**Безопасность компании в повседневной деятельности**

Работа по обеспечению безопасности требует в первую очередь взвешенных управленческих действий в различных направлениях, согласованных по времени, продолжительности и объему затрат ресурсов. Чтобы такая деятельность была целеустремленным движением вперед, а не представляла собой хаотические порывы без смысла и понятной цели, необходим общий фундамент. Важно преподнести работу по повышению безопасности не как личный произвол начальника, вызванный внезапным "озарением", а как обоснованные и направленные действия на основе четко проработанной нормативной базы. Начальственный произвол от нормальной управленческой деятельности отличается тем, что первый основывается на волевом решении руководителя, а вторая имеет в качестве базы определенный свод правил, по которым живут все без исключения сотрудники и руководители организации. Создание системы безопасности или даже попытки повлиять на ее развитие требуют минимальных знаний о сути обсуждаемых вопросов. Эта область деятельности сама по себе очень логична и структурирована, поэтому при усвоении базовых принципов ориентироваться в проблеме вам будет гораздо проще. Рассмотрим основу основ системы безопасности - ее нормативную базу, а по ходу изложения приведем примеры, которые пояснят суть некоторых вопросов, непосредственно касающихся работы с персоналом.

Нормативная база должна быть представлена пакетом из нескольких основных документов. Взгляды на этот счет у различных авторов различаются. Как первоочередные чаще всего упоминаются следующие документы.

Концепция безопасности, описывающая общие принципы и подходы к организации системы безопасности. Этот документ должен быть основательно проработан и обязательно утвержден руководством организации.

Стандарты безопасности, в которых разъясняются основные понятия, определения, термины, строятся модели систем организации, дается набор признаков и показателей безопасного состояния объектов и систем. Например, транспортное средство обеспечивает безопасную перевозку грузов, если эксплуатируется в соответствии с рядом требований, в соответствующем порядке проходит техобслуживание и имеет свидетельство о прохождении техосмотра. Подобные описания должны быть составлены для основных объектов и подсистем организации.

Процедуры безопасности. В этом документе указывается, что следует делать в данной организации для того, чтобы уровень информационной безопасности соответствовал определенному принятому стандарту.

Методы безопасности. Этим понятием обозначают документы для конечных пользователей и рядовых сотрудников, подробные инструкции к действиям. Например, инструкцию по резервному копированию личных данных в выделенную для каждого сотрудника папку на сервере.

Аварийный план. Документ, который описывает действия в случае нанесения какого-либо существенного ущерба организации, а также действия по восстановлению ее нормальной деятельности. Подробно и развернуто суть этого понятия описывается в специальной литературе и статьях по обеспечению непрерывности бизнеса. Если попытаться изложить смысл этого понятия упрощенно, то в аварийном плане должен быть представлен подробный ответ на вопрос: "Что делать, если...". Например, что делать, если вышла из строя офисная мини-АТС? Что делать, если случился пожар? Кто отвечает за восстановление работоспособности локальной сети и какими именно ресурсами обеспечен этот сотрудник? В качестве примера можно привести одну из российских компаний. В результате пожара ее помещения выгорели полностью, но спустя несколько дней работа возобновилась, причем в нормальном режиме. Мало того, этот случай стал своеобразной рекламой самой фирме, показав надежность ее работы партнерам и заказчикам.

Остановимся более подробно на концепции безопасности. Если описать ее суть коротко, то она определяет следующие моменты:

* + - что является целями и задачами безопасности;
  + - что защищает и с кем взаимодействует организация;
  + - от чего защищается организация;
  + - с помощью чего защищается организация;
  + - каким образом осуществляется защита;
  + - как управляется система безопасности и как контролируется ее эффективность.

Целью обеспечения безопасности может быть, например, обеспечение устойчивого круглосуточного сервиса для пользователей услугами компании, а задачей - учет ресурсов компании, позволяющих достичь этой цели, внедрение технологий гибкого управления этими ресурсами.

К объектам защиты относят:

* + - персонал и руководство;
  + - материальные и нематериальные активы;
  + - информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иную конфиденциальную информацию на любых материальных носителях, базы данных, программное обеспечение, информативные физические поля различного характера;
  + - средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телеграфной, телефонной, факсимильной, радио- и космической связи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);
  + - технические средства и системы охраны и защиты материальных и информационных ресурсов.

