## Безопасность программного обеспечения и человеческий фактор.

##### 4.3. БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР. ПСИХОЛОГИЯ ПРОГРАММИРОВАНИЯ.

###### 4.3.1. Человеческий фактор

Преднамеренные и непреднамеренные нарушения безопасности программного обеспечения безопасности компьютерных систем большинство отечественных и зарубежных специалистов связывают с деятельностью человека. При этом технические сбои аппаратных средств КС, ошибки программного обеспечения и т.п. часто рассматриваются лишь как второстепенные факторы, связанные с проявлением угроз безопасности.

С некоторой степенью условности злоумышленников в данном случае можно разделить на два основных класса:

* злоумышленники-любители (будем называть их хакерами);
* злоумышленники-профессионалы.

Хакеры - это люди, увлеченные компьютерной и телекоммуникационной техникой, имеющие хорошие навыки в программировании и довольно любознательные. Их деятельность в большинстве случаев не приносит особого вреда компьютерным системам. Ко второму классу можно отнести отечественные, зарубежные и международные криминальные сообщества и группы, а также правительственные организации и службы, которые осуществляют свою деятельность в рамках концепции "информационной войны". К этому же классу можно отнести и сотрудников самих предприятий и фирм, ведущих разработку или эксплуатацию программного обеспечения.

Хакеры и группы хакеров

Хакеры часто образуют небольшие группы. Иногда эти группы периодически собираются, а в больших городах хакеры и группы хакеров встречаются регулярно. Но основная форма взаимодействия осуществляется через Интернет, а ранее - через электронные доски BBS. Как правило, каждая группа хакеров имеет свой определенный (часто критический) взгляд на другие группы. Хакеры часто прячут свои изобретения от хакеров других групп и даже от соперников в своей группе.

Существуют несколько типов хакеров. Это хакеры, которые:

* стремятся проникнуть во множество различных компьютерных систем (маловероятно, что такой хакер объявится снова после успешного проникновения в систему);
* получают удовольствие, оставляя явный след того, что он проник в систему;
* желают воспользоваться оборудованием, к которому ему запрещен доступ;
* охотятся за конфиденциальной информацией;
* собираются модифицировать определенный элемент данных, например баланс банка, криминальную запись или экзаменационные оценки;
* пытаются нанести ущерб "вскрытой" (обезоруженной) системе.

Группы хакеров, с некоторой степенью условности, можно разделить на следующие:

* группы хакеров, которые получают удовольствие от вторжения и исследования больших ЭВМ, а также ЭВМ, которые используются в различных государственных учреждениях;
* группы хакеров, которые специализируются на телефонной системе;
* группы хакеров - коллекционеров кодов - это хакеры, запускающие перехватчики кода, которые ищут карту вызовов (calling card) и номера PBX (private branch exchange - частная телефонная станция с выходом в общую сеть);
* группы хакеров, которые специализируются на вычислениях. Они используют компьютеры для кражи денег, вычисления номеров кредитных карточек и другой ценной информации, а затем продают свои услуги и методы другим, включая членов организованной преступности. Эти хакеры могут скупать у коллекционеров кодов номера PBX и продавать их за 200-500$, и подобно другим видам информации неоднократно. Архивы кредитных бюро, информационные срезы баз данных уголовного архива ФБР и баз данных других государственных учреждений также представляют для них большой интерес. Хакеры в этих группах, как правило, не находят взаимопонимания с другими хакерами;
* группы хакеров, которые специализируются на сборе и торговле пиратским программным обеспечением.

Типовой потрет хакера

Ниже приводится два обобщенных портрета хакера, один составлен по данным работы и характеризует скорее зарубежных хакеров-любителей, в то время как второй - это обобщенный портрет отечественного злонамеренного хакера, составленный Экспертно-криминалистическим центром МВД России.

