

Разработка политики информационной безопасности страховой компании

Лабораторная работа №1

Студент: Агапкина Д.С
Вариант 7
Преподаватель: Блинова Е.А

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. Распространение этих сведений среди широкого круга лиц может привести к финансовому ущербу для компании и ее клиентов.

Объекты защиты

1

коммерческая
тайна самой
страховой
компании

2

коммерческая
тайна клиентов
и партнеров
организации

3

персональные
данные сотрудников
компании и
сотрудников
клиентов

4

медицинская тайна
клиентов компании,
пользующихся услугами
добровольного
медицинского страхования

1
Администратор

6
Отдел оказания
юридических услуг

2
Отдел кадров

5
Отдел операторов

3
Плановый отдел

4
Бухгалтерия

Страховая компания

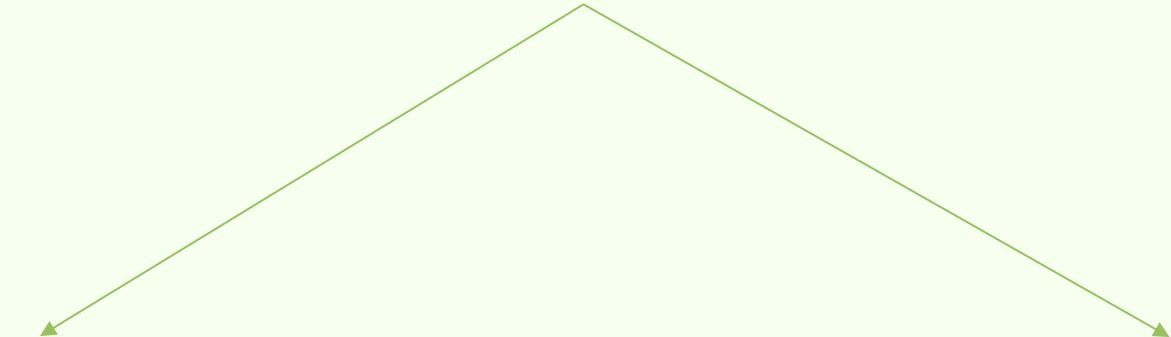
Виды угроз

Естественные
(объективные)

Искусственные
(субъективные)

Непреднамеренные
(неумышленные)

Преднамеренные
(умышленные)



Разработка мер защиты

Атака	Меры защиты	Ущерб	Вероятность	Риск
Кражи, нападения, взлом, саботаж и проникновение	Наличие охраны, системы видеонаблюдения, 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 антивирусное программное обеспечение, использовать защиту электронного почтового ящика, 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	2	0.3	0.6
Снифферы пакетов	Аутентификация, коммутируемая инфраструктура, антиснифферы, криптография	4	0.3	1.2
IP-спуфинг	Настройте контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри вашей сети	4	0.3	1.2
Переполнение буфера	Корректировка исходных кодов программы, применение проверок выхода за границы, применение проверок целостности	2	0.2	0.4
Отказ в обслуживании (Denial of Service - DoS)	Правильная конфигурация функций анти-спуфинга и анти-DoS	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 анализировать их с помощью специальных приложений, пользоваться самыми свежими версиями ОС и приложений	4	0.2	1.8

Меры безопасности

Административные

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

Организационные

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. Среди организационных мер может быть и их аудит. Существуют дополнительные меры организационного характера -> уже несколько лет сами страховщики реализуют страхование от угроз информационной безопасности.

Технические

Они рассчитаны 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.

Вывод

1

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).

2

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 -> задача обеспечения надлежащей надёжности технических средств