Обратите внимание на выделенные пункты. К защищаемым объектам относят информацию в различном виде, средства ее обработки, а также саму систему защиты. Далее исходя из фактора уязвимости, степени возможного ущерба и важности все объекты, в отношении которых могут быть осуществлены угрозы безопасности (посягательства физических или юридических лиц, стихийные бедствия), должны быть разделены по уровням уязвимости и степени риска. Также необходимо описать угрозы и их источники, соответствующие объектам.

Например, для фермерского хозяйства объектом защиты будут посевы, а источниками угрозы - климатические отклонения и их проявления (засуха, паводок). Для промышленной компании это, скорее, оборудование, дорогостоящее сырье, продукция на стадии транспортировки, а источники угрозы - криминальные группировки, политическая нестабильность в стране, поставляющей редкое сырье, и т.д.

Для банка уязвимость могут представлять финансовые средства (особенно в процессе транспортировки), информационные ресурсы и люди, занимающие руководящие должности, как объекты посягательств со стороны злоумышленников.

Вообще, к источникам угроз может относиться все, начиная от падения покупательской способности до эпидемии гриппа в офисе.

В статье Анатолия Брединского "Концепция безопасности коммерческого банка" приводится список угроз для сотрудников банка:

* + - похищения и угрозы похищения сотрудников, членов их семей и близких родственников;
  + - убийства, сопровождаемые насилием, издевательствами и пытками;
  + - психологический террор, угрозы, запугивание, шантаж, вымогательство;
  + - нападение с целью овладения денежными средствами, ценностями и документами.

Финансовой деятельности организации могут угрожать:

* + - экономические кризисы;
  + - неисполнение обязательств контрагентами;
  + - возможный произвол контрольных органов в стране пребывания;
  + - хищение материальных средств, продукции или сырья непосредственно с территории организации;
  + - мошенничество партнеров;
  + - внезапное изменение законодательной базы государства пребывания или таможенной политики.

Для информационной безопасности представляют угрозу:

* + - разглашение информации, составляющей коммерческую тайну;
  + - несанкционированный доступ к закрытым информационным ресурсам конкурентов либо криминальных структур;
  + - утечка информации по техническим каналам утечки (побочные электромагнитные излучения, акустические колебания, электромагнитные наводки в проводных сетях);
  + - намеренное или случайное повреждение данных в электронном или бумажном виде, случайное или намеренное искажение информации;
  + - недоступность такого рода данных, например в случае выхода из строя или хищения компьютерной техники;
  + - ведение в отношении организации активных мероприятий в информационном поле (информационно-психологическая война с возможным "вбросом" компрометирующих данных) с целью нанесения ущерба деловой репутации организации, ее руководству, изменения его рыночной стоимости для последующего поглощения или устранения.

Зданиям, сооружениям, имуществу организации могут угрожать:

* + - стихийные бедствия и их последствия;
  + - технические аварии;
  + - пожары;
  + - поджоги;
  + - хулиганские действия по отношению к зданию, оборудованию, ограждениям и декоративным элементам;
  + - пикетирование, блокирование входов и выходов из здания, въездов и выездов с территории;
  + - поджоги;
  + - нанесение ущерба транспортным средствам и т.д. и т.п.

Набор "фирменных" источников угроз для каждого предприятия уникален.

Чем защищается организация?

Здесь нужно определить меры обеспечения требуемого уровня безопасности, например:

1. Правовые.

2. Организационные (административные).

3. Инженерно-технические и программно-технические.

Любые действия, в том числе по собственной защите, ведутся в правовом поле. Далее, на административном уровне, определяется, что будет защищаться и каким именно образом. Технические меры принимаются уже на последнем этапе и на основании правовой базы, определения угроз и их источников, объектов защиты, политики безопасности организации.

