Глава 1
Основные понятия

Первое, с чего нам придется начать, — с определения: что такое собственно «информационная безопасность». Так сложилось, что в большинстве случаев представление о «безопасности» как таковой связано у нас со всевозможными мерами запретительно-охраняющего характера. На самом же деле такое представление не вполне точно описывает ситуацию.

При построении определения понятия «информационная безопасность» нужно учесть следующие факты:

1) информация (точнее — данные) как набор сигналов (либо физических состояний некоторого носителя) для конечного пользователя особого интереса не представляет. Мы воспринимаем информацию, скорее, как результат работы тех или иных программ и аппаратуры, без которых она бесполезна;
2) в отличие от кражи какой-либо вещи или денег кража информации непосредственно не приводит к ее потере, но имеет достаточно серьезные последствия и потому требует отдельного рассмотрения*;
3) обработка и использование информации (особенно когда речь идет о нескольких разных информационных массивах) возможна только в случае, когда ее логическая структура соответствует определенным правилам;
4) поскольку и обработка, и прием/передача информации, по определению, — это *процессы*, определить безопас-

---

* Однако сказанное вовсе не означает, что такая кража не является нанесением материального либо морального ущерба!

ность как некоторое статическое состояние нельзя. Ситуация просто не может не меняться.

Таким образом, **информационная безопасность** — это *процесс* соблюдения (сохранения) трех аспектов (атрибутов безопасности): *доступности*, *целостности* и *конфиденциальности информации*.

Опишем эти аспекты.

1. **Доступность информации.** Информация в безопасном состоянии должна быть доступной для пользователя, т. е. должна быть сохранена возможность проведения всех операций по ее обработке. Для этого необходимо наличие работоспособного оборудования, неповрежденных носителей и, конечно же, необходимых программ (причем правильно настроенных).
2. **Целостность информации** — это соответствие логической структуры информации определенным правилам, т. е. логически корректное ее состояние. Процедуры обработки и изменения информации должны преобразовывать одно целостное состояние в другое.
3. **Конфиденциальность.** Выполнение тех или иных операций с информацией должно происходить в соответствии с определенными правилами, составляющими существенную часть политики безопасности. *Нарушение конфиденциальности* — это возможность выполнения каких-либо операций с информацией (например, ее чтения или записи) теми, кто не имеет на это прав.

Следует отметить, что это — именно аспекты, т. е. стороны одного и того же процесса. Все они тесно связаны между собой, так что нарушение одного из них может приводить к нарушению другого.

Возможность нарушения (нежелательного изменения) одного из аспектов называется **угрозой**, а по возможным его целям — «нарушением доступности», «нарушением целостности» или «утечкой». Фактически, *угроза — это некоторое потенциально возможное нарушение безопасности*.

Реализация угрозы (фактическое нарушение безопасности) становится возможной благодаря существованию *уязвимостей*. **Уязвимость** — это какая-либо неудачная характеристика системы (программная ошибка, несовершенство аппаратной технологии, неверная настройка), благодаря которой становится возможным нарушение того или иного аспекта безопасности.

Заметим, что вышесказанное фактически означает, что полностью безопасных систем практически не существует, поскольку безошибочно написанных программ, безупречных универсальных технологий и способов абсолютно верной настройки сложных программно-аппаратных комплексов не существует.

Следует также учесть, что обеспечение аспектов безопасности требует компромиссов. Полное соблюдение политики конфиденциальности сильно ограничивает доступность данных; если все внимание отдается целостности, то замедляется обработка информации, а полная доступность данных практически всегда означает нарушение политики безопасности*.

При обеспечении информационной безопасности обычно стараются создать такую ситуацию, когда нарушение безопасности становится событием маловероятным и приносящим минимальный ущерб. В частности потому, что нанесение подобного ущерба становится нерентабельным (для этого приходится больше потратить ресурсов, чем можно получить выгоды), вероятность сбоев аппаратного и программного обеспечения — малой, а работы по их восстановлению — автоматизированными, быстрыми и дешевыми.

Для описания ситуаций, так или иначе связанных с нанесением ущерба, используют еще несколько терминов.

Атакой называется действие (либо последовательность действий), которое приводит к реализации угрозы.

Описанная последовательность всех событий, связанных с тем или иным нарушением безопасности информации,

---

* Чем жестче политика безопасности — тем ***неудобнее*** работать с информацией, так как очевидно, что при этом возникает много ограничений.

