**Доклад 3. Меры и средства обеспечения информационной безопасности**

Существуют два подхода к проблеме обеспечения безопасности компьютерных систем и сетей: фрагментарный и комплексный.

***Фрагментарный подход*** направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управ­ления доступом, автономные средства шифрования, специализиро­ванные антивирусные программы и т. п.

Достоинством такого подхода является высокая избиратель­ность к конкретной угрозе. Существенным недостатком данного подхода является отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечи­вают защиту конкретных объектов информационной системы (ИС) только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффектив­ности защиты.

***Комплексный подход*** ориентирован на создание защищенной среды обработки информации в информационной системе (ИС), объединяющей в единый ком­плекс разнородные меры противодействия угрозам. Организация за­щищенной среды обработки информации позволяет гарантировать определенный уровень безопасности ИС, что является несомненным достоинством комплексного подхода. К недостаткам этого подхода относятся: ограничения на свободу действий пользователей КС, чув­ствительность к ошибкам установки и настройки средств защиты, сложность управления.

Комплексный подход применяют для защиты ИС крупных ор­ганизаций или небольших ИС, выполняющих ответственные зада­чи либо обрабатывающих особо важную информацию. Нарушение безопасности информации в ИС крупных организаций может нанести огромный материальный ущерб как самим организациям, так и их клиентам. Поэтому такие организации вынуждены уделять особое внимание гарантиям безопасности и реализовывать комплексную защиту. Комплексного подхода придерживается большинство госу­дарственных и крупных коммерческих предприятий и учреждений. Этот подход нашел свое отражение в различных стандартах.

Комплексный подход к проблеме обеспечения безопасности ос­нован на разработанной для конкретной ИС политике безопасности. Политика безопасности регламентирует эффективную работу средств защиты ИС. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуаци­ях. Надежная система безопасности сети не может быть создана без эффективной политики сетевой безопасности.

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

* законодательного (стандарты, законы, нормативные акты и т. п.);
* административно-организационного (действия общего ха­рактера, предпринимаемые руководством организации, и конкретные меры безопасности, касающиеся людей);
* программно-технического (конкретные технические меры).

*Меры законодательного уровня* очень важны для обеспечения информационной безопасности. К этому уровню можно отнести весь комплекс мер, направленных на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности. Большинство людей не совершает противоправных действий потому, что это осуждается и/или наказывается обществом, и потому, что так поступать не при­нято. Информационная безопасность – это новая область деятель­ности, здесь важно не только запрещать и наказывать, но и научить, разъяснить, помочь. Общество должно осознать важность этой об­ласти, понять основные пути решения соответствующих проблем. Государство может сделать это оптимальным образом. Здесь не нужно больших материальных затрат, требуются интеллектуальные вло­жения.

*Меры административно-организационного уровня.* Администра­ция организации должна сознавать необходимость поддержания ре­жима безопасности и выделения на эти цели соответствующих ре­сурсов. Основой мер защиты административно-организационного уровня являются политика безопасности и комплекс организаци­онных мер. Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на за­щиту информации и ассоциированных с ней ресурсов организации.

К комплексу организационных мер относятся меры безопас­ности, реализуемые людьми. Можно выделить следующие группы организационных мер:

* управление персоналом;
* физическая защита;
* поддержание работоспособности;
* реагирование на нарушения режима безопасности;
* планирование восстановительных работ.

Для каждой группы в каждой организации должен существовать набор регламентов, определяющих действия персонала.

Для поддержания режима информационной безопасности осо­бенно важны меры программно-технического уровня, поскольку ос­новная угроза компьютерным системам исходит от них самих: сбои оборудования, ошибки программного обеспечения, промахи пользо­вателей и администраторов и т. п.

*Меры и средства программно-технического уровня.* В рамках современных информационных систем должны быть доступны по крайней мере следующие механизмы безопасности:

* идентификация и проверка подлинности пользователей;
* управление доступом;
* протоколирование и аудит;
* криптография;
* экранирование;
* обеспечение высокой доступности.

*Необходимость применения стандартов.* Информационные си­стемы компаний почти всегда построены на основе программных и аппаратных продуктов различных производителей. Дело в том, что на данный момент нет ни одной компании-разработчика, которая предо­ставила бы потребителю полный перечень средств (от аппаратных до программных) для построения современной ИС. Чтобы обеспечить в разнородной ИС надежную защиту информации, требуются специа­листы высокой квалификации, которые будут отвечать за безопасность каждого компонента ИС: правильно их настраивать, постоянно отсле­живать происходящие изменения, контролировать работу пользова­телей. Очевидно, что чем разнороднее информационная система, тем сложнее обеспечить ее безопасность. Изобилие в корпоративных сетях и системах устройств защиты, межсетевых экранов, шлюзов и VPN, а также растущий спрос на доступ к корпоративным данным со стороны сотрудников, партнеров и заказчиков приводят к созданию сложной среды защиты, трудной для управления, а иногда и несовместимой.

Интероперабельность продуктов защиты является важным тре­бованием для большинства корпоративных информационных систем.

