ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

РЕФЕРАТ

По дисциплине: Комплексная система защиты информации

На тему: Общие положения информационной безопасности

Выполнил: Шазимов А.

Группа 233-12

Принял(а): _____

Ташкент – 2014

Информационная безопасность (общие положения)

Информационная безопасность

Введение

Примечательная особенность нынешнего периода - переход от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергические ресурсы. Ресурсами, как известно, называют элементы экономического потенциала, которыми располагает общество и которое при необходимости могут быть использованы для достижения конкретной цели хозяйственной деятельности. Давно стали привычными и общеупотребительными такие категории, как материальные, финансовые, трудовые, природные ресурсы, которые вовлекаются в хозяйственный оборот, и их назначение понятно каждому. Но вот появилось понятие "информационные ресурсы", и хотя оно узаконено, но осознано пока еще недостаточно. Информационные ресурсы - отдельные документы и отдельные массивы, документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Информационные ресурсы являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учету и защите, так как информацию можно использовать не только для товаров и услуг, но и превратить ее в наличность, продав кому-нибудь, или, что еще хуже, уничтожить. Собственная информация для производителя представляет значительную ценность, так как нередко получение (создание) такой информации - весьма трудоемкий и дорогостоящий процесс. Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами.

Особое место отводится информационным ресурсам в условиях рыночной экономики.

Важнейшим фактором рыночной экономики выступает конкуренция. Побеждает тот, кто лучше, качественнее, дешевле и оперативнее (ВРЕМЯ-ДЕНЬГИ!!!) производит и продает. В сущности это универсальное правило рынка. И в этих условиях основным выступает правило: кто владеет информацией, тот владеет миром.

В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. Установлено, что 47% охраняемых сведений добывается с помощью технических средств промышленного шпионажа.

В этих условиях защите информации от неправомерного овладения ею отводится весьма значительное место. При этом "целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к

охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения".

Как видно из этого определения целей защиты, информационная безопасность - довольно емкая и многогранная проблема, охватывающая не только определение необходимости защиты информации, но и то, как ее защищать, от чего защищать, когда защищать, чем защищать и какой должна быть эта защита.

Основное внимание уделяется защите конфиденциальной информации, с которой большей частью встречаются предприниматели негосударственного сектора экономики.

Люди осознают и отдают себе отчет в сложности проблемы защиты информации вообще, и с помощью технических средств в частности. Тем не менее взгляд на эту проблему излагается на этом Web-сайте, считается, что этим охватывается не все аспекты сложной проблемы, а лишь определенные ее части.

Концепция информационной безопасности

1. Основные концептуальные положения системы защиты информации
2. Концептуальная модель информационной безопасности
3. Угрозы конфиденциальной информации
4. Действия, приводящие к неправомерному овладению конфиденциальной информацией

"ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - это состояние защищенности информации среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств" (Закон РФ "Об участии в международном информационном обмене").

Постулаты

Информация - это всеобщее свойство материи.
Любое взаимодействие в природе и обществе основано на информации.
Всякий процесс совершения работы есть процесс информационного взаимодействия.
Информация - продукт отражения действительности.

Действительность отражается в пространстве и времени.
Ничего не происходит из ничего.
Информация сохраняет значение в неизменном виде до тех пор, пока остается в неизменном виде носитель информации - ПАМЯТЬ.
Ничто не исчезает просто так.

Понятие "информация" сегодня употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно не использовалось. Огромные информационные потоки буквально захлестывают людей. Объем научных знаний, например, по оценке специалистов, удваивается, каждые пять лет. Такое положение приводит к заключению, что XXI век будет веком торжества теории и практики ИНФОРМАЦИИ - информационным веком.

Правомерно задать вопрос: что же такое информация? В литературе дается такое определение: информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Известно, что информация может иметь различную форму, включая данные, заложенные в компьютерах, "синьки", кальки, письма или памятные записки, досье, формулы, чертежи, диаграммы, модели продукции и прототипы, диссертации, судебные документы и др.

Как и всякий продукт, информация имеет потребителей, нуждаю-щихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения потребителя качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения обладателя - сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства, и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации.

Понимая под безопасностью состояние защищенности жизненно важных интересов личности, предприятия, государства от внутрен-них и внешних угроз, можно выделить и компоненты безопасности - такие, как персонал, материальные и финансовые средства и информацию.

1.1 Основные концептуальные положения системы защиты информации.

Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют:

весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;
значительное число фирм, специализирующихся на решении вопросов защиты

информации;
достаточно четко очерченная система взглядов на эту проблему;
наличие значительного практического опыта и др.

И, тем не менее, как свидетельствует отечественная и зарубежная печать, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту. Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов. Причем в этом должны активно участвовать профессиональные специалисты, администрация, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Опыт также показывает, что:

обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий;

безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм - систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий;

никакая СЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту.

