МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

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

Студент:

Миневич Кристина Викторовна

Вариант 7

Минск 2023

**Содержание**

[Введение 3](#_Toc32925631)

[1 Объекты защиты 4](#_Toc32925632)

[2 Структура страхового агентства 4](#_Toc32925633)

[3 Виды угроз 5](#_Toc32925634)

[4 Разработка мер защиты 8](#_Toc32925635)

[5 Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов 11](#_Toc32925636)

[Вывод 14](#_Toc32925637)

# Введение

Страховые компании оказывают услуги в сфере страховой защиты имущественных интересов юридических и физических лиц. В процессе деятельности они становятся обладателями большого объема информации, носящей характер коммерческой тайны или же персональных данных. И то, и другое защищено законом. Распространение этих сведений среди широкого круга лиц может привести к финансовому ущербу для компании и ее клиентов. Поэтому специалисты службы безопасности страховых компаний обязаны прилагать значительные усилия в области защиты информации.

Исследование проблемы информационной безопасности становится наиболее актуальным с течением времени, т.к. развиваются и появляются новые страховые агентства, преумножается количество клиентов, пользующихся предоставляемыми услугами. Любое несанкционированное вмешательство может повредить работу системы, вплоть до невозможности ее функционирования, что неизбежно повлечет за собой финансовые убытки для компании.

Защита документооборота и баз данных хранящих практически всю информацию о клиентах и сотрудниках является сложной, но обязательной задачей, без решения которой невозможно нормальное функционирование страхового агентства.

## 1 Объекты защиты

Статус информации как объекта правовой защиты регулируется законами. Среди них закон «Об информации, информационных технологиях и защите информации», Гражданский кодекс, закон «О защите персональных данных» и другие.

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.

## 2 Структура страхового агентства

Администратор – управляющий компанией, взаимодействует с клиентами.

Отдел кадров – совокупность специализированных подразделений в структуре компании, призванных управлять персоналом.

Плановый отдел – осуществляет:

* формирование ценовой и экономической политики, службы безопасности на основании действующих нормативных актов;
* формирование финансового плана (бизнес-плана) развития компании, контроль за ходом его выполнения, организацию ведения государственной статистической отчетности компании, связанной с экономическими показателями развития;
* проведение экономического анализа финансовой деятельности компании;
* анализ состава затрат при формировании цен на услуги компании;
* контроль соблюдения государственной финансовой дисциплины при заключении договоров и осуществлении экономической деятельности компании;
* внутренний финансовый контроль за правильностью применения цен (тарифов) на услуги, оказываемые компанией.

Бухгалтерия – штатно-структурное подразделение компании, предназначенное для аккумулирования данных о её имуществе и обязательствах.

Отдел операторов – отдел компании, занимающийся взаимодействием с клиентом.

Отдел оказание юридических услуг – основной отдел компании.

К основным особенностям информационной среды страховой компании относятся:

* широкая территориальная распределённость 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).

## 3 Виды угроз

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.

Не всегда установленный антивирус будет надежной защитой от спланированной атаки. Кроме внешней угрозы проникновения в компьютерные сети страховой компании существуют и внутренние. Отдельные сотрудники могут намеренно похищать коммерческую информацию с целью ее распространения или передачи конкурентам.

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).

Основные непреднамеренные искусственные угрозы предприятию (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

* 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.);
* неправомерное отключение оборудования или изменение режимов работы устройств и программ;
* 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.);
* нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
* заражение компьютера вирусами;
* неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
* разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
* проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
* игнорирование организационных ограничений (установленных правил) при работе в системе;
* 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;
* пересылка данных по ошибочному адресу абонента (устройства);
* ввод ошибочных данных;
* неумышленное повреждение каналов связи.

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

* физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
* отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
* внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
* вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
* применение подслушивающих устройств, дистанционная фото- и видеосъемка, и т.п.;
* перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сели питания, отопления 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;
* хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);
* несанкционированное копирование носителей информации;
* хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
* чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
* чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой зашиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;
* незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
* несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
* вскрытие шифров криптозащиты информации;
* внедрение аппаратных «спецвложений», программных «закладок» и «вирусов» («троянских коней» и «жучков»), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
* незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
* незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

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

## 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 |
| Снифферы пакетов | 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 |

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

Стандарты защиты информации предусмотрены ГОСТами. Кроме того, информационная безопасность страховой компании должна обеспечиваться целым комплексом мер, среди которых:

* административные;
* организационные;
* технические.

Все они должны применяться совместно. Опираться система защиты должна на управление персоналом компании и контроль над ним. Меры технического характера не менее важны, но не могут существовать в отрыве от организационных мер.

Административные меры безопасности.

