Информационная безопасность, или ИБ, — это комплекс мер, которые нужны, чтобы защитить от утечки или взлома программы, компьютерные системы и данные. Еще так называют отрасль, которая занимается этими мерами.

Самый простой пример меры по информационной безопасности — антивирус, установленный на компьютере. Но в коммерческих структурах к этому вопросу подходят более серьезно и на многих уровнях: чтобы обеспечить безопасность, нужно много чего сделать.

Средства информационной безопасности защищают данные от утечки, программы, системы и сети — от взлома, несанкционированного доступа, порчи файлов или других видов атак. Если речь о коммерческих или государственных структурах, сведения также защищают от шпионов или возможных злоумышленников внутри самого коллектива.

**Для чего нужна информационная безопасность**

Информационная безопасность защищает системы от проникновения и от атак. Сюда входит не только взлом: это и DDoS-атаки, в результате которых может «лечь» сервер сайта, и утечка данных, и многое другое. Злоумышленников намного больше, чем кажется. И никто не хочет, чтобы их сервис потерял работоспособность, а данные оказались доступны всем вокруг. Для этого и нужна информационная безопасность.

У компаний есть еще одна причина: за утечку конфиденциальных данных пользователей они несут ответственность по закону. Так что для них меры по безопасности — это еще и способ избежать проблем с законодательством и потери доверия клиентов.

Без мер по информационной безопасности кто угодно мог бы получить доступ к конфиденциальным сведениям или взломать любой сайт или систему. Компьютерным пространством стало бы фактически невозможно пользоваться.

**От каких угроз защищает ИБ**

Угрозы безопасности разделяют на две категории: внутренние и внешние.

**Внутренние.** Это угрозы, которые идут изнутри системы. Чаще всего в таких случаях речь идет об утечке данных или об их повреждении. Например, кто-то подкупил сотрудника, и тот похитил данные, составляющие коммерческую тайну. Второй вариант — злоумышленником оказался авторизованный пользователь.

Еще одна внутренняя угроза — риск банальной ошибки, в результате которой конфиденциальные сведения окажутся в открытом доступе или повредятся. Например, в открытом доступе оказалась часть базы данных или пользователь по неосторожности повредил файлы. Такое уже бывало в истории. А нужно, чтобы таких случаев не возникало: клиент не мог бы нарушить работу системы даже случайно, а информация оставалась защищена.

**Внешние.** Сюда относятся угрозы, которые приходят извне, и они могут быть куда разнообразнее. Это, например, попытка взлома системы через найденную уязвимость: злоумышленник проникает в сеть, чтобы украсть или повредить информацию. Или DDoS-атака, когда на веб-адрес приходит огромное количество запросов с разных адресов, и сервер не выдерживает, а сайт перестает работать.

Сюда же можно отнести деятельность компьютерных вирусов: они способны серьезно навредить работе системы. Действия таких вредоносных программ могут быть очень разнообразными: от рассылки спама от имени взломанного адреса до полной блокировки системы и повреждения файлов.

Еще к внешним угрозам безопасности относятся форс-мажоры и несчастные случаи. Например, хранилище данных оказалось повреждено в результате аварии или пожара. Такие риски тоже нужно предусмотреть.

**Кто работает с информационной безопасностью**

Существует отдельная должность специалиста по информационной безопасности. В крупных компаниях это может быть отдельный департамент. В маленьких — один сотрудник, причем порой он также выполняет обязанности системного администратора или сетевого инженера. Бывает и так, что информационную безопасность отдают на аутсорс: в этом случае ею занимаются сотрудники специализированной компании.

В широком смысле простейшие меры по информационной безопасности предпринимает кто угодно. Установить антивирус и блокировщик навязчивой рекламы, не посещать подозрительные сайты и не запускать непроверенные файлы — все это тоже меры ИБ, хоть и максимально простые. Но настоящий специалист по безопасности — это профессионал с широкими знаниями и множеством специфических навыков.

**Три принципа информационной безопасности**

Информационная безопасность отвечает за три вещи: доступность, конфиденциальность и целостность данных. Сейчас расскажем, что это означает.

**Доступность.** Это значит, что к информации могут получить доступ те, у кого есть на это право. Например, пользователь может зайти в свой аккаунт и увидеть все, что в нем есть. Клиент может перейти в каталог и посмотреть на товары. Сотрудник может зайти во внутреннюю базу данных для его уровня доступа. А если на систему производится атака и она перестает работать, доступность падает порой до полного отказа.