Бытует мнение, что этим занимается исключительно соответствующая служба. Отчасти, конечно, это так. Но выше мы привели список угроз, в который входит масса явлений, находящихся в компетенции различных специалистов. Кроме того, есть вероятность появления новых угроз, ранее не предусмотренных. Специалист по безопасности не волшебник и во всех вопросах ориентироваться не может, поэтому не стоит ждать от него чуда. Наоборот, необходимо помочь ему силами всего коллектива. Решение целого ряда рутинных вопросов в своих узких областях могут взять на себя сотрудники и начальники отделов. Это целесообразно по следующим причинам:

* + - некоторые правила будут приниматься с обсуждением или вообще по инициативе рядовых сотрудников, что частично снимет проблему напряженности в отношениях и отторжения указаний службы безопасности;
  + - у сотрудников службы безопасности будет больше времени для работы "на перспективу", в противном случае погрязшие в рутине работники этой службы сами будут представлять угрозу для организации.

Роль службы безопасности во взаимодействии с персоналом заключается в том, что она обеспечивает общее регулирование деятельности в своем направлении, консультирует и обучает персонал определенной системе работы, а также контролирует выполнение положений и требований внутренней нормативной базы.

Отсюда вытекает необходимость интегрирования правил безопасной работы в описание процедур, регламенты, правила внутреннего распорядка, должностные обязанности и т.д.

Например, инструкции PR-менеджера могут содержать:

* + - перечень информации, которая не должна публиковаться;
  + - порядок публикации информации, относящейся к сфере интересов компании;
  + - инструкцию, описывающую порядок взаимодействия со СМИ и их представителями;
  + - описание информационной политики организации и т.д.

В пакете документов, определяющих работу отдела автоматизации, могут быть документы, описывающие:

* + - процедуры резервного копирования данных;
  + - требования безопасности к программному обеспечению;
  + - порядок действий при нештатных ситуациях и т.д.

Безусловно, достаточно стабильная работа по защите компании возможна только тогда, когда есть структура, которая эту работу обеспечивает. Практика показывает, что до того момента, пока такая структура или группа ответственных сотрудников не создана, все работы по обеспечению безопасности неизбежно заканчиваются на этапе обследования текущей ситуации.

В том случае, когда нет возможности обеспечить выделение нескольких сотрудников для нужд безопасности, можно создать рабочую группу из наиболее компетентных в своих областях штатных сотрудников других отделов.

Возможно, им потребуется пройти отдельное обучение или хотя бы прослушать краткий курс, чтобы ориентироваться в вопросах безопасности. Каждый из них будет курировать вопросы, относящиеся к его кругу обязанностей, под общим руководством и контролем единственного сотрудника службы безопасности.

Как и любая деятельность, работа по созданию, развитию и поддержке системы безопасности требует планирования и выделения средств. Это условие самое важное. Если оно не соблюдается, об эффективной службе и системе безопасности можно забыть. Все приложенные усилия окажутся простой тратой денег и времени. Что касается человеческого фактора, то при распределении обязанностей между сотрудниками стоит придерживаться определенных правил и "не складывать все яйца в одну корзину". Например, администратор сети не может и не должен выполнять обязанности администратора безопасности. Причины просты, но редко принимаются в расчет руководителями.

Причина первая. У администратора сети и администратора безопасности противоположные задачи. Задача одного - обеспечить комфортную и прозрачную среду для работы и предоставить все необходимые сервисы пользователям. Задача второго - ограничить доступ к сети так, чтобы пользователи не имели доступа к ресурсам, которые им не нужны для выполнения производственных обязанностей.

Причина вторая. Вспомните известное изречение: "Кто будет сторожить сторожей?". В самом деле в организации системный администратор - царь и бог всех электронных ресурсов. Реально он имеет доступ ко всем ресурсам сети и всей информации. Контролировать его действия руководству практически невозможно.

В этом случае на выручку приходит администратор безопасности. Сам он не должен иметь доступа к данным, так же как и не должен иметь возможности что-либо менять в настройках программного, аппаратного обеспечения или в содержимом баз данных. Но у него должен быть доступ на просмотр всех "бюджетов" пользователей, протоколов работы оборудования и программного обеспечения, а также на просмотр файловой структуры.

Он контролирует регулярность проведения положенных процедур (например, резервного копирования), соблюдение парольных политик, а также действия пользователей.

