Защита информации понятие и назначение

В толковых словарях термин защита интерпретируется двояко: как процесс охраны, сбережения, спасения от кого, чего-нибудь неприятного, враждебного, опасного и как совокупность методов, средств и мер, принимаемых для предотвращения, предупреждения чего-то. Таким образом, **содержательная часть** в этих определениях по смыслу совпадает - **это предотвращение, предупреждение чего-то опасного, враждебного.** Если соотнести это положение с защитой информации, то самым опасным для собственника информации является **нарушение установленного статуса информации,** и поэтому содержательной частью защиты должно быть предотвращение такого нарушения.

Нарушение статуса любой информации заключается в нарушении ее физической сохранности вообще либо у данного собственника (в полном или частичном объеме), структурной целостности, доступности для правомочных пользователей. Нарушение статуса конфиденциальной информации, в том числе составляющей государственную тайну, дополнительно включает в себя нарушение ее конфиденциальности (закрытости для посторонних лиц).

**Защита информации -**деятельность по предотвращению утраты и утечки конфиденциальной информации и утраты защищаемой открытой информации.

Учитывая, что определение должно быть лаконичным, а термин утрата и утечка защищаемой информации поглощает все формы проявления уязвимости конфиденциальной и защищаемой части открытой информации, можно ограничиться более кратким определением при условии дифференцированного его преломления в практической работе:

**Защита информации -**деятельность по предотвращению утраты и утечки защищаемой информации.

А теперь проанализируем определение этого понятия, содержащееся в **ГОСТ Р50922-96 "Защита информации. Основные термины и определения",** поскольку это определение официальное, имеющее в смысловом значении обязательный характер. Оно сформулировано так: **Защита информации -**деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

С понятием защиты информации тесно связано понятие безопасности информации. Термин безопасность информации имеет двойное смысловое значение, его можно толковать:

1. **и как безопасность самой информации.**

При этом безопасность самой информации не вписывается в однозначное понимание. С одной стороны, это может означать безопасность информации с точки зрения изначальной **полноты и надежности информации (т.е. безопасность с точки зрения содержания)**, с другой стороны, — **защищенность установленного статус-кво информации (безопасность с точки зрения формы информации).**

1. **и как отсутствие угроз со стороны информации субъектам информационных отношений.**

В нормативных документах и литературе безопасность информации рассматривается только в разрезе ее защищенности, и это, вероятно, оправдано при наличии термина информационная безопасность.

Существует несколько определений понятия **безопасность информации**. Общий подход: **безопасность информации** **как состоянию защищенности (или защиты) информации.**Это не вызывает возражений, ибо сам термин безопасность означает отсутствие опасностей, что определенным образом корреспондируется с термином состояние защищенности.

Часто цель и задачи защиты информации отождествляют, что неверно.

**Цель защиты информации** – это то, ради чего она должна защищаться (предполагаемый результат деятельности по защите информации).

**Задачи защиты информации** - это, что необходимо сделать для реализации цели (результата защиты информации).

## **Структура целей защиты информации.**

Защита информации имеет два уровня целей

**Первый уровень –**непосредственные цели, которые должны быть привязаны к самой информации как непосредственному объекту защиты.

Цель защиты информации первого уровня – безопасность информации.

**Второй уровень**– конечные цели (опосредованные), которые должны быть привязаны к субъектам информационных отношений (государству, обществу, личности, конкретному хозяйствующему субъекту).

Цель защиты информации второго уровня – безопасность субъектов информационных отношений.

Защита информации — это деятельность соб­ственника информации или уполномоченных им лиц по:

* обеспечению своих прав на владение, распоряжение и уп­равление защищаемой информацией;
* предотвращению утечки и утраты информации;
* сохранению полноты, достоверности, целостности защи­щаемой информации, ее массивов и программ обработки;
* сохранению конфиденциальности или секретности защи­щаемой информации в соответствии с правилами, установленны­ми законодательными и другими нормативными актами.

В общем виде цели защиты информации сводятся к режимно-секретному информационному обеспечению деятельности госу­дарства, отрасли, предприятия, фирмы.

## **Задачи защиты информации.**

Задачи защиты информации также имеют два уровня:

**Первый уровень** – задачи обще и концептуального плана:

* на предупреждение угроз. Предупреждение угроз — это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
* на выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
* на обнаружение угроз. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;
* на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
* на ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

**Второй уровень**задач защиты информации зависит от конкретного предприятия (прикладные задачи). Они зависят:

* от видов защищаемой на предприятии информации;
* степени ее конфиденциальности;
* состава носителей защищаемой информации.

Защита информации раз­бивается на решение **двух основных групп задач**:

1. Своевременное и полное удовлетворение информационных потребностей, возникающих в процессе управленческой, инженерно-технической, маркетинговой и иной деятельности, то есть обеспечение специалистов организаций, предприятий л фирм секретной или конфиденциальной информацией.

2. Ограждение засекреченной информации от несанкциониро­ванного доступа к ней соперника, других субъектов в злонамерен­ных целях.