***Интероперабельность - это способность открытых систем использовать программы, выполняющиеся одновременно на различных платформах в общей сети, с возможностью обмена информацией между ними. Иначе говоря, программные компоненты системы, расположенные на разных аппаратных платформах в общей сети, должны быть способны работать как часть единой системы.***

Для большинства гетерогенных информационных сред важно обеспечить согласованное взаимодействие с продуктами других производителей. Принятое ор­ганизацией решение безопасности должно гарантировать защиту на всех платформах в рамках этой организации. Поэтому вполне оче­видна потребность в применении единого набора стандартов постав­щиками средств защиты, компаниями – системными интегратора­ми и организациями, выступающими в качестве заказчиков систем безопасности для своих корпоративных сетей и систем.

Стандарты образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности, и опре­деляют критерии управления безопасностью. Стандарты являются необходимой базой, обеспечивающей совместимость продуктов раз­ных производителей, что чрезвычайно важно при создании систем сетевой безопасности в гетерогенных средах.

Комплексный подход к решению проблемы обеспечения безопас­ности, рациональное сочетание законодательных, административно­-организационных и программно-технических мер и обязательное следование промышленным, национальным и международным стан­дартам являются тем фундаментом, на котором строится вся система защиты информационных систем.

Для поиска решений проблем информационной безопасности при работе в сети Интернет был создан независимый консорциум ISTF (Internet Security Task Force) – общественная организация, состоящая из представителей и экспертов компаний-поставщиков средств информационной безопасности, электронного бизнеса и про­вайдеров интернет-инфраструктуры. Цель этого консорциума – раз­работка технических, организационных и операционных руководств по безопасности деятельности в Интернете.

Консорциум ISTF выделил двенадцать областей информацион­ной безопасности, на которых в первую очередь должны сконцент­рировать свое внимание создатели электронного бизнеса, чтобы обес­печить его работоспособность. Этот список, в частности, включает следующие пункты:

* аутентификация (механизм объективного подтверждения идентифицирующей информации);
* право на частную, персональную информацию (обеспечение конфиденциальности информации);
* определение событий безопасности (Security Events);
* защита корпоративного периметра;
* определение атак;
* контроль за потенциально опасным содержимым (Malicious Content);
* контроль доступа;
* администрирование;
* реакция на события (Incident Response).

Рекомендации ISTF предназначены для существующих или вновь образуемых компаний электронной коммерции и электронно­го бизнеса. Эти рекомендации помогают определить потенциальные бреши в их компьютерных сетях, которые, если не обратить на них должного внимания, могут использоваться взломщиками. Это может привести к атакам на систему электронной коммерции, потрясениям и даже к крушению электронного бизнеса. Консорциум ISTF настоя­тельно рекомендовал воспользоваться его наработками еще до начала организации компании, намеревающейся заняться электронной ком­мерцией и бизнесом.

Реализация рекомендаций консорциума ISTF означает, что защита информации в системе электронного бизнеса должна быть комплексной.

Для комплексной защиты от угроз и гарантии экономически вы­годного и безопасного использования коммуникационных ресурсов для электронного бизнеса необходимо решить следующие задачи:

* проанализировать угрозы безопасности для системы элект­ронного бизнеса;
* разработать политику информационной безопасности;
* защитить внешние каналы передачи информации, обеспечив конфиденциальность, целостность и подлинность передавае­мой по ним информации;
* гарантировать возможность безопасного доступа к откры­тым ресурсам внешних сетей и Интернета, а также общения с пользователями этих сетей;
* защитить отдельные наиболее коммерчески значимые ин­формационные системы независимо от используемых ими каналов передачи данных;
* предоставить защищенный удаленный доступ персонала к информационным ресурсам корпоративной сети;
* обеспечить надежное централизованное управление сред­ствами сетевой защиты.

Согласно рекомендациям, ISTF и классификации «рубежей обороны» Hurwitz Group, первым и важнейшим этапом разработки системы информационной безопасности электронного бизнеса явля­ются механизмы управления доступом к сетям общего пользования и из них, а также механизмы безопасных коммуникаций, реализуе­мые межсетевыми экранами и продуктами частных защищенных вир­туальных сетей (VPN).



Сопровождая их средствами интеграции и управления всей ключевой информацией системы защиты (PKI – инфраструктура открытых ключей), можно получить целостную, централизованно управляемую систему информационной безопасности.

Следующий рубеж включает в себя интегрируемые в общую структуру средства контроля доступа пользователей в систему вместе с системой однократного входа и авторизации (Single Sign-On).

Антивирусная защита, средства аудита и предотвращения атак, по существу, завершают создание интегрированной целостной систе­мы безопасности, если речь не идет о работе с конфиденциальными данными. В этом случае потребуются также средства криптографи­ческой защиты данных и электронно-цифровой подписи.

Для реализации основных функциональных компонентов систе­мы безопасности для электронного бизнеса применяются различные методы и средства защиты информации:

* защищенные коммуникационные протоколы;
* средства криптографии;
* механизмы аутентификации и авторизации;
* средства контроля доступа к рабочим местам сети и из сетей общего пользования;
* средства борьбы с вредоносными программами и спамом;
* программы обнаружения и предотвращения атак;
* средства централизованного управления контролем доступа пользователей, а также безопасного обмена пакетами данных и сообщениями любых приложений по открытым сетям.

Применение комплекса средств защиты на всех уровнях корпо­ративной системы позволяет построить эффективную и надежную систему обеспечения информационной безопасности.