Аналогичным образом следует организовать работу и в других случаях. Например, чтобы затруднить кражу информации, можно поступить следующим образом. Закрытая база данных в зашифрованном виде хранится на съемном жестком диске. Утром, перед началом работы, один сотрудник подключает диск, второй, пользуясь аппаратным электронным ключом, начинает процедуру работы с диском, третий набирает пароль для доступа к информации. Существующие программы шифрования позволяют организовать такой режим работы. В результате ни один сотрудник по отдельности не сможет воспользоваться содержимым диска, а сговориться об этом втроем гораздо сложнее. Получается, что организация застрахована и от сговора сотрудников, и от последствий давления криминальных структур на одного из них, и от кражи техники из офиса накануне сдачи годового баланса.

Вопрос управления службой безопасности достаточно объемен и включает в себя несколько составляющих. Здесь стоит упомянуть о том, что главными принципами управления системой безопасности являются принципы единоначалия и неукоснительного подчинения всех принятым правилам. Что касается общей схемы работы, то она циклична и в упрощенном виде представляет собой цепочку. Принцип единоначалия подразумевает четкую иерархию управления в различных ситуациях. Второй принцип гласит о том, что принятым правилам должны следовать как рядовые сотрудники, так и руководители организации.

Кроме того, служба безопасности должна быть подчинена непосредственно высшему руководству. Переподчинение ее какому-либо из заместителей высшего руководителя (например, по юридическим вопросам) недопустимо. Залог успешной деятельности службы безопасности - максимально возможная независимость от должностных лиц. Мало кто задумывается, что опасность для организации, исходящая от сотрудника, прямо пропорциональна занимаемому им положению.

Очень важен вопрос взаимодействия с другими службами или подразделениями. Для того чтобы снять вопросы полномочий при совместной работе над решением задач в смежных областях, необходимо описать, кто, кому и в каких случаях подчинен.

Вопрос достаточно сложный и субъективный. Сложен он потому, что необходимо количественно оценить качественные изменения, а необъективен в силу изначальной субъективности оценки важности активов организации - материальных и нематериальных. Как, например, можно оценить тот факт, что сотрудники стали втрое реже терять служебные документы? Количественно - трудно. Качественно - оценка не так наглядна. Тем не менее выводы, имеющие сравнительный характер, сделать можно. Например, подсчитав время простоя серверов за 2-3 месяца или попытавшись сопоставить какие-то действия службы безопасности с ростом прибыли. Чего уж точно не следует делать, так это требовать сиюминутных результатов в виде пойманных за руку сотрудников-вредителей. Наоборот, в случае "роста показателей" необходимо задуматься, откуда берутся злоумышленники и что их толкает на вредоносные действия.

Оценивать стоит скорее тенденции, которые развиваются в организации. И только в отдельных случаях можно оценивать сумму предотвращенного ущерба. Это возможно, если оценены все активы предприятия и определен хотя бы порядок сумм возможного ущерба. Исходя из этих цифр можно принимать решения об увеличении или уменьшении бюджета или судить об эффективности службы безопасности.

Работа по обеспечению безопасности требует взвешенных, обоснованных управленческих действий, поэтому она должна строиться с соблюдением определенных базовых принципов. Продолжением базовых принципов обеспечения безопасности деятельности должен быть пакет документов, четко определяющий все организационные связи и полномочия лиц, а также понятия безопасного и небезопасного состояния и требования безопасности. Этот пакет документации индивидуален для каждого предприятия или организации из-за их различий в структуре, размерах, целях и т.д.

Не имеет смысла возлагать на службу безопасности абсолютно все задачи по защите предприятия. Функция службы безопасности скорее методическая, контрольная и консультирующая, а не исполнительская. Ее стратегические решения принимаются коллегиально с привлечением сотрудников соответствующих служб и отделов.

Любые шаги по созданию системы безопасности следует начинать одновременно с формированием постоянного коллектива ответственных сотрудников (как минимум на уровне постоянной рабочей группы).

Наконец, чем более интегрированы элементы системы безопасности в существующую структуру организации, тем эффективнее вся система в целом. Если мы говорим о нормативной базе в общем, то важнейшими моментами будут ее поддержка в актуальном состоянии и подробная проработка.