В первом случае отмечается, что многие хакеры обладают следующими особенностями:

* мужчина: большинство хакеров - мужчины, как и большинство программистов;
* молодой: большинству хакеров от 14 до 21 года, и они учатся в институте или колледже. Когда хакеры выходят в деловой мир в качестве программистов, их программные проекты источают большую часть их излишней энергии, и корпоративная обстановка начинает менять их жизненную позицию. Возраст компьютерных преступников показан на рис.4.1;
* сообразительный: хакеры часто имеют коэффициент интеллекта выше среднего. Не смотря на свой своеобразный талант, большинство из них в школе или колледже не были хорошими учениками. Например, большинство программистов пишут плохую документацию и плохо владеют языком;
* концентрирован на понимании, предсказании и управлении: эти три условия составляет основу компетенции, мастерства и самооценки и стремительные технологические сдвиги и рост разнообразного аппаратного и программного обеспечения всегда будут вызовом для хакеров;

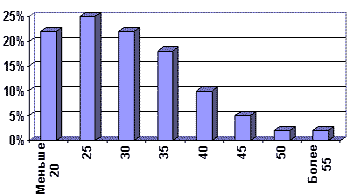


Рис. 4.1. Возрастное распределение обнаруженных компьютерных преступников

* увлечен компьютерами: для многих пользователей компьютер - это необходимый рабочий инструмент. Для хакера же - это "удивительная игрушка" и объект интенсивного исследования и понимания;
* отсутствие преступных намерений: по данным  лишь в 10% рассмотренных случаев компьютерной преступности нарушения, совершаемые хакерами, привели к разрушению данных компьютерных систем. В связи с этим можно предположить, что менее 1% всех хакеров являются злоумышленниками.

Обобщенный портрет отечественного хакера выглядит следующим образом: это мужчина в возрасте от 15 до 45 лет, либо имеющий многолетний опыт работы на компьютере, либо почти не обладающий таким опытом; в прошлом к уголовной ответственности не привлекался; является яркой, мыслящей личностью, способной принимать ответственные решения; хороший, добросовестный работник; по характеру нетерпимый к насмешкам и к потере своего социального статуса в рамках окружающей его группы людей; любит уединенную работу; приходит на службу первым и уходит последним; часто задерживается на работе после окончании рабочего дня и очень редко использует отпуска и отгулы.

Криминальные сообщества и группы, сценарий взлома компьютерной системы

В связи со стремительным ростом информационных технологий и разнообразных компьютерных и телекоммуникационных средств и систем, наблюдается экспоненциальный рост как количества компьютерных атак, так и объем нанесенного от них ущерба (см. табл.4.3). Это показали исследования, проведенные в 90-х гг. в США. Анализ показывает, что такая тенденция постоянно сохраняется.

За последнее время в нашей стране не отмечено ни одного компьютерного преступления, которое было бы совершено одиночкой. Более того, известны случаи, когда организованными преступными группировками нанимались бригады из десятков хакеров. Им предоставлялись отдельные охраняемые помещения, оборудованные самыми передовыми компьютерными средствами и системами для проникновения в компьютерные сети коммерческих банков (см. табл.4.4).

Специалисты правоохранительных органов России неоднократно отмечали тот факт, что большинство компьютерных преступлений в банковской сфере совершается при непосредственном участии самих служащих коммерческих банков. Результаты исследований, проведенных с привлечением банковского персонала, показывают, что доля таких преступлений приближается к отметке 70%. При осуществлении попытки хищения 2 млрд. рублей из филиала одного крупного коммерческого банка преступники оформили проводку фиктивного платежа с помощью удаленного доступа к компьютеру через модем, введя пароль и идентификационные данные, которые им передали сообщники из состава персонала этого филиала. Далее эти деньги были переведены в соседний банк, где преступники попытались снять их со счета, оформив поддельное платежное поручение.

По данным Экспертно-криминалистического центра МВД России принципиальный сценарий взлома защитных механизмов банковской компьютерной системы представляется следующим. Компьютерные злоумышленники-профессионалы обычно работают только после тщательной предварительной подготовки. Они снимают квартиру на подставное лицо в доме, в котором не проживают сотрудники ФСБ, МВД или МГТС. Подкупают сотрудников банка, знакомых с деталями электронных платежей и паролями, и работников телефонной станции, чтобы обезопасить себя на случай поступления запроса от службы безопасности банка. Нанимают охрану из бывших сотрудников МВД. Чаще всего взлом банковской компьютерной системы осуществляется рано утром, когда дежурный службы безопасности теряет свою бдительность, а вызов помощи затруднен.

