Лекция № 1.
Понятие информационной безопасности

Стремительное развитие компьютерной сферы и высоких технологий в последние два десятилетия привело к тому, что информация приобрела конкретные финансовые, репутационные, временные и экономические выражения. В связи с этим для большинства организаций защита информации становится одной из приоритетных задач.

В современных условиях информатизации общества одним из решающих факторов определяющих надежное функционирование и устойчивость любой организации является информационная безопасность.

Понятие "информация" (от лат. information) в прямом смысле означает осведомление, придание формы тому, что было ранее неизвестно. Информация является базовой составляющей знания. Знание, в свою очередь, накапливается и реализуется человеком в форме интеллектуального продукта. Иными словами, знание в отличие от информации представляет собой увеличивающийся, самовозрастающий ресурс в информационных процессах организации.

Определяющей основную роль информации в системе ресурсного обеспечения организации является утверждение, кто владеет информацией - тот владеет миром, и тогда становится понятна роль системы информационной безопасности организации не только сотрудникам служб информационной безопасности с целью обеспечения ее безопасности, но и руководящему звену организации при построении информационной системы. В этом случае информация рассматривается как система ресурсного управления разумной деятельностью человека в социальной, производственной и деловой сферах. Ее основная задача определяется как управление человеческим сознанием через мотивированную деятельность. Мотив это внутреннее состояние человека, детерминируемое внешней средой, в результате полученной и осознанно обработанной информации, к определенному виду деятельности. Мысль, мысле форма, мыследеятельность—рефлексия - деятельность.

Разумный человек сначала человек мысленно взвешивает аргументы, а затем уже переходит к осознанной деятельности. Разумна она или нет, определяется идеологией близкого по духу социального окружения. А также организационной культурой предприятия, его психологическим климатом, уровнем интеллекта руководителя и стилем его управленческой деятельности, уровнем компетентности.

Основная утечка информации чаще всего происходит в результате низкой компетентности первых лиц организации от недопонимания своей ответственности по созданию и управлению системой информационной безопасности. В частности, психологической защиты личности, как одного из элементов безопасности системы. Концепция информационной безопасности разрабатывается с позиций собственника, акционеров, руководителей

высшего звена управления в соответствии с целью и порядком решаемых задач. Мнения этих категорий лиц далеко не всегда совпадают с мотивационными составляющими сотрудников рядового звена, что в основном и приводит к межличностным конфликтам, в результате которых страдает вся система безопасности.

Обеспечивать информационную безопасность - значит осуществлять постоянную деятельность по выявлению, предупреждению, локализации и нейтрализации угроз и сведению к минимуму ущерба, в том числе и с учетом человеческого фактора.

На всех стадиях информационного процесса ведущая роль принадлежит человеку использующему информацию для практической реализации знаний. От того, как будут учтены в информационных процессах, психологические установки – мотиваторы, как свойства личности человека, а также личностные свойства сотрудника, сформированные социальными отношениями, зависит эффективность использования информации. Поэтому деятельность по обеспечению безопасности организации концентрируются на защите информационных ресурсов в векторе организации психологической безопасности с целью защиты человеческого ресурса (человеческого капитала) как от внутренних, так и внешних деструктивных воздействий социума. Психологическая безопасность организации - такое состояние системы информационно-психологических отношений, в котором система способна успешно, устойчиво и непрерывно развиваться в условиях интенсивного воздействия внешних и внутренних факторов, оказывающих на систему как стабилизирующее, так и деструктивное информационно-психологическое воздействие.

Организация как объект защиты представляет собой широкое понятие и включает в себя коллектив - свою основу. Коллектив - это объединение всех работников, осуществляющих совместную трудовую деятельность. Решающее влияние на настроение и функционирование организации оказывает коллектив. Так, сплоченность или конфликтность коллектива, его стабильность, уровень квалификации и сознательности работников, деловая активность, дисциплинированность - все это прямо определяет эффективность организации.

Таким образом, коллектив является социальной основой деловой организации. Сплоченный коллектив есть контактная и структурированная организация работников объединенных единой целью и решающих задачи в соответствии со свойственными каждому психофизиологическими ресурсами и предрасположенностью к определенному виду деятельности.

Организации относятся к числу сверхсложных систем и состоят из элементов и подсистем разной природы (технические, правовые, психологические, социокультурные), они многофункциональны (производят продукцию, услуги, формируют человека и среду). Для объекта такой сложности приходится строить и сложную методологию системного подхода.

Будучи элементом сверхсложной системы, человек как интеллектуальный ресурс, включенный в организацию, испытывает влияние

всей системы в целом. Управление системами, в которые включены люди, требует применять системный подход с законов психологии. Именно системный подход позволяет рассмотреть организацию как систему, созданную по принципу интеграции человеческих и технологических ресурсов. От этого происходит цепь производных принципов, главные из которых - целостность объекта и комплексность его анализа необходимого для построения системы безопасности.

