Понятие информационной безопасности

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин *"информационная безопасность"* используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ "Об участии в международном информационном обмене" (закон утратил силу, в настоящее время действует "Об информации, информационных технологиях и о защите информации") *информационная безопасность* определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком-либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин *"информационная безопасность"* будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

Под ***информационной безопасностью*** мы будем понимать защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и *поддерживающей инфраструктуры*.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам *информационной безопасности* начинается с выявления *субъектов информационных отношений* и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы *информационной безопасности* – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с *информационной безопасностью*, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором – "да нет у нас никаких секретов, лишь бы все работало".
2. *Информационная безопасность* не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. *Субъект информационных отношений* может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная *безопасность*" (как эквивалент или заменитель *ИБ*) представляется нам слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую *очередь* на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее *безопасность* определяется всей совокупностью составляющих и, в первую *очередь*, самым *слабым звеном*, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой *пароль* на "горчичнике", прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от *поддерживающей инфраструктуры*, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта *инфраструктура* имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении *ИБ* перед существительным "*ущерб*" стоит прилагательное "неприемлемый". Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда *стоимость* защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) *выражение*, а целью защиты информации становится уменьшение *размеров ущерба* до допустимых значений.

Основные составляющие информационной безопасности

Информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только системный, *комплексный подход*.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и *поддерживающей инфраструктуры*.

Иногда в число основных составляющих *ИБ* включают защиту от несанкционированного копирования информации, но, на наш взгляд, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и *непротиворечивость* информации, ее защищенность от разрушения и несанкционированного изменения.

Наконец, *конфиденциальность* – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если *по* тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит *ущерб* всем *субъектам информационных отношений*. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент *информационной безопасности*.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (*продажа* железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля *динамической целостности* применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом *ИБ* в тех случаях, когда *информация* служит "руководством к действию". Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, *нарушение целостности*которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации. *Конфиденциальность* – самый проработанный у нас в стране аспект *информационной безопасности*. К сожалению, практическая реализация мер *по* обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить*представление* о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий *субъектов информационных отношений*, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей *по* важности *целостность* – какой смысл в информационной услуге, если она содержит искаженные сведения?

Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).