Таблица 4.3

|  |  |
| --- | --- |
| **Год** | **События, цифры, факты** |
| 21.11. 1988 | Вирус Морриса на 24 часа вывел из строя сеть ARPANET. Ущерб составил98 млн. долларов. |
| 1989 | К. Митник подключился к одному из компьютеров ИВС объединенной системы ПВО Североамериканского континента (North American Air Defense Command) |
| 1989 | Группа хакеров MOD уничтожила почти всю информацию в компьютере, используемом корпорацией Educational Broadcasting Corp., общественной телевизионной станцией WNET, канал 13 в Нью-Йорке |
| 1990 | К. Нейдорф осуществил доступ к телефонную сеть системы 911 в девяти штатах США и получил конфиденциальную информациюв виде кодов доступа |
| 1994 | Национальная аудиторская служба Великобритании (National Audit Office - NAO) зарегистрировала 655 случаев НСД и 562 случая заражения вирусами компьютерных систем британских правительственных организаций, что в 1.4 и 3.5 раза соответственно превышает уровень 1993 г. |
| 1994 | В США ущерб от НСД к информационно-вычислительным ресурсам превысил $10 млрд. (в 1991 г. по оценкам USA Research $1.75 млрд.) |
| 1995 | В США из 150 проверенных исследовательских и производственных вычислительных комплексов 48% подверглись успешной реализации НСД. |
| 1995 | В Великобритании ущерб от НСД к информационно-вычислительным ресурсам превысил 5 млрд. Фунтов стерлингов (в 4 раза больше по сравнению с 1989 г.) |
| 1995 | В сети Bitnet (международная академическая сеть) за 2 часа вирус, замаскированный под рождественское поздравление, заразил более 500 тысяч компьютеров по всему миру, при этом сеть IBM прекратила вообще работу на несколько часов. |
| Декабрь 1996 | Компьютерная атака на WebCom (крупнейшего провайдера услуг WWW в США) вывела из строя на 40 часов больше 3000 абонентских пунктов WWW. Атака представляла собой "синхронный поток", которая блокирует функционирование сервера и приводит к "отказу в обслуживании". Поиск маршрута атаки длился 10 часов. |

Таблица 4.4

|  |  |
| --- | --- |
| **Год** | **События, цифры, факты** |
| 1993 | Была совершена попытка хищения 68 миллионов долларов путем манипуляции с данными в компьютерных сетях Центрального Банка России |
| 1994 | В. Левин проник в компьютерную систему Ситибанка и сумел перевести 2.8 миллиона долларов на счета своих сообщников в США, Швейцарии, Нидерландах и Израиле |
| 1995 | Ущерб, нанесенный банкам США за счет несанкционированного использования компьютерных сете путем введения и "навязывания" ложной информации из Москвы и Санкт-Петербурга российскими хакерами составил за I квартал 1995 г. составил $300 млн. |
| 1997 | Правоохранительными органами России было выявлено 15 компьютерных преступлений, связанных НСД к банковским базам данных. В ходе расследования установлены факты незаконного перевода 6,3 млрд. рублей. Доля компьютерных преступлений от общего числа преступлений в кредитно-финансовой сфере в 1997 г. составила 0,02% при их раскрываемостине более 1-5%. |
| 1998 | Предотвращено хищения на сумму 2 млрд. рублей из филиала одногоиз самых крупных коммерческих банков России |

Злоумышленники в профессиональных коллективах программистов-разработчиков

Согласно существующей статистики в коллективах людей занятых той или иной деятельностью, как правило, только около 85% являются вполне лояльными (честными), а остальные 15% делятся примерно так: 5% - могут совершить что-нибудь противоправное, если, по их представлениям, вероятность заслуженного наказания мала; 5% - готовы рискнуть на противоправные действия, даже если шансы быть уличенным и наказанным складываются 50 на 50; 5% - готовы пойти на противозаконный поступок, даже если они почти уверены в том, что будут уличены и наказаны. Такая статистика в той или иной мере может быть применима к коллективам, участвующим в разработке и эксплуатации информационно-технических составляющих компьютерных систем.

Таким образом, можно предположить, что не менее 5% персонала, участвующего в разработке и эксплуатации программных комплексов, способны осуществить действия криминального характера из корыстных побуждений либо под влиянием каких-нибудь иных обстоятельств.

По другим данным  считается, что от 80 до 90% компьютерных нарушений являются внутренними, в частности считается, что на каждого "... подлого хакера приходится один обозленный и восемь небрежных работников, и все они могут производить разрушения изнутри".

