МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Проект политики информационной безопасности страховой компании»**

Студент:

Кравцова Диана Вячеславовна

Вариант 7

Преподаватель:

Блинова Евгения Александровна

Минск 2021

# 

# **Введение**

Страховые компании, как и любые другие хозяйствующие субъекты, нуждаются в защите своей конфиденциальной информации. В связи с развитием информационных технологий, обслуживающих все управленческие процессы страховых компаний, всё более разнообразными и сложными становятся угрозы и атаки, способные нанести огромный материальный и моральный ущерб. Поэтому страховые компании должны обеспечивать безопасность обрабатываемых персональных данных своих клиентов, в связи с тем, что их услуги в большой степени являются персонализированными и оказываются индивидуально, а также информацию, которую страховщики используют для достижения уставных целей, ради которых они созданы. Её разглашение или утечка лишит возможности реализовать данные цели. Для того, чтобы сохранить доверие клиентов, необходимо обеспечить сохранение коммерческой тайны. Для оптимального решения этой задачи необходимо разработать политику информационной безопасности страховой компании, которой неукоснительно должны следовать все его служащие.

## **Объекты защиты**

Основными объектами системы информационной безопасности в страховой компании являются:

* коммерческая тайна самой страховой компании, данные о ее договорах, финансовых взаимоотношениях, бухгалтерская информация;
* коммерческая тайна клиентов и партнеров организации, данные об их активах, имуществе, платежах, произошедших страховых событиях;
* персональные данные сотрудников компании и сотрудников клиентов, эта информация иногда включает номера автомобилей, водительских удостоверений, кредитных карт;
* медицинская тайна клиентов компании, пользующихся услугами добровольного медицинского страхования.

Эти данные могут стать объектом противоправного покушения, их сохранность требует принятия серьезных мер безопасности. Несанкционированный доступ к охраняемым законом сведениям является уголовным преступлением, предусмотренным статьей 349 Уголовного кодекса РБ.

## **1.2 Структура страховой компании**

Информационная среда страховой компании является распределенной структурой, объединяющей информационные подсистемы главного офиса, филиалов и представителей, закрепленных за филиалами.

Главный офис осуществляет следующие функции:

* выполняет процедуры (получает лицензии, регистрирует и т. п.), необходимые для осуществления страхования, перестрахования, инвестиционной и иной деятельности, связанной со страхованием;
* определяет единую стратегию предприятия, задачи и пути их эффективного решения, осуществляет стратегическое, тактическое и оперативное планирование;
* изучает состояние и тенденции страхового рынка, разрабатывает на основе этих исследований страховые программы и продукты, правила (условия) страхования, определяет стратегию маркетинга;
* разрабатывает и реализует единую политику в сфере управления предприятием, формирует системы его управления, организационные структуры и штаты, осуществляет методическое руководство обособленными подразделениями, организует, координирует и контролирует их деятельность по реализации стратегических задач, определяет методы и тактические приёмы работы на страховом рынке;
* осуществляет постановку и ведение бухгалтерского учёта, формирует единую учётную политику;
* разрабатывает Бизнес-план, организует и контролирует его выполнение, обеспечивает соблюдение планово-финансовой дисциплины, осуществляет уплату налогов и других обязательных платежей в бюджет и внебюджетные фонды, распределение прибыли, проводит анализ страховой и финансово-хозяйственной деятельности;
* осуществляет расчёт страховых тарифов, определяет технологию проведения страховых операций, разрабатывает инструкции, методические рекомендации, иные локальные нормативные правовые акты.

К основным функциям филиалов относятся:

* организует и осуществляет страхование, страховое посредничество, оценку страховых рисков, оказание консультационных услуг, иную деятельность, связанную со страхованием;
* взаимодействует с местными исполнительными и распорядительными органами по вопросам, связанным с деятельностью представительства;
* осуществляет в порядке, установленном главным офисом, оперативное планирование страховой деятельности;
* ведёт бухгалтерский учёт, формирует полную и достоверную информацию о деятельности филиала и представительств, составляет и своевременно предоставляет полную и достоверную бухгалтерскую, статистическую и налоговую отчётность.

Представители филиалов работают под его непосредственным руководством и подотчётно ему. Основные функции представителей:

* изучает потребности страхователей, состояние страхового рынка;
* осуществляет на территории района и (или) города в порядке, предусмотренным филиалом, страхование по видам страхования, на которые филиалом получены лицензии, страховое посредничество, оценку страховых рисков и убытков и иную деятельность, связанную со страхованием;
* организует работу страховых агентов;
* обеспечивает соблюдение требований о страховой и финансово-хозяйственной деятельности.