включая приведшие к ее нарушению обстоятельства и последующие за реализацией действия, называется **инцидентом.**

Прежде чем перейти к непосредственному описанию различных угроз, теоретически возможных типов атак и примеров реальных инцидентов, следует отметить несколько обстоятельств не технического, а, скорее, психологического характера. Многим кажется, что:

1. *Проблемы обеспечения безопасности редко касаются «обычных» пользователей, потому что «у них нет секретов»*. Однако и у обычного пользователя есть то, что имеет смысл защищать. Это, как минимум, его время и репутация. Компьютер пользователя, его ресурсы могут быть использованы для показа и распространения нежелательной рекламы и даже для совершения противоправных действий. Личная информация пользователя может быть украдена для составления баз данных. Кроме того, потеря личной информации чрезвычайно чувствительна — вне зависимости от того, можно ли ею торговать.
2. *Компьютеры, редко работающие в сети, вряд ли подвергнутся нападению, поскольку злоумышленники о них не узнают*. Значительная часть современных атак и угроз не направлена на кого-то конкретно, а выполняется по принципу «боя по площадям». Незащищенная машина без выполнения хотя бы основных процедур защиты остается не пораженной в среднем не более 30 минут после начала работы со средой Интернет.
3. *Проще нанять специалиста — он все сделает (вариант: «всю нашу информацию защищают специалисты другой организации»)*. Во-первых, специалист будет исходить в настройке из ваших описаний, которые вы, скорее всего, сделаете неточно. Во-вторых, защита — это не статичное состояние, а процесс, т. е. некоторые действия нужно предпринимать всегда во время работы (да и вызов специалиста вряд ли бесплатен). И, в-третьих, никакая защита не гарантирует отсутствие ущерба от ваших же собственных ошибок.

4. *Если вообще не подключать компьютер к сети, то никакие угрозы его не коснутся.* К сожалению, далеко не все угрозы возникают при подключении компьютера к сети. Из того, что ваши данные не достанутся злоумышленникам, еще не следует, что вас не будет волновать их потеря. Кроме того, значительная часть производственных задач, возникающих перед современным пользователем, требует взаимодействия с другими пользователями, и отказ от этих возможностей — не самое оптимальное решение, на наш взгляд*.

Несмотря на большое количество теоретических сведений и технических средств, применяемых для обеспечения информационной безопасности, можно выделить несколько *общих принципов*, необходимость соблюдения которых практически не зависит от используемых технических средств.

1. **Применение превентивных мер.** По техническим причинам реализация подавляющего большинства угроз при обработке информации с помощью компьютера происходит значительно быстрее, чем пользователь может распознать атаку и предпринять какие-то меры. По этой причине защита должна быть продумана и реализована ***до*** того, как возникнет проблема.
2. **Уменьшение «поверхности атаки».** Чем меньше объектов, которые могут быть подвержены тем или иным угрозам, тем меньше вероятность нарушения аспектов безопасности. Из этого вытекает необходимость минимизации количества программ и их взаимодействия с внешними источниками информации.
3. **Защита на всех этапах обработки информации.** Степень уязвимости системы определяется по ее наиболее уязвимому узлу. Вне зависимости от общего количества при-

* Осуществление платежей, подача отчетных данных в налоговые органы, удаленная разработка и обслуживание программных комплексов, консультации, торговля — вот неполный список возможностей, которые компьютерные сети предоставляют уже сейчас. Разумеется, можно все это делать и традиционными способами — при личных поездках, наличных расчетах, поиске и т. д. И — потратить в итоге в несколько раз больше времени, чем те, кто пользуется сетями...

нятых мер последние будут бесполезны, если в их числе останутся хоть какие-то слабозащищенные этапы обработки.

4. **«Эшелонирование» защиты.** Все защитные комплексы создаются по принципу «эшелонов» — этапов, слоев обработки. Это позволяет отчасти компенсировать их недостатки, снизить общую вероятность поражения системы, минимизировать ущерб успешной реализации угрозы. Тем не менее каждый «эшелон» при построении всей системы считается «единственным» (т. е. все предшествующие «эшелоны» защиты уже считаются преодоленными злоумышленником) и делается максимально закрытым (см. принципы 1 и 2).