###### 4.3.2. Информационная война

В настоящее время за рубежом в рамках создания новейших оборонных технологий и видов оружия активно проводятся работы по созданию так называемых средств нелетального воздействия. Эти средства позволяют без нанесения разрушающих ударов (например, современным оружием массового поражения) по живой силе и технике вероятного противника выводить из строя и/или блокировать его вооружение и военную технику, а также нарушать заданные стратегии управления войсками.

Одним из новых видов оружия нелетального воздействия является информационное оружие, представляющее собой совокупность средств поражающего воздействия на информационный ресурс противника. Воздействию информационным оружием могут быть подвержены прежде всего компьютерные и телекоммуникационные системы противника. При этом центральными объектами воздействия являются программное обеспечение, структуры данных, средства вычислительной техники и обработки информации, а также каналы связи.

Появление информационного оружия приводит к изменению сущности и характера современных войн и появлению нового вида вооруженного конфликта - информационная война.

Несомненным является то, что информационная война, включающая информационную борьбу в мирное и военное время, изменит и характер военной доктрины ведущих государств мира. Многими зарубежными странами привносится в доктрину концепция выигрывать войны, сохраняя жизни своих солдат, за счет технического превосходства.

Ввиду того, что в мировой практике нет прецедента ведения широкомасштабной информационной войны, а имеются лишь некоторые прогнозы и зафиксированы отдельные случаи применения информационного оружия в ходе вооруженных конфликтов и деятельности крупных коммерческих организаций (см. таблицы данного раздела), анализ содержания информационной войны за рубежом возможен по отдельным публикациям, так как, по некоторым данным информация по этой проблеме за рубежом строго засекречена.

Анализ современных методов ведения информационной борьбы (см. табл.4.5) позволяет сделать вывод о том, что к прогнозируемым формам информационной войны можно отнести следующие:

* глобальная информационная война;
* информационные операции;
* преднамеренное изменение замысла стратегической и тактической операции;
* дезорганизация жизненно важных для страны систем;
* нарушение телекоммуникационных систем;
* обнуление счетов в международной банковской системе;
* уничтожение (искажение) баз данных и знаний важнейших государственных и военных объектов.

К методам и средствам информационной борьбы в настоящее время относят:

* воздействие боевых компьютерных вирусов и преднамеренных дефектов диверсионного типа;
* несанкционированный доступ к информации;
* проявление непреднамеренных ошибок ПО и операторов компьютерных систем;
* использование средств информационно-психологического воздействия на личный состав;
* воздействие радиоэлектронными излучениями;
* физические разрушения систем обработки информации.

Таблица 4.5

|  |  |
| --- | --- |
| **Год** | **События, цифры, факты** |
| 1985 | Разведслужбой ФРГ с засекреченного объекта в пригороде Франкфурта успешно проведена операция "Project RAHAB" по проникновению в ИВС и базы данных государственных учреждений и промышленных компаний Великобритании, Италии, СССР, США, Франции и Японии. |
| 1985 | Спецподразделение LAKAM разведслужбы Израиля МОССАД осуществило НСД к ИВС Центра по обеспечению разведывательных операций ВМС США (US Naval Intelligence Support Center - NISC). |
| 1988 | Матиас Шпеер из Ганновера осуществил НСД к информации о программе СОИ и разработках ядерного, химического и биологического оружия из секретных электронных досье Пентагона. |
| Декабрь 1988 | В Ливерморской лаборатории США (Lawrence Livermore National Laboratories - LLNL), занимающейся разработкой ядерного оружия, было зафиксировано 10 попыток НСД через каналы связи с INTERNET. |
| 1989 | Во Франции зарегистрированы попытки НСД в информационные банки данных военного арсенала в Шербуре. |
| Конец 80-х | Группа компьютерных взломщиков из ГДР (Д. Бржезинский, П. Карл, М. Хесс и К. Кох) овладели паролями и кодами доступа к военным и исследовательским компьютерам в США, Франции, Италии, Швейцарии, Великобритании, ФРГ, Японии. |
| 1995 | В космическом центре NASA им. Джонсона (Johnson Space Center) регистрировалось 3-4 попытки НСД в сутки (на 50% больше чем в 1994 г.), 349.2 часов затрачено на восстановление функционирования сети. |
| 1995 | Центр информационной борьбы ВВС (Air Force Information Warfare Center) за первых 3 недели после создания зарегистрировал более 150 попыток НСД только к одному сетевому узлу. |
| Январь 1997 | Через Internet выведена из строя главная машина для хранения информационного архива по проекту FreeBSD (freefall.freebsd.org). |

