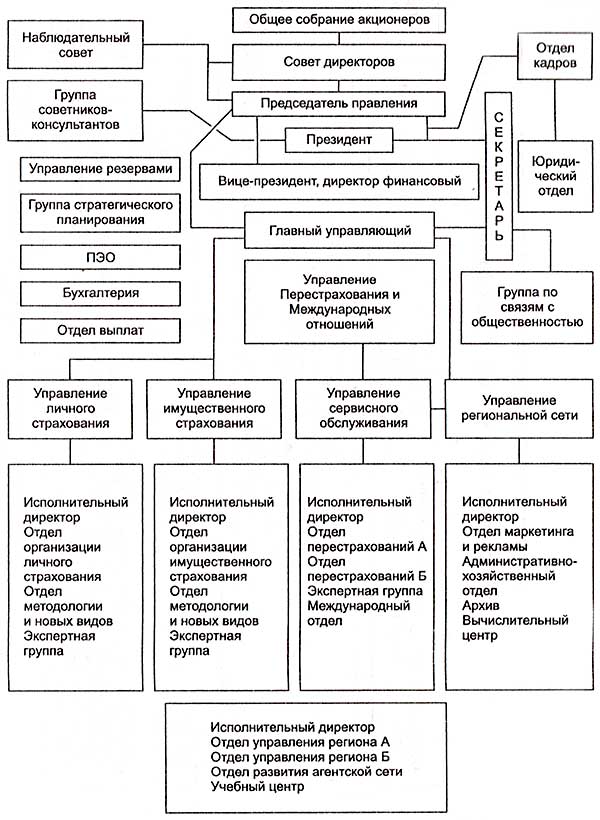


Рисунок 1.1 – Структура страховой компании

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

Субъект – это 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).

# Субъекты информационных отношений

Не менее важным направлением разработки политики информационной безопасности является анализ, характеристика и разработка мер защиты субъектов информационной системы. Далее описаны субъекты, существующие в организации страховой компании:

* сотрудники организации, являющиеся пользователями технологического оборудования, имеющие доступ к информации, размещенной в носителях на магнитной и оптической основе;
* сотрудники отделов и управлений, анализирующие данные в массивах и базах данных;
* пользователи услуг страховой компании, имеющие доступ к информационным ресурсам посредством электронных изданий;
* процессы передачи информации по каналам связи.

# Основные угрозы и их источники

Самой главной целью разработки политики информационной безопасности является классификация всех возможных типов потенциальных угроз, а также оценка рисков реализации данных угроз. На основании этих данных разрабатываются средства и методы для эффективного управления информационной безопасностью в страховой компании.

Угрозы безопасности могут быть внешнего и внутреннего, искусственного и естественного, а также преднамеренного и непреднамеренного происхождения. Самыми частыми целями преступных посягательств в страховых компаниях являются базы данных, содержащие информацию о номерах телефонов, автомобилей, медицинских историях.

Кроме того, не исключен риск заражения компьютерных систем компании различными вирусами, которые могут причинить существенный ущерб в виде блокировки доступа и уничтожения важных файлов и передачи информации третьим лицам.

Далее будут подробнее рассмотрены основные типы, по которым можно классифицировать потенциальные угрозы.

# Внутренние угрозы

Внутренние дестабилизирующие факторы влияют:

На программные средства (ПС):

* некорректный исходный алгоритм;
* неправильно запрограммированный исходный алгоритм.

На аппаратные средства (АС):

* системные ошибки при постановке задачи проектирования;
* отклонения от технологии изготовления комплектующих изделий и аппаратных средств в целом;
* нарушение режима эксплуатации, вызванное внутренним состоянием АС.

К конкретным внутренним угрозам, которые имеют место в страховой компании, можно отнести:

* нарушения в работе алгоритмов используемых в работе программных средств, а также нарушение эксплуатации используемых аппаратных средств;
* системные ошибки в технологическом оборудовании, которые могут привести к уничтожению критически важных данных;
* внутренние ошибки в клиентских базах данных, которые могут привести к искажению и уничтожению пользовательских данных.

Внутренние угрозы не являются высоковероятными вследствие развития технической аппаратуры, однако, при своей реализации внутренние угрозы могут нанести существенный ущерб для страховой компании.

# Внешние угрозы

Внешние дестабилизирующие факторы влияют:

На программные средства (ПС):

* неквалифицированные пользователи;
* несанкционированный доступ к ПС с целью модификации кода.

На аппаратные средства (АС):

* внешние климатические условия;
* электромагнитные и ионизирующие помехи;
* перебои в электроснабжении;
* недостаточная квалификация обслуживающего персонала.

