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](#_Toc127089379)

[1. Объекты защиты 5](#_Toc127089380)

[1.1. Описание структуры организации 5](#_Toc127089381)

[1.2. Внутренняя структура организации 5](#_Toc127089382)

[1.3. Обзор объектов и субъектов информационных отношений 8](#_Toc127089383)

[1.3.1. Объекты информационных отношений 8](#_Toc127089384)

[1.3.2. Субъекты информационных отношений 8](#_Toc127089385)

[2. Основные угрозы и их источники 9](#_Toc127089386)

[2.1. Внутренние угрозы 9](#_Toc127089387)

[2.2. Внешние угрозы 10](#_Toc127089388)

[2.3. Естественные угрозы 10](#_Toc127089389)

[2.4. Искусственные угрозы 11](#_Toc127089390)

[2.5. Непреднамеренные угрозы 11](#_Toc127089391)

[2.6. Преднамеренные угрозы 12](#_Toc127089392)

[3. Оценка угроз, рисков и уязвимостей 13](#_Toc127089393)

[3.1. Оценка ущерба организации 13](#_Toc127089394)

[3.2. Оценка вероятности реализации угроз 14](#_Toc127089395)

[3.3. Оценка рисков 14](#_Toc127089396)

[4. Меры, методы и средства обеспечения защищённости ресурсов 16](#_Toc127089397)

# 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.

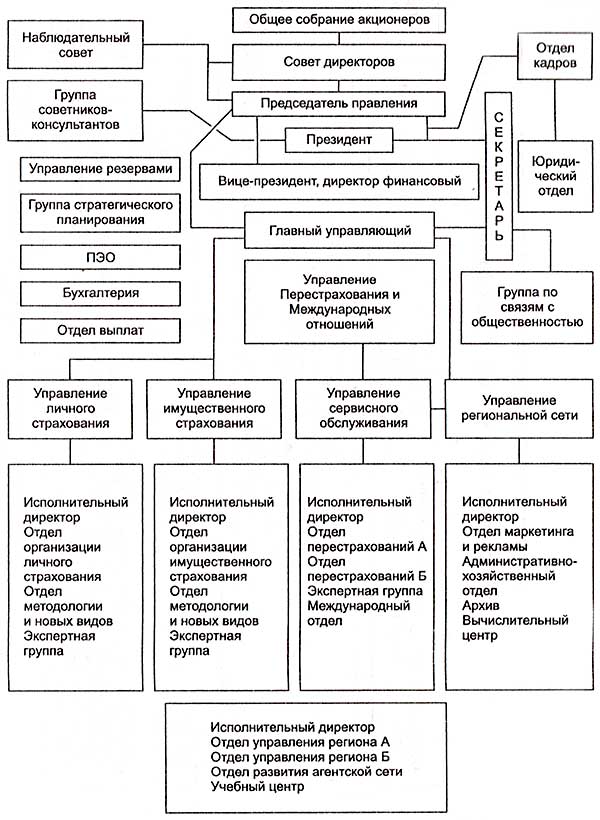


Рисунок 1.1 – Структура страховой компании

# Обзор объектов и субъектов информационных отношений

В данном подразделе 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.

Все непреднамеренные угрозы можно отнести к человеческому фактору. Человеческий фактор – это совокупность характеристик человека, которые свидетельствуют о его надёжности и производительности в определённых ситуациях. На это влияют многие факторы, такие как возраст, душевное состояние, физическое здоровье, эмоции, склонность к определенным распространенным ошибкам, когнитивным заблуждениям и т.д.

В качестве примеров непреднамеренных угроз в страховой компании можно привести:

* профессиональные ошибки сотрудников страховой компании из-за излишней самоуверенности, недостатка знаний или случайностей;
* нарушения целостности и безопасности баз данных, программных средств и прочих информационных средств ввиду случайных ошибок сотрудников;
* непреднамеренные ошибки, нарушения правил эксплуатации, стандартов безопасности, трудовой дисциплины, а также некачественное исполнение обязанностей сотрудников ввиду следующих факторов: психоэмоционального и физического состояния, проблемах в межличностных отношениях, конфликтах на работе и прочих непреднамеренных форс-мажорных обстоятельств.

# 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.

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.

# Оценка угроз, рисков и уязвимостей

Следующим этапом разработки политики информационной безопасности является оценка рисков. Риски можно представить как совокупность двух факторов: произведения ущерба от реализации угрозы и вероятности её реализации.

Также при оценивании рисков учитываются ценность ресурсов, значимость угроз и эффективность существующих и планируемых средств и методов защиты. Ценность ресурсов может определяться количественной или качественной характеристикой, или их комбинацией.

На основании величины рисков определяются наиболее важные и приоритетные угрозы, и на основании того, какие именно угрозы являются самыми рискованными и критически важными, определяются наиболее приоритетные меры, методы и средства защиты информационных ресурсов, а также необходимые средства управления информационной безопасностью.