Таким образом, в большинстве развитых стран мира в рамках концепции информационной войны разрабатывается совокупность разнородных средств, которые можно отнести к информационному оружию. Такие средства могут использоваться в совокупности с другими боевыми средствами во всех возможных формах ведения информационной войны. Кроме существовавших ранее средств поражающего воздействия в настоящее время разрабатываются принципиально новые средства информационной борьбы, а именно бое вые компьютерные вирусы и преднамеренные программные дефекты диверсионного типа.

###### 4.3.3. Психология программирования

При создании высокоэффективных и надежных программ (программных комплексов), отвечающих самым современным требованиям к их разработке, эксплуатации и модернизации необходимо не только умело пользоваться предоставляемой вычислительной и программной базой современных компьютеров, но и учитывать интуицию и опыт разработчиков языков программирования и прикладных систем. Помимо этого, целесообразно дополнять процесс разработки программ экспериментальными исследованиями, которые основываются на применении концепции психологии мышления при исследовании проблем вычислительной математики и информатики. Такой союз вычислительных, информационных систем и программирования принято называть психологией программирования.

Психология программирования - это наука о действиях человека, имеющего дело с вычислительными и информационными ресурсами автоматизированных систем, в которой знания о возможностях и способностях человека как разработчика данных систем могут быть углублены с помощью методов экспериментальной психологии, анализа процессов мышления и восприятия, методов социальной, индивидуальной и производственной психологии.

К целям психологии программирования наряду с улучшением использования компьютера, основанного на глубоком знании свойств мышления человека, относится и определение, как правило, экспериментальным путем, склонностей и способностей программиста как личности. Особенности личности играют критическую роль в определении (исследовании) рабочего стиля отдельного программиста, а также особенностей его поведения в коллективе разработчиков программного обеспечения. Ниже приводится список характеристик личности и их предполагаемых связей с программированием. При этом особое внимание уделяется тем личным качествам программиста, которые могут, в той или иной степени, оказать влияние на надежность и безопасность разрабатываемого им программного обеспечения.

Внутренняя/внешняя управляемость. Личности с выраженной внутренней управляемостью стараются подчинять себе обстоятельства и убеждены в способности сделать это, а также в способности повлиять на свое окружение и управлять событиями. Личности с внешней управляемостью (наиболее уязвимы с точки зрения обеспечения безопасности программного обеспечения) чувствуют себя жертвами не зависящих от них обстоятельств и легко позволяют другим доминировать над ними.

Высокая/низкая мотивация. Личности с высокой степенью мотивации способны разрабатывать очень сложные и сравнительно надежные программы. Руководители, способные повысить уровень мотивации, в то же время, могут стимулировать своих сотрудников к созданию программ с высоким уровнем их безопасности.

Умение быть точным. На завершающих этапах составления программ необходимо особое внимание уделять подробностям и готовности проверить и учесть каждую деталь. Это позволит повысить вероятность обнаружения программных дефектов как привнесенных в программу самим программистом (когда нарушитель может ими воспользоваться в своих целях), так и другими программистами (в случае, если некоторые из них могут быть нарушителями) при создании сложных программных комплексов коллективом разработчиков.

Кроме того, психология программирования изучает, с точки зрения особенностей создания безопасного программного обеспечения, такие характеристики качества личности как исполнительность, терпимость к неопределенности, эгоизм, степень увлеченности, склонность к риску, самооценку программиста и личные отношения в коллективе.

Корпоративная этика

Особый психологический настрой и моральные стимулы программисту может создать особые корпоративные условия его деятельности, в частности различные моральные обязательства, оформленные в виде кодексов чести. Ниже приводится "Кодекс чести пользователя компьютера".

