**Основы ИБ. Что такое информационная безопасность?**

Информационная безопасность — это особое состояние, когда пользователь получает гарантии защищенности важных данных и оборудования, которое их сохраняет, обрабатывает и передает. Целостности сведений угрожают случайно или преднамеренно, естественными либо искусственными способами. Владельцы данных используют различные способы их защиты, а специалисты по ИБ постоянно разрабатывают новые стратегии и тактики, чтобы формировать, использовать и развивать информационную среду в интересах каждого юзера — от гражданина до предприятия и государства.

Сведения защищают на нескольких уровнях: законодательном (международные и российские нормы права), административном (локальные акты предприятий), процедурном (меры пользователей) и программно-техническом (непосредственные инструменты защиты данных). Законодательные решения создают базу, которая обозначает понятия сферы информационной безопасности и меры наказания, применяемые к нарушителям ИБ.

**Цели информационной безопасности**

Любое государственное либо частное предприятие обязано надежно и эффективно обеспечивать информационную безопасность. Это очень важно, т. к. технологии постоянно развиваются, а сфера применения компьютеров и другого оборудования расширяется. Цели ИБ формируют, исходя из задач, которые стоят перед системой кибербезопасности отдельной компании.

Данные необходимо защищать везде — от ресурсов отдельных пользователей до порталов государственного уровня. Кроме непосредственного обеспечения безопасности, нужно предоставлять каждому юзеру качественную и достоверную информацию, а также оказывать правовую поддержку при работе со сведениями. Поэтому главная цель ИБ — сформировать условия, которые обеспечат высококачественную и эффективную защиту важных данных от намеренного либо случайного вмешательства. Последнее способно повредить, удалить, изменить или другим способом воздействовать на конфиденциальные сведения. В сфере бизнеса информационная безопасность заключается в числе прочих мер в обеспечении непрерывности коммерческих процессов.

Чем важнее данные, тем больше они нуждаются в защите. Постоянно развивающиеся инструменты ИБ отслеживают любые изменения в системном коде и попытки несанкционированного проникновения в хранилище информации. Если уделять кибербезопасности мало времени и средств, то могут нагрянуть катастрофические последствия в виде утери важных сведений, заражения вредоносными кодами, неправомерного доступа посторонних лиц к банку данных и т. д. Главная задача ИБ — максимально ограничить подобные ситуации и предусмотреть все потенциальные опасности. Чем выше надежность системы, тем ниже вероятность взлома.

**Принципы ИБ**

Чтобы достичь целей, стоящих перед ИБ, специалистам необходимо обеспечить следующие принципы защиты данных:

* Доступность. Уполномоченные лица должны в любой момент иметь простой и беспрепятственный доступ к важной информации.
* Целостность. Основная масса пользователей может только просматривать защищаемую информацию. Редактировать, копировать, удалять уполномочен узкий круг специалистов.
* Конфиденциальность. Доступ к секретным сведениям имеют только уполномоченные лица. У других пользователей нет права даже просматривать защищенную информацию.

Типы контроля

Цели информационной безопасности возможно достигнуть не только, соблюдая принципы ИБ, но и осуществляя необходимый контроль, который подразделяют на 3 основных разновидности. Физический контроль подразумевает отслеживание поведения сотрудников за рабочими компьютерами, мониторинг вычислительного и бытового оборудования. К последнему относятся системы отопления и кондиционирования, сигнализации, видеонаблюдения, запирания дверей и т. д. Обеспечивая логический контроль, используют специальные технические инструменты: защитное ПО, [брандмауэры](https://itspectr.ru/chto-takoe-brandmauer-chto-delaet-kak-vklyuchit-i-otklyuchit/), логины/ пароли и др. В рамках административного контроля применяют государственные законодательные акты и нормы, принятые в организации. Эти стандарты обозначают рамки, которые нельзя нарушать бизнесу и отдельным пользователям.

**Виды угроз ИБ**

Угрозы ИБ подразделяют на 3 вида:

Техногенные. Это угрозы, вызванные уязвимостями в техническом обеспечении и защитных инструментах. Их сложно спрогнозировать.

Антропогенные. Так называемый «человеческий фактор». Пользователь может допустить непреднамеренные действия (например, случайно отключить антивирус) и специальные (совершить информационное преступление — например, взломать систему доступа). Этот вид угроз легче спрогнозировать и устранить неприятные последствия случайного или намеренного вмешательства.