Можно с одинаковым успехом разработать и совершенно глупые, и абсолютно гениальные методики, планы и правила, но без поддержки рядовых сотрудников результат (а точнее, его отсутствие) будет одинаков. В конце концов именно за счет реализации способностей сотрудника на рабочем месте и развивается организация. При заключении трудового соглашения обе стороны - и сотрудник, и наниматель - налагают на себя массу сложных и взаимосвязанных обязательств, как формальных и подзаконных, так и лежащих в области морали. Поэтому целесообразно четко определить права и обязанности сторон в процессе трудовой деятельности.

Очень часто руководители не знают или забывают об одном из базовых принципов системы безопасности "защита всех от всех". Это означает, что система безопасности должна гарантировать определенные права и уровень безопасности не только организации по отношению к внешним или внутренним источникам угрозы, но и обеспечивать ее защиту от проблем, возникших из-за некомпетентности руководителя. На самом же деле угроза организации часто пропорциональна статусу, "весу" и полномочиям лица, являющегося ее источником.

По данным опросов, в частных компаниях утечка информации часто происходит в результате небрежности первых лиц организации. Более 75% менеджеров не считают нужным убирать конфиденциальные документы со стола или выключать монитор своего компьютера при приеме посетителей. Это приводит примерно к 30% случаев утечки информации. Если посчитать, на какое количество (а это считанные единицы в организации) таких лиц приходится 30% утечек, то наличие угрозы со стороны руководства будет доказано без труда. Следует учесть, что речь пока идет только об информационной безопасности.

По наиболее распространенному мнению, самый дешевый и эффективный способ повысить общий уровень информационной безопасности - это развивать и поддерживать высокий уровень информационной культуры и общей культуры делопроизводства. Всем известно, что чаще крадут (деньги или информацию - не столь важно) там, где царит безалаберность, необязательность и неразбериха. В этом случае труднее понять, что на самом деле произошло, труднее собрать фактический материал для внутреннего расследования. А злоумышленнику легче скрыть следы.

Поэтому необходимо добиваться от сотрудников понимания и четкой установки на совершенствование деловых качеств - аккуратности, пунктуальности, обязательности, методичности, дисциплинированности. В этом случае коллективу легче привить писаные и неписаные правила, которые непосредственно касаются защиты информации.

В большинстве западных компаний действует двухуровневая система внутренней безопасности. Первый уровень обеспечивается штатной службой безопасности. Второй обеспечивают сами сотрудники. Взаимодействие службы безопасности с коллективом обеспечивают координаторы из числа сотрудников промежуточного уровня.

Эффективность такой схемы в наших условиях вполне реальна. Однако необходимо создать определенную "прослойку" имеющих одинаковые принципы и этические нормы людей. В том случае, если численность этой группы окажется достаточно большой, вновь прибывшие сотрудники окажутся под давлением общепринятых в коллективе взглядов. Часто моральный аспект проблемы внутрифирменного мошенничества, хищений и т.д. недооценивается. Но идеологической работой заниматься необходимо, так как идеологическое поле не терпит пустоты. Если в организации не уделяется внимание формированию системы ценностей, их место может занять стихийная, суррогатная система.

Если все знают, что путь документа можно проследить в любой момент времени, что постоянно ведется выборочный контроль деловой переписки, что при совместной работе с информацией четко определены права и обязанности, желание мошенничать быстро сходит на нет. Рекомендуется объяснить сотрудникам, что такого рода контроль преследует своей целью процветание и стабильность фирмы, предупреждение ошибок в работе, формирование "чувства локтя".

По возможности, следует построить профили сотрудников. Для психологического профиля это совокупность показателей, описывающих личностные качества, тип поведения, ценностные приоритеты. Также можно составить профиль работы в информационной системе (порядок работы с приложениями и сетевыми ресурсами, Интернетом). В том случае, если имеется информация о существенном изменении каких-либо параметров поведения сотрудника, есть смысл как минимум побеседовать с ним или обратить на этого человека пристальное внимание. Для того чтобы не возникало возмущения со стороны работников, рекомендуется в один из подписываемых документов вписать пункт с формулировкой, похожей на приведенную (пример взят из книги И. Конеева и А. Белова "Информационная безопасность предприятия"): "Средства вычислительной техники, объекты информационного пространства и сама информационная сеть, включая программное, сетевое, организационное, нормативное обеспечение, являются собственностью организации и переданы сотрудникам организации во временное пользование для выполнения служебных обязанностей".