При решении **первой группы задач** — **обеспечение специалис­тов информацией**— всегда, конечно, учитывается, что специа­листы могут использовать как открытую, так и засекреченную ин­формацию. Снабжение специалистов открытой информацией ничем не ограничивается, кроме ее фактического наличия. При снабжении же специалиста засекреченной информацией действу­ют ограничения: наличие соответствующего допуска (к какой сте­пени секретности информации он допущен) и разрешения на до­ступ к конкретной информации. В решении проблемы доступа специалиста к соответствующей засекреченной информации всег­да существуют противоречия, с одной стороны, — максимально ограничить его доступ к засекреченной информации и тем самым уменьшить вероятность утечки этой информации; с другой сторо­ны, — наиболее полно удовлетворить его потребности в информа­ции, в том числе и засекреченной для обоснованного решения им служебных задач.

В обычных, не режимных условиях, специалист имеет возможность использовать в целях решения стоящей перед ним проблемы разнообразную информацию: ретроспективную, узко- и широкотематическую, отраслевую и межотраслевую, фак­тографическую и концептуальную. При обеспечении его засекре­ченной информацией возможности доступа к ней ограничивают­ся двумя факторами: его служебным положением и решаемой спе­циалистом в настоящее время проблемой.

**Вторая группа задач** — **это ограждение защищаемой информа­ции от несанкционированного доступа к ней соперника**, включа­ет такие условия, как:

1. Защита информационного суверенитета страны и расширение возможности государства по укреплению своего могущества за счет формирования и управления развитием своего информационного потенциала.
2. Создание условий эффективного использования информационных ресурсов общества, отрасли, предприятия, фирмы, структурного подразделения, индивида.
3. Обеспечение безопасности защищаемой информации: пред­ отвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации и т.п., вмеша­тельства в информацию и информационные системы.
4. Сохранение секретности или конфиденциальности засекреченной информации в соответствии с установленными правилами ее защиты, в том числе предупреждения ее утечки и несанкцио­нированного доступа к ее носителям, предотвращению ее копи­рования, фотографирования и др.
5. Сохранение полноты, достоверности, целостности инфор­мации и ее массивов и программ обработки, установленных соб­ственником информации или уполномоченными им лицами.
6. Обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальной персональной информации, в том числе накапливаемой в банках данных.
7. Недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности, принадлежащей государству, предприятиям и фирмам, частным лицам.

Значение защиты информации определяется не только в системе информационной безопасности, но и в системе национальной безопасности. Цели защиты информации для государства, общества и отдельных личностей различна. Они в конечном итоге дополняют друг друга и каждый из субъектов объективно заинтересован в защите информации других субъектов. В различных сферах деятельности политической, экономической, военной, социальной интересы всех субъектов должны или совпадать или дополнять друг друга. С учетом этого значения защиту информации следует рассматривать с привязкой не к субъектам, а к сферам деятельности независимо от того ко всем или одному субъекту относится эти сферы деятельности. При этом значение защиты информации целесообразно определить через те последствия (положительные или отрицательные), которые наступают в результате защиты или при ее отсутствии:

1. В области внешней политики обеспечивает свои внешне - политические интересы, т. е. иметь преимущества над другими государствами. Достигаются с помощью секретно - сепаратных договоров о военно-политическом сотрудничестве. Защита информации повышает политический уровень такого государства и его международный авторитет. Защита информации может давать и отрицательный результат : если предоставить очень большой объем закрытой информации, во внешней политике это может привести к осложнению в области международной политики.

2. В военной области защита информации позволяет сохранить в тайне от потенциального противника сведения о составе военной техники, ее количестве, тактики, технических данных о разработке новых систем оружия и военной технике, об организации обороны подготовке на случай войны. С другой стороны чрезмерная закрытость информации о вооружении вызывает сомнения других государств, приводит к гонке вооружений. Неоправданный объем защищенной информации в этой области сокращает возможность использования научно-технических достижений в гражданских областях экономики.

3. В экономической сфере деятельности защита информации дает возможность иметь высокие доходы, сохранять приоритет, заключать выгодные контракты, добиваться преимущества над конкурентами, избегать экономического ущерба. Излишняя засекреченность в экономике снижает доверие к ее отраслям или предприятиям со стороны потенциальных партнеров и потребителей продукции, тормозит инвестиции и подрывает престиж предприятия.

4. В социальной сфере - в политических, экономических, правовых и других областях, определяющих общественную и частную жизнь человека защита информации направлена на улучшения морального и материального благосостояния человека.

Меры обеспечения сохранности и защиты информации в государственной организации, на предприятии или фирме различаются по своим масштабам и формам. Они зависят от производственных, финансовых и других возможностей фирмы, от количества охраняемых на нем секретов и их значимости. При этом выбор таких мер необходимо осуществлять по принципу экономической целесообразности, придерживаясь в финансовых расчетах «золотой середины», поскольку чрезмерное закрытие информации, так же как и халатное отношение к ее сохранению, могут вызвать потерю определенной доли прибыли или привести к непоправимым убыткам. Отсутствие у руководителей предприятий четкого представления об условиях, способствующих утечке конфиденциальной информации, приводят к ее несанкционированному распространению.

Наличие большого количества уязвимых мест на любом современном предприятии или фирме, широкий спектр угроз и довольно высокая техническая оснащенность злоумышленников требует обоснованного выбора специальных решений по защите информации.