Рассмотрим конкретные внешние дестабилизирующие факторы, которые имеют риски реализации в страховой компании:

* несанкционированный доступ к базам данных, программным средствам и прочим документам третьими лицами, который может повлечь искажение, потерю и утечку личных данных пользователей и конфиденциальных данных страховой компании;
* несанкционированный доступ к базам данных, программным средствам и прочим документам сотрудниками страховой компании, не имеющих привилегий на доступ к этим данным;
* доступ к данным сотрудниками страховой компании, не обладающих достаточной квалификацией;
* заражения компьютерных систем компании компьютерными вирусами, которые могут причинить ущерб в виде блокировки доступа или уничтожения файлов, а также передачи информации третьим лицам;
* человеческий фактор.

Внешние угрозы являются гораздо более высоковероятными и также могут нанести серьёзный ущерб, поэтому вследствие их высоких рисков они должны классифицироваться в политике информационной безопасности, и требуют разработки методов и средств обеспечения требуемого уровня защищённости информационной системы.

# Естественные угрозы

Потенциальные угрозы также можно классифицировать по природе их возникновения: естественные и искусственные.

Естественные угрозы – это угрозы, вызванные объективными физическими процессами техногенного характера, или стихийными природными явлениями, которые не зависят от деятельности человека.

К естественным угрозам в страховой компании можно отнести внешние климатические условия, перебои в электроснабжении, а также электрические, магнитные, электромагнитные и ионизирующие помехи.

# Искусственные угрозы

Искусственные угрозы отличаются от естественных тем, что они вызваны деятельностью человека. К искусственным угрозам можно отнести следующие вышеописанные потенциальные угрозы:

* несанкционированный доступ к базам данных, программным средствам и прочим документам третьими лицами и сотрудниками страховой компании;
* доступ к базам данных, программным средствам и прочим документам сотрудниками, не обладающими достаточной квалификацией;
* заражения компьютерных систем компании компьютерными вирусами;
* человеческий фактор.

Если сравнивать между собой естественные и искусственные угрозы, то оба типа угроз могут понести серьезный ущерб и убытки компании, однако, ввиду того, что искусственные угрозы являются гораздо более распространёнными и высоковероятными, их риск становится гораздо выше.

# Непреднамеренные угрозы

Помимо вышеперечисленных классификаций потенциальных угроз, угрозы информационной безопасности также можно разделить по степени умысла на преднамеренные и непреднамеренные.

Непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) угрозы – это угрозы, к которым относятся непреднамеренные нарушения правил сбора, обработки и передачи информации, а также случайные нарушения требований безопасности и другие действия сотрудников страховой компании, приводящие к непроизводительным затратам времени и ресурсов, разглашению личной информации клиентов компании или конфиденциальной информации компании, потере важных данных или нарушению работоспособности страховой компании.

Можно сказать, что практически все непреднамеренные угрозы в организациях связаны с человеческим фактором, который не имеет никакого злого умысла и имеет сугубо случайный характер. Также, некоторые случаи возникновения угроз заражения компьютерных систем компании компьютерными вирусами могут относиться к непреднамеренным.

Несмотря на случайность данных угроз, они также должны классифицироваться в политике информационной безопасности, и для данных угроз необходимы средства и методы их предотвращения, снижения вероятности и устранения.

# Преднамеренные угрозы

Преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) угрозы – это угрозы, обусловленные осмысленными корыстными действиями легально допущенных к информации сотрудников страховой компании, приводящие к непроизводительным затратам времени и ресурсов, разглашению личной информации клиентов компании или конфиденциальной информации компании, потере важных данных или нарушению работоспособности страховой компании.

Если рассматривать понятие «человеческий фактор» как все ошибки и неточности, совершаемые людьми ввиду их человеческой природы, такие как, например, уровень стресса или ошибка выжившего, то к данному типу угроз относятся все виды влияния человеческого фактора, которые обусловлены злым умыслом либо некачественным или неквалифицированным исполнением обязанностей.

К преднамеренным угрозам и ошибкам относятся все правонарушения против безопасности, нарушения трудовой дисциплины, конфликты, кражи и т.д. В этих случаях у человека есть вина, мотив, осознание действия и он, как правило, имеет чёткое представление о том, что произойдёт в случае обнаружения его ошибки, или же он точно знает, что его лень, халатность или недопонимание рано или поздно приведут к ошибке.

К преднамеренным угрозам в страховой компании можно отнести:

* удаленный несанкционированный доступ третьих лиц или сотрудников компании к информационным ресурсам страховой компании с целью получения материальной выгоды;
* неправомерный доступ к ресурсам компании ранее уволенными сотрудниками, который может повлечь утечку данных компаниям-конкурентам;
* халатность сотрудников и невыполнение поставленных обязательств;
* физическое неправомерное нарушение целостности средств хранения важных информационных источников техногенного и естественного характера третьими лицами путём взлома, краж, и т.п.