Интернет можно по праву назвать главным символом 21-го века. Глобальная Сеть стала Всемирной, не только охватив своей паутиной все континенты и страны, но и проникнув в каждую сферу жизни. Через Интернет решаются вопросы, начиная от заказа пиццы в ближайшем кафе, заканчивая многомиллионными сделками.

Такая территория очень быстро стала привлекать мошенников. Поэтому встаёт вопрос об информационной безопасности.

Определение информационной безопасности

**Информационная безопасность**– это набор технологий, стандартов и административных практик, необходимых для защиты данных.

Другими словами, информационная безопасность представляет собой сохранение, защиту информации и ее наиболее важных элементов, включая системы и устройства, которые позволяют использовать, хранить и передавать эту информацию.

Угрозы безопасности информационных систем

Возможные дыры в информационной безопасности могут возникнуть с двух направлений:

Внешняя угроза

* **Люди.** Доступ к конфиденциальным данным случайно или преднамеренно получают пользователи внешней сети. Это могут быть и сотрудники компании, и злоумышленники.
* **Форс-мажорные обстоятельства.** Например, стихийные бедствия.

Внутренняя угроза

* **Технические факторы.** Из-за ошибки программирования может произойти сбой оборудовании или отключение электроснабжения, оставляет возможность проникновения в сеть.

Риски при использовании незащищенного интернета

Конфиденциальными данными можно распорядиться по-разному:

* **Кража информации.**
	+ Украсть для корыстных целей– к примеру, для последующей перепродажи.
	+ Конфиденциальная информация может быть использована для шантажа или вымогательства (вирус «Петя»).
* **Подмена информации**, как в хранилище, так и непосредственно при её передаче.
* **Программы-шпионы**, которые отслеживают ваши действия на компьютере.
* **Фишинговые письма**, которые позволяют мошенникам украсть личные персональные данные.
* **Присвоение авторства** также встречается часто, когда злоумышленник, взломав электронную почту, начинает рассылать сообщения от имени взломанного пользователя.
* **Разглашение информации**, которая составляет личную или коммерческую тайну. Такое часто встречается при попытке отомстить, испортить репутацию.
* И, наконец, важные, необходимые вам данные могут быть просто **удалены окончательно**.

Как мы видим, риски для ведения бизнеса значительны. Бизнес сам по себе подразумевает высокий риск. Но те угрозы, которые можно устранить, нужно устранить, пока они не пустили на дно до этого уверенно идущий в водах предпринимательства флагман.

Кому необходима защита информации



Защита информации

Если кратко отвечать на этот вопрос, то всем.

В случае с юр. лицами (фирмами и компаниями) защита крайне необходима. Успешная компания всегда на виду, и масштаб трагедии при потере данных идет на сотни миллионов.

Физическим лицам также требуется защищать свою информацию. Получение конфиденциальных данных может вылиться в проблемы. Варианты ущерба различны: от потери репутации до получения чужих кредитов.

Основные методы и средства защиты информации в Сети

В крупных компаниях есть специальный отдел, который занимается техническим обслуживанием аппаратуры, защитой от внешнего проникновения.

Средний же и малый бизнес обычно обращается за помощью к профессионалам либо покупает уже готовый, специально для них разработанный продукт.

Можно выделить такие средства защиты:

1. Программные и технические.
2. Административные и законодательные.
3. Смешанные.

Разумеется, третий вариант предпочтительнее, так как он комплексно включает в себя составляющие из первых двух.

**Программные средства защиты**

* Использование антивирусов. В их задачу входит нахождение, удаление либо же изоляция программ, которые определяются, как вредоносные.
* Применение «песочниц». Это инструменты для работы с сомнительными приложениями в виртуальном пространстве.
* Использование брандмауэров. Такие программы предназначены для слежения за траффиком. В их задачу входит сообщить, если на компьютер начинают поступать непонятные сигналы из непроверенных источников.
* Применение DLP- и SIEM-систем. Это внутренняя защита от недобросовестных сотрудников. В первом случае программа не даёт копировать информацию на сторонние носители, например, флэшку; вторая отслеживает запросы к базе данных и сообщает, если считает ситуацию подозрительной. Например, запросы не типичные или слишком частые.

Методы защиты информации в интернете

Это только основные типы существующих на сегодняшний день программных средств защиты. На самом деле их гораздо больше, они возникают ежегодно, как и новые угрозы. IT-сфера развивается очень динамично.

**Административные средства защиты**

1. Проведение инструктажа среди сотрудников. Необходимо создать свод правил, нарушение которых ведет к штрафу.
2. Составление официальных договоров о неразглашении. Сотрудники должны понимать, что на них лежит большая ответственность.
3. Создание системы степеней доступа. Каждый работник должен иметь собственный аккаунт и пароль. Доступ к конфиденциальной информации должны иметь только те, кому она совершенно необходима для работы. Современное ПО позволяет со 100%-й вероятностью вычислить, с какого конкретно компьютера произошёл взлом или утечка информации.
4. Оптимизация работы отдела кадров. На этапе собеседования стоит качественно отбирать сотрудников.

Кроме того, существуют **аппаратные методы и средства защиты информации** в Интернете. Они представляют собой переходный этап между программными и физическими средствами. Чаще всего, это всё-таки существующее в реальности устройство. К примеру, генераторы шума, предназначенные для шифрования данных и маскировки беспроводных каналов.

Эффективные методы программных средств

Здесь подразумевается обычно криптография (шифрование посредством алгоритма или устройства, которое проводит операцию автоматически). **Шифровать информацию**можно десятками различных методов – от перестановки до гаммирования.

**Метод подстановки** достаточно простой. Просто исходный алфавит (русский или английский) заменяется альтернативным. В случае с перестановкой используются также цифровые ключи.

Высшую степень защиты обеспечивает**гаммирование.** Но для такой криптографической работы потребуется специалист высокого уровня, что не может не сказаться на стоимости услуги.

Дополнительной системой безопасности может стать создание специальной **электронной, цифровой подписи**.

Выводы

Несмотря на существенные угрозы, исходящие из интернета, реально создать эффективно работающую систему безопасности. Первое что нужно сделать провести [ит-аудит безопасности данных](https://sky-dynamics.ru/it-audit/), [подключить программы на пк](https://sky-dynamics.ru/obsluzhivanie-kompjuterov/), позволяющие сохранить конфиденциальную и любую другую важную для бизнеса или частной жизни информацию. Технических средств и методик более чем достаточно, также можно обеспечить своей компании [мониторинг IT-инфраструктуры](https://sky-dynamics.ru/sistema-monitoringa-it-infrastruktury/). Весь вопрос – в желании и возможности их применять.