* Обещаю не использовать компьютер в ущерб другим людям.
* Обещаю не вмешиваться в работу компьютера других людей.
* Обещаю "не совать нос" в компьютерные файлы других людей.
* Обещаю не использовать компьютер для воровства.
* Обещаю не использовать компьютер для лжесвидетельства.
* Обещаю не копировать и не использовать чужие программы, которые были оплачены не мною.
* Обещаю не использовать компьютерные ресурсы других людей без разрешения и соответствующей компенсации.
* Обещаю не присваивать результаты интеллектуального труда других людей.
* Обещаю думать об общественных последствиях разрабатываемых мною программ или систем.
* Обещаю всегда использовать компьютер с наибольшей пользой для живущих ныне и будущих поколений.

## Организационные средства защиты.

Организационные основы защиты информации на предприятии

Основные направления, принципы и условия организационной защиты информации  
  
Из упоминавшихся ранее средств и методов обеспечения информационной безопасности особо были выделены организационные, которые в совокупности с другими элементами системы защиты информации на предприятии подробно описаны в последующих главах учебника. Для наиболее полного и глубокого анализа происходящих в сфере защиты конфиденциальной информации процессов, понимание сущности планируемых и проводимых в этих целях мероприятий прежде всего необходимо рассмотреть одно из важнейших направлений защиты конфиденциальной информации — организационную защиту информации.  
  
Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом. Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учетом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата.  
  
Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информации.  
  
Однако организационной защите информации среди этих направлений отводится особое место.  
  
Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и инженерно-геологические) реализовать на практике спланированные руководством предприятия меры по защите информации. Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке.  
  
Роль руководства предприятия в решении задач по защите информации трудно переоценить. Основными направлениями деятельности, осуществляемой руководителем предприятия в этой области, являются: планирование мероприятий по защите информации и персональный контроль за их выполнением, принятие решений о непосредственном доступе к конфиденциальной информации своих сотрудников и представителей других организаций, распределение обязанностей и задач между должностными лицами и структурными подразделениями, аналитическая работа и т.д. Цель принимаемых руководством предприятия и должностными лицами организационных мер — исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.  
  
Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите.  
  
Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.  
  
Используются два примерно равнозначных определения организационной зашиты информации.  
  
Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.  
  
Организационная защита информации на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.  
  
Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе — раскрывает ее структуру на уровне предприятия. Вместе с тем оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств. Основные направления организационной защиты информации приведены ниже.  
  
Организационная защита информации:  
  
- Организация работы с персоналом;  
- Организация внутриобъектового и пропускного режимов и охраны;  
- Организация работы с носителями сведений;  
- Комплексное планирование мероприятий по защите информации;  
- Организация аналитической работы и контроля.  
  
Основные принципы организационной защиты информации:  
  
- принцип комплексного подхода — эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;  
  
- принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);  
  
- принцип персональной ответственности — наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.  
  
Среди основных условий организационной защиты информации можно выделить следующие:  
  
- непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;  
- неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.  
  
При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.  
  
Основные подходы и требования к организации системы защиты информации  
  
Успешное решение комплекса задач по защите информации не может быть достигнуто без создания единой основы, так называемого «активного кулака» предприятия, способного концентрировать все усилия и имеющиеся ресурсы для исключения утечки конфиденциальной информации и недопущения возможности нанесения ущерба предприятию. Таким «кулаком» призвана стать система защиты информации на предприятии, создаваемая на соответствующей нормативно-методической основе и отражающая все направления и специфику деятельности данного предприятия.  
  
Под системой защиты информации понимают совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях.  
  
Для решения организационных задач по созданию и обеспечению функционирования системы защиты информации используются несколько основных подходов, которые вырабатываются на основе существующей нормативно-правовой базы и с учетом методических разработок по тем или иным направлениям защиты конфиденциальной информации.  
  
Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению конфиденциальной информацией и, тем самым, нанесению ущерба предприятию. Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учетом особенностей их расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).  
  
Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также на деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.  
  
При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, которые связаны с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. В соответствии с названными приоритетами формируется перечень возможных угроз информации, подлежащей защите, и определяются конкретные силы, средства, способы и методы ее защиты.  
  
К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.  
  
Система защиты информации должна быть:  
  
- централизованной — обеспечивающей эффективное управление системой со стороны руководителя и должностных лиц, отвечающих за различные направления деятельности предприятия;  
- плановой — объединяющей усилия различных должностных лиц и структурных подразделений для выполнения стоящих перед предприятием задач в области защиты информации;  
- конкретной и целенаправленной — рассчитанной на защиту абсолютно конкретных информационных ресурсов, представляющих интерес для конкурирующих организаций;  
- активной — обеспечивающей защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;  
- надежной и универсальной — охватывающей всю деятельность предприятия, связанную с созданием и обменом информацией.  
  