**Конфиденциальность.** Второй принцип — конфиденциальность. Он означает, что информация должна быть защищена от людей, не имеющих права ее просматривать. То есть в тот же аккаунт пользователя не сможет войти чужой человек. Без регистрации нельзя комментировать что-то на сайте, без личного кабинета — оплатить заказ. Человек, который не работает в компании, не может зайти в ее внутреннюю сеть и посмотреть там на конфиденциальные данные. Если систему взламывают, конфиденциальность оказывается нарушенной.

**Целостность.** Целостность означает, что информация, о которой идет речь, не повреждена, существует в полном объеме и не изменяется без ведома ее владельцев. Комментарий не сможет отредактировать посторонний человек — только автор или иногда модератор. Сведения в базе данных меняются только по запросу тех, у кого есть доступ. А в вашем аккаунте не появятся письма, написанные от вашего лица без вашего ведома. При взломе системы целостность опять же может нарушиться: информацию могут модифицировать, повредить или стереть.

**Какие данные охраняет ИБ**

**Персональные.** Персональные данные — информация, которая связана с какими-то людьми. Это ФИО, телефон, адрес жительства, электронная почта и многое другое. По российским законам эти данные нужно охранять от несанкционированного доступа. Поэтому компании спрашивают разрешение на обработку персональных данных, если вы регистрируетесь на сайтах или заказываете какие-то услуги. Они обязаны это делать. А потом — хранить эту информацию, чтобы к ней не получили доступ чужие люди.

Истории про нарушение конфиденциальности этих данных вы наверняка слышали. Например, мошенники могут звонить клиентам банков, а их номера получают из слитых баз. Вот пример того, к чему может привести недостаточная информационная безопасность.

**Тайные.** Еще одна категория сведений — те, которые составляют тайну: государственную, коммерческую, профессиональную и служебную.

К гостайне относятся сведения, важные для безопасности страны, и они засекречены максимально строго. Коммерческая тайна — информация, критичная для нормальной работы компании: если она раскроется, организация может потерять деньги или конкурентное преимущество. При этом компания не имеет право засекречивать некоторые сведения: имена владельцев, условия труда и так далее.

Отдельно стоят профессиональная и служебная тайна. Профессиональная тайна — это, например, врачебная: история болезни пациента не должна раскрываться посторонним людям, как и данные о его состоянии. А еще — адвокатская, нотариальная и некоторые другие. А служебная тайна — некоторая информация, которая принадлежит определенным службам, например налоговой.

Все эти сведения нужно защищать: их утечка или повреждение способны причинить серьезные проблемы.

**Общедоступные.** Не удивляйтесь. Информация, которая известна всем, все еще должна быть доступной и целостной. Поэтому ее тоже следует защищать, иначе кто угодно сможет изменить цену товара в интернет-магазине и подставить этим покупателей. Или «уронить» сайт, чтобы никто не смог на него войти.

**В каких сферах ИБ важнее всего**

Есть отрасли, для которых защита информации очень важна, так как потеря данных способна нанести им катастрофический ущерб. Обычно это сферы, которые работают с деньгами или с другими ценностями.

**Банки и финансы.** Банковские сервисы относятся к безопасности очень строго. Защищать информацию здесь нужно не только от возможных взломщиков, но и от мошенников, и от других злоумышленников. Поэтому банки обычно защищены на очень высоком уровне. Даже для авторизации в личном кабинете с незнакомого устройства нужны дополнительные действия: сначала система проверит, что вы — это вы.

**Государственные сервисы.** Второй случай крайне важных данных — государственные сервисы и системы. Если это внутренняя сеть, в ней могут храниться сведения, составляющие государственную тайну, а ее утечка — прямая угроза безопасности страны. А в сервисах для граждан множество персональной информации: паспортные данные, сведения о работе, штрафах, семье и многом другом. Потеря таких сведений поставит под удар огромный процент населения.

**Компании с большой базой персональных данных.** Это различные крупные сервисы, в которых зарегистрировано много людей. Если их персональные данные «утекут», кто угодно сможет воспользоваться ими в своих целях — а компания будет нести за это ответственность.