С учетом накопленного опыта можно определить систему защиты информации как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

С позиций системного подхода к защите информации предъявляются определенные требования. Защита информации должна быть:

непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;
плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);

целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;
конкретной. Защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
активной. Защищать информацию необходимо с достаточной степенью настойчивости;
надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;
универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;
комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства.

Комплексный характер защиты проистекает из того, что защита - это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимо обусловливающих друг друга сторон, свойств, тенденций.

Зарубежный и отечественный опыт показывает, что для обеспечения выполнения столь многогранных требований безопасности система защиты информации должна удовлетворять определенным условиям:

охватывать весь технологический комплекс информационной деятельности;
быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа;
быть открытой для изменения и дополнения мер обеспечения безопасности информации;
быть нестандартной, разнообразной. При выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей;
быть простой для технического обслуживания и удобной для эксплуатации пользователями;
быть надежной. Любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации;
быть комплексной, обладать целостностью, означающей, что ни одна ее часть не может быть изъята без ущерба для всей системы. К системе безопасности информации предъявляются также определенные требования:
четкость определения полномочии и прав пользователей на доступ к определенным видам информации;
предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;

сведение к минимуму числа общих для нескольких пользователей средств защиты;
учет случаев и попыток несанкционированного доступа к конфиденциальной информации;
обеспечение оценки степени конфиденциальной информации;
обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя. Система защиты информации как любая система должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого СЗИ может иметь:
правовое обеспечение. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действий;
организационное обеспечение. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами - такими, как служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая деятельность и др.;
аппаратное обеспечение. Предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности собственно СЗИ;
информационное обеспечение. Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;
программное обеспечение. К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации;
математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;
лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;
нормативно-методическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Удовлетворить современные требования по обеспечению безопасности предприятия и защиты его конфиденциальной информации может только система безопасности. Под системой безопасности будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий.

1.2. Концептуальная модель информационной безопасности.

Понимая информационную безопасность как "состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций", правомерно определить угрозы безопасности информации, источники этих угроз, способы их реализации и цели, а также иные условия и действия, нарушающие безопасность. При этом, естественно, следует рассматривать и меры защиты информации от неправомерных действий, приводящих к нанесению ущерба.

Практика показала, что для анализа такого значительного набора источников, объектов и действий целесообразно использовать методы моделирования, при которых формируется как бы "заместитель" реальных ситуаций. При этом следует учитывать, что модель не копирует оригинал, она проще. Модель должна быть достаточно об-щей, чтобы описывать реальные действия с учетом их сложности.

Можно предложить следующие компоненты модели информационной безопасности на первом уровне декомпозиции.

По нашему мнению, такими компонентами концептуальной модели безопасности информации могут быть следующие:

объекты угроз;
угрозы;
источники угроз;
цели угроз со стороны злоумышленников;
источники информации;
способы неправомерного овладения конфиденциальной информацией (способы доступа);
направления защиты информации;
способы защиты информации;
средства защиты информации.

Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности. Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкционированного доступа к охраняемым сведениям.

Источниками конфиденциальной информации являются люди, доку-менты, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства. Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности.

Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы. Последние могут быть реализованы как аппаратно, программ-но, так и смешанно-программно-аппаратными средствами.

В качестве способов защиты выступают всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие не-санкционированному доступу. В обобщенном виде рассмотренные компоненты в виде концептуальной модели безопасности информации приведены на следующей схеме.

Основные элементы концептуальной модели будут рассмотрены более подробно в следующих разделах книги. Концепция безопасности является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз.

1.3. Угрозы конфиденциальной информации

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями. Такими действиями являются:

ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;
модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;
разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации. Каждая угроза влечет за собой

определенный ущерб - моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале - полностью, реально - значительно или хотя бы частично. Но и это удается далеко не всегда.

С учетом этого угрозы могут быть классифицированы по следующим кластерам :

по величине принесенного ущерба:
предельный, после которого фирма может стать банкротом;
значительный, но не приводящий к банкротству;
незначительный, который фирма за какое-то время может компенсировать и др.;
по вероятности возникновения:
весьма вероятная угроза;
вероятная угроза;
маловероятная угроза;
по причинам появления:
стихийные бедствия;
преднамеренные действия;
по характеру нанесенного ущерба:
материальный;
моральный;
по характеру воздействия:
активные;
пассивные;
по отношению к объекту:
внутренние;
внешние.

Источниками внешних угроз являются:

недобросовестные конкуренты;
преступные группировки и формирования;
отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

администрация предприятия;
персонал;
технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз на усредненном уровне можно охарактеризовать так:

82% угроз совершается собственными сотрудниками фирмы либо при их прямом или опосредованном участии;
17% угроз совершается извне - внешние угрозы;
1% угроз совершается случайными лицами.