Основные методы, силы и средства, используемые для организации защиты информации  
  
Один из важнейших факторов, влияющих на эффективность системы защиты конфиденциальной информации, — совокупность сил и средств предприятия, используемых для организации защиты информации.  
  
Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования. Предприятия, работающие с конфиденциальной информацией и решающие задачи по ее защите в рамках повседневной деятельности на постоянной основе, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации. Если предприятия лишь эпизодически работают с конфиденциальной информацией в силу ее небольших объемов, вместо создания подразделений они могут включать в свои штаты отдельные должности специалистов по защите информации. Данные подразделения и должности являются органами защиты информации.  
  
Предприятия, работающие с незначительными объемами конфиденциальной информации, могут на договорной основе использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников, высокоэффективные средства защиты информации, а также большой опыт практической работы в данной области.  
  
Ведущую роль в организации защиты информации на предприятии играют руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.  
  
Руководитель предприятия несет персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации. Он обязан:  
  
- знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;  
- определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;  
- проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации;  
- оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.  
  
Заместитель руководителя предприятия обязан постоянно изучать все стороны и направления деятельности предприятия для принятия своевременных мер по защите информации; руководить работой службы безопасности (иных структурных подразделений, решающих задачи по защите информации); выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ. Более подробно обязанности руководителя предприятия и его заместителя, отвечающего за защиту информации, рассмотрены в других статьях.  
  
На предприятиях для организации работ по защите информации могут создаваться следующие основные виды структурных подразделений:   
режимно-секретные;  
подразделения по технической защите информации и противодействию иностранным техническим разведкам;  
подразделения криптографической защиты информации; мобилизационные;  
подразделения охраны и пропускного режима.  
  
Функции, возлагаемые на перечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях.  
  
По решению руководителя предприятия данные подразделения организационно могут объединяться в службу безопасности, руководитель которой в некоторых случаях может быть наделен статусом заместителя руководителя предприятия и полномочиями должностного лица, осуществляющего руководство работой структурных подразделений предприятия, деятельность которых связана с использованием и защитой информации.  
  
Режимно-секретное подразделение, мобилизационное подразделение и подразделение по технической защите информации и противодействию иностранным техническим разведкам создаются на предприятиях, выполняющих работы с использованием сведений, составляющих государственную тайну (вне зависимости от наличия на предприятии иной информации с ограниченным доступом).  
  
Режимно-секретное подразделение является основным структурным подразделением предприятия и решает задачи организации, координации и контроля деятельности других структурных подразделений (персонала предприятия) по обеспечению защиты сведений, составляющих государственную тайну. На предприятиях, не выполняющих работы со сведениями, составляющими государственную тайну, для решения аналогичных задач в отношении других видов информации с ограниченным доступом создается и функционирует служба безопасности (служба защиты информации).  
  
Подразделение по технической защите информации и противодействию иностранным техническим разведкам решает задачи организации и проведения комплекса технических мероприятий, направленных на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, отнесенных к конфиденциальной информации и подлежащих защите.  
  
Подразделение криптографической защиты информации создается в целях предотвращения утечки конфиденциальной информации при ее передаче по открытым каналам (линиям) связи с помощью технических средств, а также при использовании локальных вычислительных сетей, имеющих выход за пределы территории предприятия.  
  
Подразделение охраны и пропускного режима создается в целях предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах предприятия посторонних лиц и транспорта, нанесения ущерба предприятию путем краж (хищений) с территории предприятия материальных средств и иного имущества. В некоторых случаях для решения задач охраны и пропускного режима на предприятиях могут создаваться отдельные самостоятельные подразделения.  
  
Мобилизационное подразделение решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материальных ресурсов.  
  
Кроме перечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения, для которых выполнение мероприятий по защите информации не является основной функцией.  
  