Эти способы защиты включают в себя разработку внутренних нормативных документов, обеспечивающих информирование сотрудников о системе действий, необходимых для обеспечения информационной безопасности. Такие документы хранятся в открытом доступе, в страховой компании должно быть организовано ознакомление с ними персонала.

Служба безопасности страховой компании разрабатывает и предлагает на утверждение руководства политику защиты конфиденциальной информации. Этот локальный нормативный акт должен содержать:

* основные принципы защиты конфиденциальной информации в компании;
* обязанности каждого сотрудника в части защиты доверенных ему сведений;
* задачи руководства по обеспечению охраны информации;
* регламенты обращения с компьютерной техникой и средствами коммуникации;
* меры ответственности за нарушение положений документа.

Кроме того, приложением ко всем трудовым договорам должен стать перечень информации, носящей характер коммерческой, а в самих договорах должны быть предусмотрены меры ответственности за ее разглашение.

Организационные меры безопасности.

В большей степени они направлены на устранение внутренней угрозы утечки информации и мотивацию сотрудников на соблюдение утвержденных регламентов. Эти меры предпринимаются службой безопасности во взаимодействии с сотрудниками служб управления персоналом.

В числе организационных мер обеспечения информационной безопасности можно назвать следующие:

* установление различных степеней допуска сотрудников к сведениям, содержащим коммерческую тайну;
* ограничение круга лиц, имеющих допуск к конфиденциальной информации страховой компании;
* организация порядка использования материальных носителей, установление контроля над копированием и сканированием документов, ограничение доступа сотрудников к внешней электронной почте;
* проведение периодических проверок соблюдения регламентов;
* привлечение специалистов для проведения тренингов по защите информации;
* проведение мероприятий по созданию режима коммерческой тайны;
* внесение в договоры компании с клиентами норм, касающихся обязательств соблюдения последними режима коммерческой тайны в отношении переданной им информации;
* привлечение к ответственности лиц, виновных в разглашении информации.

Иногда система работы с безопасностью информации требует создания в компании специального подразделения, в чьи функции будет входить только эта деятельность.

Также следует учитывать, что при проектировании большинства информационных систем уровень защиты от внешнего проникновения был значительно ниже, чем необходим в настоящее время. Среди организационных мер может быть и их аудит, который установит соответствие современным стандартам.

Существуют дополнительные меры организационного характера, позволяющие снизить потери от утечек информации. Уже несколько лет сами страховщики реализуют такой продукт, как страхование от угроз информационной безопасности. Он достаточно популярен. Применение этого способа защиты поможет минимизировать ущерб в случае распространения коммерческой тайны.

Технические меры.

Эта группа мер рассчитана на использование действенных технических средств защиты. Для ее реализации используются аппаратные, программные и криптографические средства.

Первые предполагают установку систем резервного копирования и защиту от несанкционированного проникновения, вторые отвечают за работу антивирусов и иных защитных программ, третьи обеспечивают шифрование всей хранимой и передаваемой по каналам связи информации. Наиболее часто для защиты информации применяются межсетевые экраны и системы обнаружения вторжений. Технические средства требуют постоянного обновления и модернизации, так как скорость устаревания программных продуктов очень высока. Сегодня предлагаются программы, которые обеспечивают комплексные меры по защите информации, это DLP-системы и SIEM-системы. Первые предотвращают утечку данных при их передаче по каналам электронной почты, с использованием мессенджеров или при передаче на принтер. Если программа зафиксирует преобразование информации в момент ее передачи, что может означать ее перехват, она прекращает ее направление на внешние каналы. SIEM-системы представляют из себя комплексные средства управления безопасности, они определяют все уязвимые места системы и предоставляют информацию обо всех возможных угрозах, выявляя паттерны, отличные от стандартного поведения самой системы и ее пользователей.

С каждым днем мошенники разрабатывают новые средства преодоления защитных барьеров, и степень опасности утраты ценных сведений растет, а вместе с ней и риск возможных финансовых потерь. Минимизировать риски можно, пройдя аудит своих систем защиты и получив рекомендации по их модернизации.

Основой защиты технического уровня являются следующие

механизмы безопасности:

* идентификация и аутентификация пользователей;
* управление доступом;
* протоколирование и аудит;
* криптография;
* экранирование;
* обеспечение высокой доступности и т.д.

Таким образом, политика информационной безопасности должна рассматриваться как система, как комплекс инструментов по защите информации.

Комплексное применение современных технических средств в работе службы безопасности страховой компании может обеспечить высокий уровень защиты информации от утечек и несанкционированного доступа. Следует учитывать, что все предпринимаемые действия должны в полной мере соответствовать требованиям белорусского законодательства.

# Вывод

Опыт показывает, что для достижения удачных решений по защите информации необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.