То есть, для оценки рисков необходимо создать шкалу оценки ущерба страховой компании, вероятностно-временную шкалу реализации угрозы, которые будут рассмотрены далее.

# Оценка ущерба организации

Для оценки возможного ущерба страховой компании от реализации потенциальных угроз составляется таблица численной оценки ущерба организации, где каждой качественной степени ущерба соответствует целочисленное значение от 0 до 5. Благодаря численному ранжированию величины ущерба возможно просчитать риски на каждый тип потенциальной угрозы. Численные оценки ущерба организации представлены в таблице 3.1.

Таблица 3.1 – Численная шкала оценки ущерба страховой компании

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие данных принесет ничтожно малый моральный и экономический ущерб страховой компании |
| 1 | Ущерб от атаки есть, но он незначителен, и положение страховой компании на рынке не затронуто |
| 2 | Финансовые операции не ведутся в течение некоторого времени, страховая компания терпит убытки, но её положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери финансов и доверия со стороны клиентов, ощутимая часть которых уходит |
| 4 | Потери очень значительные, страховая компания на период до года теряет свое положение на рынке. Для восстановления положения потребуются крупные финансовые займы |
| 5 | Страховая компания прекращает существование |

# Оценка вероятности реализации угроз

Кроме того, чтобы оценить величину ущерба от реализации каждой потенциальной угрозы информационной безопасности страховой компании, необходимо также учитывать вероятность того, что данная угроза вообще будет реализована. Эта вероятность обусловлена следующими факторами:

* привлекательность информационных ресурсов для злоумышленников: клиентские базы данных, документы с личной информацией пользователей и сотрудников, финансовые отчётности, номера страховых полисов и прочая информация;
* возможность использования информационного ресурса в целях получения прибыли;
* степень лёгкости, с которой угроза может быть использована;
* надёжность и безопасность существующих и планируемых систем защиты информации.

Численная классификация вероятностей реализаций различных потенциальных угроз представлена в таблице 3.2.

Таблица 3.2 – Вероятностно-временная шкала реализации угроз

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события |
| 0 | Данный вид угрозы отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

После описания численных оценок степени ущерба страховой компании и вероятности реализации потенциальных угроз, возможно на основании этих данных оценить риски для каждой вышеописанной потенциальной угрозы. Оценка рисков будет представлена в следующем подразделе.

# Оценка рисков

На основании таблиц 3.1 и 3.2 можно составить таблицу рисков. На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем. В качестве максимального допустимого уровня риска положим 1, а максимальный интегральный (суммарный) уровень риска примем равным 4.

Далее в каждой строке таблицы проверяется, превышает ли данная угроза предельно допустимый уровень риска или нет. Если такое превышение имеет место, данная угроза должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности.

Оценка рисков представлена в таблице 3.3.

Таблица 3.3 – Оценка рисков страховой компании

|  |  |  |  |
| --- | --- | --- | --- |
| Описание угрозы | Ущерб | Вероятность | Риск (Ущерб × Вероятность) |
| нарушения в работе алгоритмов рабочих программных средств | 1 | 0,1 | 0,1 |
| системные ошибки в техническом оборудовании | 1 | 0,1 | 0,1 |
| внутренние ошибки в клиентских базах данных | 3 | 0,2 | 0,6 |
| НСД хакеров и группировок хакеров к личным данным клиентов страховой компании | 4 | 0,1 | 0,4 |
| НСД и копирование личных данных клиентов сотрудниками страховой компании | 4 | 0,2 | 0,8 |
| доступ к данным сотрудниками страховой компании, не обладающих достаточной квалификацией | 1 | 0,4 | 0,4 |
| заражения компьютерных систем страховой компании компьютерными вирусами | 2 | 0,4 | 0,8 |
| непреднамеренные ошибки сотрудников по причине человеческого фактора | 1 | 0,5 | 0,5 |
| перебои в работе электричества, обеспечивающего функционирование баз данных | 4 | 0,2 | 0,8 |
| проникновение на рабочее место лиц, не являющихся сотрудниками страховой компании | 3 | 0,2 | 0,6 |
| **Итого** | 24 | **2,4** | **5,1** |

Исходя из данных таблицы оценки рисков, риски каждой угрозы не превышают предельных допустимых значений (1), однако суммарный риск от всех угроз превышает максимальное допустимое значение – 4.

Следовательно, в системе безопасности набирается множество небольших угроз, которые необходимо решать комплексно. В этом случае выбираются угрозы с наибольшим уровнем риска (0,8), и работа по снижению вероятности или устранению этих угроз является наиболее приоритетной в разработке политики информационной безопасности.

# Меры, методы и средства обеспечения защищённости ресурсов