Кроме того, в прошлом номере мы говорили, что сотрудник при приеме на работу должен дать подписку о том, что его личность может стать объектом внимания службы безопасности. Каждый руководитель должен сам определить для себя этичность и целесообразность таких действий по отношению к сотрудникам. В конце концов на практике можно столкнуться с таким же грамотным подчиненным, потеряв в результате его доверие в лице возможного союзника и сторонника.

Вполне реально создание системы мотивации, которая обеспечивает безопасное поведение персонала и содержит следующие принципы:

* + - доступность (в идеале заработать проще, чем украсть);
  + - ощутимость (премия не менее 20% от оклада; оклад больше наиболее вероятного ущерба от воровства);
  + - минимальный разрыв между результатом труда и стимулирующей выплатой по времени;
  + - создание "разности потенциалов" за счет баланса мер наказания и поощрения;
  + - сочетание различных мер воздействия.

По совершенно объективным причинам новичок слабо представляет себе специфику своей новой работы. Конечно, его ввели в курс дела, ознакомили с будущими обязанностями. Но это не значит, что он сориентировался в новой обстановке. Поэтому необходим краткий курс обучения, знакомящий нового сотрудника с компанией и приводящий его поведение к "общему стандарту". В адаптационный период сотрудник знакомится с режимом работы, конфиденциальной информацией в организации, правилами поведения в типовых ситуациях, стратегией компании. Информация об организации, структуре управления, логике движения информационных потоков, о моральном кодексе сотрудников, памятка об основных правилах могут выдаваться в виде буклета.

Безусловно, до этого момента необходимо подписать с сотрудником соглашение о неразглашении сведений, составляющих коммерческую тайну, так как сами процедуры конфиденциального делопроизводства могут быть включены в перечень сведений, составляющих коммерческую тайну. Каждый сотрудник должен быть ознакомлен с теми частями Положения о коммерческой тайне, которые касаются лично его. Также необходимо разъяснить сотруднику все его обязанности в отношении сохранения коммерческой тайны, ответить на его вопросы. В конечном итоге у сотрудника должно сформироваться благоприятное мнение о службе безопасности, понимание обоснованности определенных правил и заведенного порядка. Работник должен быть твердо уверен, что при соблюдении четко определенных разумных требований и правил ему лично ничего не грозит, что главной функцией службы безопасности является предупредительная, а не карательная функция.

Например, стоит объяснить ценность для организации находящегося у сотрудника документа. Напомните, что при передаче конфиденциального документа он обязан взять расписку у того сотрудника, которому передается информация, или перерегистрировать документ на другое имя у секретаря. Поясните, что если документ будет утерян или разглашен, то эти несколько неудобные меры помогут определить степень его виновности или невиновности в этом неприятном инциденте. Необходимо рассказать о важной воспитательной роли, которая отводится правилам работы с документами, о повышении общей культуры и организованности работы в результате принятия этих правил. И конечно, не стоит забывать старую пословицу: "Повторение - мать учения". Все инструктажи и тренинги необходимо периодически повторять, проверять знания сотрудников на предмет знания ими правил и регламентов деятельности организации.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003.
2. Ильин А.И., Синица Л.М. Планирование на предприятии. Мн., 2002.
3. Котлер Ф. Основы маркетинга. М., 1991.
4. Методические рекомендации по планированию, учету и калькулированию себестоимости продукции на промышленных предприятиях Министерства промышленности / Под ред. Л.Г. Сивчик. Мн., 1998.
5. Основные положения по разработке и применению систем сетевого планирования и управления. М., 1967.
6. Практикум по курсу «Экономика предприятий» / Под ред. В.Я. Хрипача. Мн., 1997.
7. Липсиц И.В. Бизнес-план - основа успеха. М., 1994.
8. Рекомендации по разработке бизнес-планов инвестиционных проектов. Утверждены Министерством экономики РБ 31.03.1999 г. / НЭГ, 1999, №37-39.
9. Организация и современные методы защиты информации / Под общей ред. Диева С.А., Шаваева А.Г. - М.: Концерн "Банковский деловой центр", 1998.