К таким подразделениям относятся кадровый орган, орган юридической службы (юрисконсульт), орган психологической и воспитательной работы, пресс-служба предприятия и др. Особо необходимо отметить важность участия в организации защиты информации производственных, так называемых «тематических» структурных подразделений (отдельных должностных лиц), которые создают продукцию и товары или оказывают услуги (например, производство стрейч пленки), и в связи с этим самым непосредственным образом взаимодействуют с другими предприятиями и органами государственной власти.  
  
Для проведения работ по организации защиты информации используются также возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. В их числе — постоянно действующая техническая комиссия, экспертная комиссия, комиссия по рассекречиванию носителей конфиденциальной информации, комиссия по категорированию объектов информатизации и др. Функции, возлагаемые на данные комиссии, рассмотрены в других статьях.  
  
Чтобы добиться максимальной эффективности при решении задач защиты информации, наряду с возможностями упомянутых штатных и нештатных подразделений (должностных лиц) необходимо использовать имеющиеся на предприятии средства защиты информации.  
  
Под средствами защиты информации понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, а также средства, устройства и системы контроля эффективности защиты информации.  
  
Технические средства защиты информации — устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.  
  
Криптографические средства защиты информации — средства (устройства), обеспечивающие защиту конфиденциальной информации путем ее криптографического преобразования (шифрования).  
  
Программные средства защиты информации — системы защиты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.  
  
Эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия соответствующих сил и средств. Вместе с тем определяющую роль в вопросах организации защиты информации, применения в этих целях сил и средств предприятия играют методы защиты информации, определяющие порядок, алгоритм и особенности использования данных сил и средств в конкретной ситуации.  
  
Методы защиты информации — применяемые в целях исключения утечки информации универсальные и специфические способы использования имеющихся сил и средств (приемы, меры, мероприятия), учитывающие специфику деятельности по защите информации.  
  
Общие методы защиты информации подразделяются на правовые, организационные, технические и экономические.  
  
Методы защиты информации с точки зрения их теоретической основы и практического использования взаимосвязаны. Правовые методы регламентируют и всесторонне нормативно регулируют деятельность по защите информации, выделяя, прежде всего, ее организационные направления. Тесную связь организационных и правовых методов защиты информации можно показать на примере решения задач по исключению утечки конфиденциальной информации, в частности относящейся к коммерческой тайне предприятия, при его взаимодействии с различными государственными и территориальными инспекторскими и надзорными органами. Эти органы в соответствии с предоставленными им законом полномочиями осуществляют деятельность по получению (истребованию), обработке и хранению информации о предприятиях и гражданах (являющихся их сотрудниками).  
  
Передача информации, в установленном порядке отнесенной к коммерческой тайне или содержащей персональные данные работника предприятия, должна осуществляться на основе договора, предусматривающего взаимные обязательства сторон по нераспространению (неразглашению) этой информации, а также необходимые меры по ее защите.  
  
Организационные механизмы защиты информации определяют порядок и условия комплексного использования имеющихся сил и средств, эффективность которого зависит от применяемых методов технического и экономического характера.  
  
Технические методы защиты информации, используемые в комплексе с организационными методами, играют большую роль в обеспечении защиты информации при ее хранении, накоплении и обработке с использованием средств автоматизации. Технические методы необходимы для эффективного применения имеющихся в распоряжении предприятия средств защиты информации, основанных на новых информационных технологиях.  
  
Среди перечисленных методов защиты информации особо выделяются организационные методы, направленные на решение следующих задач:  
реализация на предприятии эффективного механизма управления, обеспечивающего защиту конфиденциальной информации и недопущение ее утечки;  
осуществление принципа персональной ответственности руководителей подразделений и персонала предприятия за защиту конфиденциальной информации;  
определение перечней сведений, относимых на предприятии к различным категориям (видам) конфиденциальной информации;  
  
ограничение круга лиц, имеющих право доступа к различным видам информации в зависимости от степени ее конфиденциальности;  
подбор и изучение лиц, назначаемых на должности, связанные с конфиденциальной информацией, обучение и воспитание персонала предприятия, допущенного к конфиденциальной информации;  
организация и ведение конфиденциального делопроизводства;  
осуществление систематического контроля за соблюдением установленных требований по защите информации.  
  
Приведенный перечень организационных методов не является исчерпывающим и, в зависимости от специфики деятельности предприятия, степени конфиденциальности используемой информации, объема выполняемых работ, а также опыта работы в области защиты информации, может быть дополнен иными методами.