Стихийные. Эти проблемы трудно предвидеть и почти невозможно предотвратить. К ним относятся стихийные бедствия и сопутствующие им явления (землетрясения, пожары, подтопления).

Таким образом, вся работа системы ИБ заключается в создании защищенных каналов передачи данных, безопасности серверного оборудования, носителей информации, рабочих мест.

**Объекты информационной безопасности**

К объектам ИБ относятся любые информационные ресурсы, которые необходимо защищать от несанкционированного доступа. Это — разнообразные порталы, где пользователям предоставляют уникальные сведения (аналитические и системные организации, работающие с информацией, в т. ч. и личными пользовательскими данными), официальные сайты СМИ, [локальные сети](https://itspectr.ru/chto-takoe-kompyuternaya-set-vidy-i-osnovnye-princzipy/) предприятий. Объектами ИБ являются и глобальные системы, которые создают, размещают и распространяют данные в сети, шифраторы, юридическая помощь юзерам, особое программное обеспечение, а также защита интеллектуальной собственности и закрытой информации.

Обеспечение информационной безопасности организаций

С чем же конкретно борется система информационной безопасности? С различными угрозами, которые искажают данные, нарушают работоспособность систем, похищают важные сведения.

**Угрозы на государственном уровне**

Проблемы бывают внешние и внутренние. К первым относят шпионские атаки других государств, в результате которых похищают различные секреты и технологии. Также внешней угрозой является так называемая «информационная война», в рамках которой в сети распространяют негативные сведения о государстве, дезинформируя население и ухудшая его осведомленность о делах внутри страны.

Внутренние проблемы требуют более серьезного обеспечения ИБ, т. к. многих угроз можно избежать, если качественно защищать информационные ресурсы современными методами, продолжать развивать технологии и делать их доступными для обычных пользователей, а также повышать компьютерную грамотность.

Преднамеренные угрозы

Это — хакерские атаки на интернет-ресурсы с целью получения несанкционированного доступа к хранилищу данных либо управлению порталом. Злоумышленники обычно «трудятся» по заказу иностранных государств, корыстных пользователей или предприятий-конкурентов. В этом случае задачей ИБ является как можно быстрее выявить и нейтрализовать действия преступной группировки, а также не допустить возникновения подобных проблем в дальнейшем.

Сражения с вирусами

Большинство хакерских атак происходит с использованием вирусных программ. Главная загвоздка при попытках решить эту проблему заключается в том, что разработчики, создающие антивирус, на шаг отстают от создателей вредоносных кодов. Поэтому хакеры зачастую успевают сделать свое дело, прежде чем сработает система информационной безопасности, которая сразу не распознает несанкционированное вмешательство.

Особые утилиты, призванные бороться с засилием вредоносных программ, обнаруживают и нейтрализуют вирус, но только после того, как он уже проник в систему. Хотя в этом есть и свой плюс — инструменты ИБ запоминают вредоносный код и при следующей атаке успешно ее отражают. Но при проникновении нового вируса ситуация повторяется.

**Средства ИБ**

Обычно в решении проблем информационной безопасности рядовые пользователи участия не принимают. Специалисты используют следующие средства:

* специальный софт, обеспечивающий безопасность индивидуального устройства (ПК, ноутбука, смартфона, планшета);
* защитные инструменты и функционал, способные наладить деятельность целого массива информации;
* сверхмощное ПО, гарантирующее безопасность и шифрование данных, используемых в банковской и финансовой деятельности;
* отдельные инструменты, исправляющие различные уязвимости.

**Методы защиты данных**

Для борьбы с конкретными угрозами и защиты информации используют различные методы. И, чем больше оборудования задействовано в едином информационном пространстве, тем более сильной и многофункциональной должна быть защита. Максимальную безопасность необходимо обеспечить ядру данных. Плюс к этому нужно гарантировать каждому пользователю защиту при доступе к общим интернет-ресурсам.

Для обеспечения ИБ специалисты делают следующее:

* ограничивают уровень доступа к сведениям;
* зашифровывают передаваемую информацию;
* контролируют использование БД;
* отслеживают поведение пользователей;
* создают новейшие вычислительные процессы, защищенные несколькими уровнями шифрования.

Кроме этого, специалисты по ИБ применяют особые устройства, способные оперативно распознать несанкционированное вмешательство и нейтрализующие множество известных угроз.