5. **Разграничение доступа.** Доступ пользователей к выполнению тех или иных операций должен соответствовать задачам, стоящим перед каждым конкретным пользователем. Чем меньше таких операций доступно каждому пользователю, тем меньше ущерб, который может быть нанесен (не обязательно самим пользователем, возможно — одной из его программ).*

6. **Желание быть защищенным.** Самый уязвимый компонент защиты — это плохо обученный пользователь. Никакие ухищрения не помогут, если пользователь не соблюдает мер предосторожности и не понимает, какие угрозы возникают во время его работы.**

Основная часть нашего элективного курса посвящена задачам, возникающим при обеспечении информационной

---

* Популярное обоснование отключения защитных мер: «они мешают мне работать». В этом случае надо задуматься либо об организации защиты, либо, что более вероятно, об организации работы — иначе эта работа может неожиданно прерваться совсем! Заметим, кстати, что в подобном случае «обосновавшие» отключение защиты лица предпочитают возлагать ответственность за любые сбои на технический персонал.

** Бóльшая часть ущерба наносится обычно в результате не столько направленных вредоносных действий, сколько ошибок. В подавляющем же большинстве других случаев вред наносится сотрудником пострадавшей организации из ее внутренней сети.

безопасности в условиях взаимодействия с глобальной сетью (точнее — межсетевой средой) Интернет. Для удобства обсуждения и разъяснения некоторых ее особенностей необходимо вспомнить основы модели обмена данными в Интернете.

При разработке основных концепций, до сих пор лежащих в основе функционирования Интернет, использовалась *модель сетевого взаимодействия*, получившая название *DOD*. В ней предполагается разделение всех функций обмена данными в сетях на четыре взаимодействующих между собой слоя — уровня.

Именно эту модель мы и будем использовать для структурирования материала в нашем пособии. О возникающих угрозах и средствах их устранения или снижения вреда мы будем рассказывать, «поднимаясь вверх» по перечисленным в этой модели уровням.

Модель сети DOD

Уровни	Назначение	Протокол в стеке TCP/IP
Прикладной	Программы, с которыми работает пользователь	HTTP, FTP, SMTP
Транспортный	Транспорт данных — деление на пакеты, контроль доставки, сбор сообщений	TCP, UDP
Сетевой	Управление потоками данных; пересылка, установление связи и т. д.; соединение отдельных сетей	IP, ICMP, ARP
Доступ к среде	Физическая передача и прием сигналов, контроль ошибок	

Рассказывая об основных механизмах работы, угрозах и способах защиты от них, мы будем приводить примеры экспериментов — действий, проведя которые, можно убедиться, что:

1) описываемая проблема/механизм действительно существуют;

2) механизм работы компонентов, программ и описываемых угроз, по крайней мере, в основном совпадает с утверждениями авторов (к сожалению, не всегда можно описать его точно — приходится что-то упрощать);

3) предлагаемые меры защиты действительно способны хотя бы снизить вероятность реализации угрозы или уменьшить вред от нее.

В некоторых случаях эти эксперименты крайне нежелательно проводить в условиях работающей сети — именно потому, что защитные меры в ней не приняты или, наоборот, приняты, а ваши эксперименты будут восприняты как попытка причинения вреда*. Поэтому там, где это возможно (то есть — почти во всех случаях), авторы рекомендуют использовать для подобных экспериментов *виртуальные машины*. Примером может служить свободно доступная программа *Microsoft Virtual PC*. К сожалению, ее аппаратные требования при этом достаточно высоки (фактически — необходимы ресурсы для работы трех компьютеров на одном), но выгоды — очевидны.

Некоторые эксперименты зависят от имеющегося оборудования, поэтому время от времени утверждения авторов придется проверять в другом месте либо верить внешним источникам.

---

* Все подобные эксперименты обязательно должны быть согласованы с системным администратором или человеком, выполняющим его функции. Любознательность, приводящая к помехам в работе, всегда встречается без всякого понимания. Причем ваши мотивы будут восприниматься уже через призму оценки ваших действий.

Некоторые разделы нашего курса будут завершаться рассмотрением правовых норм той или иной деятельности в информационной сфере. Это — необязательные части элективного курса (они будут далее помечены звездочкой, как, например, следующая глава — разъяснение основных понятий в соответствии с российским законодательством); их можно пропускать, если не хватает учебного времени или материал не входит в сферу ваших интересов.