Процесс построения системы представляет собой цепь взаимоувязанных процедур и процессов. Стоит отметить тот факт, что все необходимые процедуры и процессы, начиная от проведения аудита информационной инфраструктуры и заканчивая изучением психологического поведения сотрудников, составляют именно цепочку, то есть, при выпадении одного звена лишаются опоры последующие звенья.

Психология поведения сотрудников во многом определяется не только их личностными качествами, но и внутренней средой организации, условиями деятельности и другими внешними по отношению к человеку факторами. При определенных условиях каждый сотрудник может быть в той или иной степени «честным», «надежным», «порядочным» и он же, при других условиях, способен проявить противоположные качества.

Самая большая сложность здесь состоит в том, что законы, действующие в технике, отличаются от законов, работающих в психологии деятельности. Описание, типа: «Если на объект [А] воздействовать фактором [В], то получится расчетный результат [С]», вполне применимое к работе неживых систем, а при включении в них людей, приобретает несколько иной вид: «Если на что-то, что с определенной долей достоверности можно принять за (А) воздействовать чем-то похожим на (В), то вполне может быть, что получится результат, близкий к (С) относительно ваших перспективных ожиданий». Поведение человека в рамках одной стратегии регулируется исключительно его мотивами и управляется стимулирующими факторами. Переход от одной стратегии к другой регулируется системой мотивов. Внутренняя мотивация соответствует стратеги "максимум труда - максимум дохода", где поведение человека определяется видом деятельности, к которой он предрасположен. Сильные стороны как сумма ведущих функций определяются мотивацией к конкретному виду деятельности в векторе его способностей и наклонностей

Если во главу угла ставится система стимулирования, без учета мотивационных составляющих срабатывает стратегия "минимум труда - минимум дохода. Которая возникает, как вынужденная реакция человека на сложившуюся ситуацию, которая и формирует у работника чувства "внутреннего увольнения", подавленности, способствует становлению терминаторного, то есть разрушительного поведения и человек переходит уже в категорию инсайдера. Инсайдер - собственный персонал организации допущенный к основным ресурсам, который сможет нанести значительный ущерб организации своими несанкционированными действиями.

Повторяющиеся скандалы вокруг продажи на российском нелегальном рынке закрытых информационных баз, стабильно растущая проблема потери конфиденциальных данных в государственных учреждениях, крупных фирмах, а также и в банках, торговля инсайдерской информацией — все это реалии сегодняшнего дня. И вряд ли они объясняются только возросшей активностью и мастерством хакеров. Специалисты считают, что главная причина носит инсайдерский, «внутренний» характер.

Если и можно выделить какие-то типичные черты банковских и финансовых инсайдеров, то роднит их, пожалуй, лишь то, что в своих организациях работая на технических должностях, никогда не занимались атаками на уровне техники или хакерством и не подозревались как проблемные служащие.

- Возраст инсайдеров колеблется в широком диапазоне: от 18 до 59 лет. «Одиночек» больше, чем семейных (64% против 36%).
- Служебное положение самое разное: в обслуживании работали 36% инсайдеров, в администрации — 23%, в профильных подразделениях 19% и 22% — в технических службах.
- По мнению руководителей и коллег, очень немногие из инсайдеров были трудно управляемыми или не внушающими доверия .
- Правда, 20% инсайдеров коллеги воспринимали как людей «не в настроении».
- Необычное поведение перед инцидентом, обратившее на себя внимание начальства или коллег, продемонстрировали 37% инсайдеров. Кто-то жаловался на маленькую зарплату, другой слишком часто звонил из офиса по сотовому телефону. Были случаи отказа работать под началом нового руководителя или вспышки недовольства по отношению к коллегам, а то и некоторая «самоизоляция».
- Более четверти инсайдеров (30%) имели в прошлом неприятности, закончившиеся возбуждением уголовного дела.

Инсайдерские инциденты были обнаружены не только сотрудниками службы безопасности, но порой и людьми, не работавшими в организации.

- В 60% случаев инсайдеры были обнаружены лицами, не отвечающими за безопасность: потребителями — 25%, контролерами — 10%, прочим персоналом — 5%.

Теперь легко сделать вывод, что на первом месте уверенно просматривается кража информации собственными сотрудниками.

Самые крупные компании особо опасаются несанкционированных действий сотрудников, которые могут причинить вред организации, информационного саботажа со стороны бывших и нынешних служащих, промышленного шпионажа, утечки информации через мобильные устройства. И для компаний меньшего масштаба все эти угрозы также входят в TOP-10. Поэтому крупные предприятия планируют уделить большое внимание работе со своими служащими, чтобы научить их следовать политике информационной безопасности и избегать ошибок по невнимательности, халатности или крайне низкой компетентности.

На сегодняшний день видны опасности внутренних угроз, ясны и причины, по которым инсайдеры являются на сегодняшний день самой серьезной внутренней угрозой. Большое число утечек информации происходит по неосторожности или элементарной неграмотности сотрудников структурных подразделений, а также сотрудников склонных к воровству или нелояльных к руководству.