К основным особенностям информационной среды страховой компании относятся:

* широкая территориальная распределенность компонентов информационной системы (главный офис и филиалы);
* значительное расширение сферы использования автоматизированных систем обработки информации;
* абстрагирование владельцев данных от физических структур и места размещения данных (информации);
* наличие большого числа информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации) (сеть Интернет и другие специализированные компьютерные сети);

## **1.3 Угрозы безопасности информации и их источники**

Угроза безопасности - потенциальное нарушение безопасности, любое обстоятельство или событие, которое может явиться причиной нанесения ущерба предприятию в целом.

Перечень угроз безопасности включает атаки как внешнего, так и внутреннего происхождения. Информационные базы данных, принадлежащие страховым компаниям, часто становятся объектами покушений хакеров. Частыми целями преступных посягательств являются клиентские базы данных, содержащие информацию о номерах телефонов, номерах автомобилей, медицинских историях. В ряде случаев мошенники, используя данные, похищенные у страховщиков, создавали сайты-клоны.

Кроме того, не исключен риск заражения компьютерных систем компании различными вирусами, которые могут причинить существенный ущерб в виде:

* блокировки доступа к важным файлам;
* уничтожения файлов;
* передачи информации третьим лицам.

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на предприятие объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы – это угрозы предприятию, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

* непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
* преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к предприятию могут быть внешними или внутренними (составляющие самой организации - её аппаратура, программы, персонал, конечные пользователи).

Основными источниками угроз безопасности информации страховой компании являются:

* неумышленные действия, приводящие к частичному или полному отказу системы, или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
* преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия сотрудников филиалов страховой компании, отвечающих за обслуживание и администрирование программного и аппаратного обеспечения, средств защиты и обеспечения ИБ;
* деятельность преступных групп, экономических структур, а также отдельных лиц по добыванию и/или искажению информации, нарушению работоспособности системы в целом или ее отдельных компонентов;
* неумышленная порча носителей информации;
* запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
* вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
* некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

Наиболее значимыми угрозами безопасности информации страховой компании (способами нанесения ущерба субъектам информационных отношений) являются:

* нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов страховой компании, а также фальсификация (подделка) документов;
* разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
* отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

Пользователи, операторы и другие сотрудники страховой компании являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций, регламентов и порядков.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

## **1.4 Разработка мер защиты**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Атака | Меры защиты | Ущерб | Вероятность | Риск |
| Кражи, нападения, взлом, саботаж и проникновение | Наличие охраны;  Наличие системы видеонаблюдения;  Наличие пропускной системы с удостоверением личности для рабочего персонала. | 4 | 0,1 | 0,4 |
| Отказы и неисправности технических средств | Наличие отдела, отвечающего за ремонт технических средств | 1 | 0,3 | 0,3 |
| Фарминг | Использовать и регулярно обновлять лицензионное антивирусное программное обеспечение;  Использовать защиту электронного почтового ящика (отключить предварительный просмотр);  Не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов. | 1 | 0,2 | 0,2 |
| Mailbombing | Давать адрес электронной почты только проверенным источникам; В качестве преграды для mailbombing-а может выступать и Web-сайт провайдера, иногда настраиваемый таким образом, чтобы он автоматически определял почтовые атаки. Если количество сообщений из одного источника превышает некие разумные пределы, то все они автоматически поступают в Recycle Bin на сервере. | 2 | 0,3 | 0,6 |
| Анализатор трафика | Аутентификация - cильные средства аутентификации являются первым способом защиты от сниффинга пакетов. Под "сильным" мы понимаем такой метод аутентификации, который трудно обойти. Примером такой аутентификации являются однократные пароли (OTP - One-Time Passwords);  Коммутируемая инфраструктура - еще одним способом борьбы со сниффингом является создание коммутируемой инфраструктуры. Если, к примеру, во всей организации используется коммутируемый Ethernet, хакеры могут получить доступ только к трафику, поступающему на тот порт, к которому они подключены. Коммутируемая инфраструктуры не ликвидирует угрозу сниффинга, но заметно снижает ее остроту;  Антиснифферы как ещё один способ борьбы со сниффингом, который заключается в установке аппаратных или программных средств, распознающих снифферы, работающие в Вашей сети. Эти средства не могут полностью ликвидировать угрозу, но, как и многие другие средства сетевой безопасности, они включаются в общую систему защиты.  Криптография - самый эффективный способ борьбы со сниффингом пакетов хотя и не предотвращает перехвата и не распознает работу снифферов, но делает эту работу бесполезной. | 4 | 0,3 | 1.2 |
| IP-спуфинг | Угрозу спуфинга можно ослабить с помощью:  контроля доступа. Чтобы снизить эффективность IP-спуфинга, настройте контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри вашей сети;  фильтрации RFC 2827. Вы можете пресечь попытки спуфинга чужих сетей пользователями вашей сети. Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов вашей организации. | 4 | 0,3 | 1.2 |
| Переполнение буфера | Корректировка исходных кодов программы для устранения уязвимостей. Переполнение буфера происходит, прежде всего, из-за неправильного алгоритма работы программы, который не предусматривает проверок выхода за границы буферов. Также возможно применение специальных утилит автоматического поиска уязвимостей в исходном коде программы.  Использование неисполнимых буферов. Суть метода заключается в запрещении исполнения кода в сегментах данных и стека, т.е. параметры сегментов данных и стека содержат только атрибуты записи и чтения, но не исполнения. Применение проверок выхода за границы. В основе данного метода лежит выполнение проверок выхода за границы переменной при каждом обращении к ней. Это предотвращает все возможные атаки по переполнению буфера, так как полностью исключает само переполнение.  Применение проверок целостности. Решение, получено благодаря проекту Synthetix. Цель Synthetix - специализация кода для увеличения производительности операционных систем. При этом вводится понятие так называемого квази-постоянства (Quasi-invariant), т.е. состояния среды, которое неизменно в определенных рамках. Такое квази-постоянство позволяет устранить ряд избыточного кода проверки выполнения различных условий. | 2 | 0,2 | 0,4 |
| Отказ в обслуживании (Denial of Service - DoS) | Функции анти-спуфинга - правильная конфигурация функций анти-спуфинга на ваших маршрутизаторах и межсетевых экранах поможет снизить риск DoS. Эти функции, как минимум, должны включать фильтрацию RFC 2827. Если хакер не сможет замаскировать свою истинную личность, он вряд ли решится провести атаку. Функции анти-DoS - правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени. | 2 | 0,3 | 0,6 |
| Атака типа man-in-the-middle. | Использование шифрования данных | 4 | 0,3 | 1.2 |
| Фишинг | Использовать только проверенные ресурсы и пути доступа к ним;  Использовать антивирусные средства и регулярно обновлять их сигнатуры. | 4 | 0.3 | 1.2 |
| Парольные атаки | Одноразовые пароли;  Криптографическая аутентификация. | 4 | 0.3 | 1.2 |
| Атаки на уровне приложений | Необходимо читать лог – файлы операционных систем и сетевые лог – файлы и/или анализируйте их с помощью специальных приложений;  Пользоваться самыми свежими версиями ОС и приложений и самыми последними коррекционными модулями (патчами); | 4 | 0.2 | 0.8 |