Угроза - это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

1.4. Действия, приводящие к неправомерному овладению конфиденциальной информацией.

Отношение объекта (фирма, организация) и субъекта (конкурент, злоумышленник) в информационном процессе с противоположными интересами можно рассматривать с позиции активности в действиях, приводящих к овладению конфиденциальными сведениями. В этом случае возможны такие ситуации:

владелец (источник) не принимает никаких мер к сохранению конфиденциальной информации, что позволяет злоумышленнику легко получить интересующие его сведения;

источник информации строго соблюдает меры информационной безопасности, тогда злоумышленнику приходится прилагать значи-тельные усилия к осуществлению доступа к охраняемым сведениям, используя для этого всю совокупность способов несанкционированного проникновения: легальное или нелегальное, заходовое или беззаходовое;

промежуточная ситуация - это утечка информации по техническим каналам, при которой источник еще не знает об этом (иначе он принял бы меры защиты), а злоумышленник легко, без особых усилий может их использовать в своих интересах.

В общем, факт получения охраняемых сведений злоумышленниками или конкурентами называют утечкой. Однако одновременно с этим в значительной части законодательных актов, законов, кодексов, официальных материалов используются и такие понятия, как разглашение сведений и несанкционированный доступ к конфиденциальной информации .

Разглашение - это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и научной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации. К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами средствами передачи официальной информации (почта, телефон, телеграф и др.). Неформальные коммуникации включают личное общение (встречи, переписка и др.); выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газеты, интервью, радио, телевидение и др.). Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их

тщательного соблюдения. Тут важно отметить, что субъектом в этом процессе выступает источник (владелец) охраняемых секретов. Следует отметить информационные особенности этого действия. Информация содержательная, осмысленная, упорядоченная, аргументированная, объемная и доводится зачастую в реальном масштабе времени. Часто имеется возможность диалога. Информация ориентирована в определенной тематической области и документирована. Для получения интересующей злоумышленника информации последний затрачивает практически минимальные усилия и использует простые легальные технические средства (диктофоны, видео мониторинг).

Утечка - это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации осуществляется по различным техническим каналам. Известно, что информация вообще переносится или пере-дается либо энергией, либо веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги (написанный текст) и др. С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому классифицируются и каналы утечки информации на визуально-оптические, акустические, электро-магнитные и материально-вещественные. Под каналом утечки ин-формации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

Несанкционированный доступ - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам. Несанкционированный доступ к источникам конфиденциальной информации реализуется различными способами: от инициативного сотрудничества, выражающегося в активном стремлении "продать" секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения - стационарных или в подвижном варианте, оборудованных самыми современными техническими средствами. Если исходить из комплексного подхода к обеспечению информационной безопасности, то такое деление ориентирует на защиту информации как от разглашения, так и от утечки по техническим каналам и от несанкционированного доступа к ней со стороны конкурентов и злоумышленников. Такой подход к классификации действий, способствующих неправо-мерному овладению конфиденциальной информацией, показывает многогранность угроз и многоаспектность защитных мероприятий, необходимых для обеспечения комплексной информационной без-опасности.

С учетом изложенного остается рассмотреть вопрос, какие условия способствуют

неправомерному овладению конфиденциальной ин-формацией. Указываются следующие условия:

разглашение (излишняя болтливость сотрудников) - 32%;
несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок - 24%;
отсутствие на фирме надлежащего контроля и жестких условий обеспечения информационной безопасности - 14%;
традиционный обмен производственным опытом - 12%;
бесконтрольное использование информационных систем - 10%;
наличие предпосылок возникновения среди сотрудников конфликтных ситуаций 8%;
а также отсутствие высокой трудовой дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа кадров по сплочению коллектива.

Среди форм и методов недобросовестной конкуренции находят наибольшее распространение:

экономическое подавление, выражающееся в срыве сделок и иных соглашений (48%),
парализации деятельности фирмы (31%),
компрометации фирмы (11%),
шантаже руководителей фирмы (10%);
физическое подавление:
ограбления и разбойные нападения на офисы, склады, грузы (73%),
угрозы физической расправы над руководителями фирмы и ведущими специалистами (22%),
убийства и захват заложников (5%);
информационное воздействие:
подкуп сотрудников (43%),
копирование информации (24%),
проникновение в базы данных (18%),
продажа конфиденциальных документов (10%),
подслушивание телефонных переговоров и переговоров в помещениях (5%),
а также ограничение доступа к информации, дезинформация;
финансовое подавление включает такие понятия, как инфляция, бюджетный дефицит, коррупция, хищение финансов, мошенничество; психическое давление может выражаться в виде хулиганских выходок, угрозы и шантажа, энергоинформационного воздействия.