ЗАЩИТА ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

Введение

Последние двадцать - тридцать лет, можно сказать, стали вехой в плане ранжирования приоритетов и ценностей. На авансцену вышла её Величество Информация. Обладатели ценных знаний могут управлять значительными процессами на нашей планете. Но существуют незыблемые законы конкуренции: имеешь силу и власть – можешь быстро ты пропасть. И в точном соответствии с концепцией войны мы оберегаем свои силы, чтобы в решающей битве низвергнуть врага. Кто-то прячет ножи, кто-то автоматы, кто-то химгородки, а некоторые камуфлируют свои ядерные запасы под заводы по изготовлению мороженного.

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю — национальном, отраслевом, корпоративном или персональном. Для иллюстрации этого положения ограничимся одним примером.

Согласно распоряжению президента США Клинтона (15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических угроз, так и от атак, проводимых с помощью информационного оружия. В начале октября 1997 года, при завершении подготовки доклада президенту, Роберт Марш, глава вышеупомянутой комиссии, заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.

На наш взгляд, нет оснований предполагать, что Россия обладает большей защищенностью.

В данной работе мы попытаемся составить карту, характеризующую состояние основных аспектов информационной безопасности в России. Нас будут интересовать как уже освоенные области, так и "белые пятна", незаслуженно обойденные вниманием.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать ее специфику, состоящую в том, что информационная безопасность есть составная часть информационных технологий — области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, регламенты, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

Многогранная информация

Сначала обратимся к основным определениям терминов, используемых в этой работе.

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

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. Из этого довольно очевидного положения можно вывести два важных для нас следствия:

- Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты.
- Информационная безопасность не сводится исключительно к защите информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести материальные и/или моральные убытки) не только от несанкционированного доступа к информации, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита информации стоит по важности отнюдь не на первом месте.

Информационная безопасность — многогранная, можно сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход. В этом разделе мы укажем важнейшие на наш взгляд грани.

Спектр интересов субъектов, связанных с использованием информационных систем, можно подразделить на следующие основные категории:

- доступность (возможность за приемлемое время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного ознакомления).

Рассмотри эти категории.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, 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. Имеются в виду продажа железнодорожных и авиабилетов, банковские услуги и т.п.

Важность доступности как аспекта информационной безопасности находится в разительном противоречии с тем вниманием, которое уделяют данному аспекту потенциально заинтересованные стороны. Если вопросы защиты от несанкционированного доступа (то есть обеспечение конфиденциальности и целостности информации) курирует Гостехкомиссия России, а криптографические средства (что опять-таки связано с обеспечением конфиденциальности и целостности) — ФАПСИ, то доступностью на государственном уровне не занимается пока никто. На законодательном уровне вопросы доступности затрагиваются только в новой редакции Уголовного кодекса (раздел IX — "Преступления против общественной безопасности", глава 28 — "Преступления в сфере компьютерной информации", статья 274 — "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети").

Авторам не известны отечественные аппаратно-программные продукты общего назначения, повышающие доступность систем (равно как и организации, занимающиеся разработкой таких продуктов). Имеющиеся зарубежные решения не везде применимы и весьма дороги, что существенно сужает круг возможных российских покупателей.

Целостность

Целостности повезло больше, чем доступности. Как уже отмечалось, различные аспекты целостности курируют ФАПСИ и Гостехкомиссия. Вышеупомянутая глава 28 УК предусматривает наказания за нарушение целостности. Есть отечественные продукты, обеспечивающие или контролирующие целостность.

В то же время, положение дел с целостностью далеко от идеала. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен. Пример области применения средств контроля динамической целостности — анализ потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность

Конфиденциальность — самый проработанный у нас в стране аспект информационной безопасности. На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб. Отечественные аппаратно-программные продукты позволяют закрыть практически все потенциальные каналы утечки информации.

К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить полное представление о потенциальных рисках и степени их серьезности. Во-вторых, авторам не известны отечественные аппаратные реализации шифраторов с достаточным быстродействием, что накладывает ограничения на виды и объемы шифруемой информации. Программные разработки охватывают лишь часть распространенных компьютерных платформ.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного (законы, нормативные акты, стандарты и т.п.);
- административного (действия общего характера, предпринимаемые руководством организации);
- процедурного (конкретные меры безопасности, имеющие дело с людьми);

- программно-технического (конкретные технические меры).

Программно-технический уровень

Львиная доля активности в области информационной безопасности приходится на программно-технический уровень. Если иметь в виду зарубежные продукты, здесь существует полный спектр решений. Если ограничиться разработками, имеющими российские сертификаты по требованиям безопасности, картина получается существенно более разреженной.

Согласно современным воззрениям, в рамках информационных систем должны быть доступны по крайней мере следующие механизмы безопасности:

- идентификация и проверка подлинности (аутентификация) пользователей;
- управление доступом;
- протоколирование и аудит;
- криптография;
- (межсетевое) экранирование;
- обеспечение высокой доступности.