## **1.5 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

Все меры обеспечения безопасности информационной системы страховой компании подразделяются на:

* правовые (законодательные);
* морально-этические;
* технологические;
* организационные (административные);
* физические;
* технические (аппаратурные и программные).

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы страховой компании.

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или страховой компании в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

К технологическим мерам защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений и т.п.

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

### **1.5.1 Формирование политики безопасности**

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности информации в страховой компании целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность страховой компании в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила:

* каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности информации;
* кто имеет права доступа к информации ограниченного распространения, кто и при каких условиях может читать и модифицировать информацию и т.д.;

### **1.5.2 Регламентация допуска сотрудников к использованию информационных ресурсов**

В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационной системой страховой компании и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком, согласно, регламента предоставления доступа пользователей.

Основными пользователями информации в информационной системе являются сотрудники филиалов страховой компании. Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

* каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с сотрудниками, ответственным за информационное сопровождение данного ресурса;
* начальник имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;
* наиболее ответственные технологические операции должны производиться по правилу «в две руки» - правильность введенной информации подтверждается другим должностным лицом, не имеющим права ввода информации.

Все сотрудники страховой компании, зарегистрированные как легальные пользователи информационной системы страховой компании и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению служебной и коммерческой тайны, а также правил работы с информацией в страховой компании.

Обработка информации в компонентах информационной системы страховой компании должна производиться в соответствии с утвержденными технологическими инструкциями.

### **1.5.3 Подбор и подготовка персонала, обучение пользователей**

Пользователи информационной системы страховой компании, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в страховой компании.

Обеспечение безопасности информации возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами страховой компании. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационной системы страховой компании, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационной системы страховой компании должны быть ознакомлены с организационно - распорядительными документами по обеспечению информационной безопасности страховой компании, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под подпись.

### **1.5.4 Подразделение обеспечения информационной безопасности**

Основные меры обеспечения информационной безопасности заключаются в следующем:

* формирование требований к системам защиты в процессе создания и дальнейшего развития существующих компонентов информационной системы страховой компании;
* подготовка решений по обеспечению конфиденциальности, доступности, целостности данных;
* обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;
* генерация и распределение между пользователями необходимых атрибутов доступа к ресурсам информационной системы страховой компании;
* наблюдение за функционированием системы защиты и ее элементов;
* проверка надежности функционирования системы защиты;
* разработка мер нейтрализации моделей возможных атак;
* обучение пользователей и обслуживающего персонала правилам безопасной обработки информации;
* контроль за действиями администраторов баз данных, серверов и сетевых устройств;
* контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с информацией;
* организация по указанию руководства служебного расследования по фактам нарушения правил обращения с информацией и оборудованием;
* принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;
* cбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.