**Важные сектора экономики.** Энергетические, нефтегазовые и другие предприятия тоже должны быть хорошо защищены. В системах таких структур есть информация, которая составляет коммерческую тайну, и в этом случае она критична. Более того, оборудованием и механизмами тоже может управлять автоматика, цифровая система. Если кто-то получит к ней доступ, то сможет застопорить всю работу предприятия.

**Дата-центры.** Это помещения, где стоит и работает серверное оборудование. К их оснащению и доступу к ним предъявляются повышенные требования, чтобы сервера были защищены от внешних воздействий и от различных угроз. В том числе от злоумышленников: в случае с физическим оборудованием украсть или повредить информацию может быть довольно просто. Поэтому нужно не допустить, чтобы кто-либо в принципе получил несанкционированный доступ к помещению.

**Электронная коммерция.** Интернет-магазины и другие сайты, которые работают с платежами пользователей, тоже должны заботиться о безопасности — по понятным причинам. Утечка платежных данных — это очень серьезно и может привести к потере денег.

**Какими методами пользуются специалисты по ИБ**

Какую информацию нужно защищать и зачем — разобрались. Теперь поговорим о том, как именно это делают. Информационная безопасность — это не одно действие, а целый набор разнообразных мер:

* поиск технических уязвимостей и защита от них;
* «защита от дурака», чтобы никто не смог навредить данным по ошибке;
* создание инфраструктуры, которая устойчива к частым способам атаки;
* шифрование информации внутри сети или системы;
* защита паролей и других конфиденциальных сведений;
* защита базы данных от несанкционированного вмешательства;
* контроль доступа людей к критичной информации;
* предоставление доступа по защищенным каналам;
* отслеживание поведения пользователей, чтобы вовремя пресечь возможную угрозу;
* построение системы оповещений об уязвимостях и взломах;
* регулярное проведение аудитов, которые описывают состояние системы.

И это только малая часть возможных действий, причем за каждым из них скрывается огромная и разнообразная работа.

**Инструменты для защиты информации**

Специалист по информационной безопасности работает с определенными инструментами — они помогают защитить сведения от посягательств. Их условно можно разделить на физические, технические и административные.

**Физические.** Это инструменты, которые существуют в физическом мире. К ним обычно относится различное оборудование. Пластиковые ключи-карты и замки, которые открываются по ним, — это физический инструмент. Установленные в дата-центре резервные сервера — тоже. Еще сюда можно отнести видеонаблюдение и сигнализацию, использование сейфов, работу с физическими источниками информации, мониторинг оборудования и многое другое.

**Технические и программные.** Это то, что относится скорее к софту, а не к железу, от защищенных протоколов до антивируса. Шифрование данных, передача сведений через HTTPS, установка брандмауэра и так далее — такие меры. Есть и специальные инструменты: защитное ПО и сервисы, программы для поиска уязвимостей и имитации атак, многое другое. К техническим средствам еще можно отнести построение инфраструктуры защищенной системы и сети.

Некоторые компании называют техническими средствами все, что связано с техникой. Это ярко видно, например, в официальных документах, даже если фактически они описывают физические методы.

**Административные.** Сюда относится построение внутренней инфраструктуры, регламенты и контроль доступа. Например, разработка матрицы доступа — документа, который определяет, какие полномочия есть у каждого сотрудника. Эти меры защищают не от технических угроз, а скорее от человеческого фактора. Так человек без соответствующих полномочий не сможет получить доступ к конфиденциальным данным.

**Как начать заниматься информационной безопасностью**

На «личном», персональном уровне обеспечить себе защиту не так сложно. Нужно пользоваться брандмауэром и антивирусом, посещать сайты только с защищенным соединением, не скачивать подозрительный контент. А если подозреваете, что какой-то ресурс за вами шпионит, — пользоваться VPN или прокси.

Другое дело — стать специалистом по информационной безопасности. Это куда сложнее: профессия комплексная, требует большого количества разнородных знаний. Понадобится изучить, как функционируют системы и сети, знать об основных уязвимостях и атаках, уметь их закрывать и отражать. Более того, специалист по ИБ должен сам уметь атаковать системы: это важно, например, при пентесте. Желательно знать некоторые языки программирования, и точно нужно знать внутренние языки для управления ОС.

На курсах мы дадим вам представление о том, как стать ИБ-шником, и поможем стартовать в этой сложной, но интересной отрасли.