Кроме того, информационной системой в целом и механизмами безопасности в особенности необходимо управлять. И управление, и механизмы безопасности должны функционировать в разнородной, распределенной среде, построенной, как правило, в архитектуре клиент/сервер. Это означает, что упомянутые средства должны:

- опираться на общепринятые стандарты;
- быть устойчивыми к сетевым угрозам;
- учитывать специфику отдельных сервисов.

В соответствии с действующим в России порядком, за идентификацию/аутентификацию, управление доступом, протоколирование/аудит отвечает Гостехкомиссия России, за криптографию — ФАПСИ, межсетевое экранирование является спорной территорией, доступностью не занимается никто.

На сегодняшний день подавляющее большинство разработок ориентировано на платформы Intel/DOS/Windows. В то же время, наиболее значимая информация концентрируется на иных, серверных платформах. В защите нуждаются не отдельные персональные компьютеры, не только локальные сети на базе таких компьютеров, но, в первую очередь, существенно более продвинутые современные корпоративные системы. Пока для этого почти нет сертифицированных средств.

Рассмотрим типичную государственную организацию, имеющую несколько производственных площадок, на каждой из которых могут находиться критически важные серверы, в доступе к которым нуждаются работники, базирующиеся на других площадках, и мобильные пользователи. В число поддерживаемых информационных сервисов входят файловый и почтовый сервисы, системы управления базами данных (СУБД), Web-сервис и т.д. В локальных сетях и при межсетевом доступе основным является протокол TCP/IP. Схематически информационная система такой организации представлена на Рис. 1.

Рисунок 1. Информационная система типичной государственной организации.

Для построения эшелонированной обороны подобной информационной системы необходимы по крайней мере следующие защитные средства программно-технического уровня:

- межсетевые экраны (разграничение межсетевого доступа);
- средства поддержки частных виртуальных сетей (реализация защищенных коммуникаций между производственными площадками по открытым каналам связи);
- средства идентификации/аутентификации, поддерживающие концепцию единого входа в сеть (пользователь один раз доказывает свою подлинность при входе в сеть организации, после чего получает доступ ко всем имеющимся сервисам в соответствии со своими полномочиями);
- средства протоколирования и аудита, отслеживающие активность на всех уровнях — от отдельных приложений до сети организации в целом, оперативно выявляющие подозрительную активность;
- комплекс средств централизованного администрирования информационной системы организации;
- средства защиты, входящие в состав приложений, сервисов и аппаратно-программных платформ.

На данный момент из интересующего нас спектра продуктов были сертифицированы по требованиям безопасности для применения в госорганизациях ряд межсетевых экранов, операционных систем и реляционных СУБД. Даже если включить в этот перечень продукты, сертифицированные ФАПСИ для применения в коммерческих организациях (систему "ШИП", поддерживающую виртуальные частные сети, и средства криптографической защиты семейства "Верба"), большинство рубежей остается без защиты.

Таким образом, на сегодняшний день государственная организация не может получить современную информационную систему, защищенную сертифицированными средствами.

Коммерческие структуры, в отличие от госорганизаций, в определенной степени свободнее в своем выборе защитных средств. Тем не менее, в силу целого ряда обстоятельств (необходимость взаимодействия с госструктурами, расширительная трактовка понятия гостайны — "гостайна по совокупности", необходимость получения лицензии на эксплуатацию криптосредств, ограничения на импорт криптосредств) эта свобода не слишком велика. Практически на все категории субъектов информационных отношений перенесен подход, рассчитанный на госструктуры.

Таковы два основных, на мой взгляд, измерения, задающие систему координат в пространстве информационной безопасности. У информационной безопасности есть и другие грани, но, чтобы чрезмерно не усложнять карту, мы оставим ее двумерной.

Мы описали двумерное пространство информационной безопасности. Представим результаты наших рассмотрений в наглядной форме, расставив оценки (от 0 до 5), показывающие степень освоенности различных областей в соответствии с современными требованиями и действующим законодательством

Оценка положения дел в информационной безопасности России.

	Доступность	Целостность	Конфиденциальность
законодательный уровень	1	2	3
административный уровень	0	0	1
процедурный уровень	0	1	2
программно-технический уровень	0	1	2

Информационная безопасность в России развивается крайне неравномерно. Есть давно освоенные области (законодательство о лицензировании и сертификации, программно-технические меры обеспечения конфиденциальности и статической целостности), но большая часть областей, в том числе критически важных, остается белым пятном. Даже на освоенных областях пока не удалось достичь соответствия современным требованиям. Все это позволяет оценить ситуацию с информационной безопасностью в России как крайне тяжелую. Позитивные перемены происходят очень медленно, так что общее отставание от современного уровня продолжает накапливаться.

В то же время, при правильной организации дела положение можно кардинально улучшить в короткие сроки. Объективно все заинтересованные стороны выиграют от проведения комплексного, современного подхода. Необходима, однако, государственная программа самого высокого уровня, координирующая, направляющая и контролирующая ход работ в области информационной безопасности.