НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»

ОРГАНИЗАЦИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

(КОНСПЕКТ)

Санкт-Петербург

Содержание:

1. Основы организации и обеспечения работ по защите конфиденциальной информации.

Основу организации и обеспечения защиты конфиденциальной информации составляет комплексный подход. В соответствии с ним совокупность взаимосвязанных элементов, функционирование которых направлено на обеспечение безопасности информации, образует **систему защиты информации.** Такими элементами являются люди, инженерные конструкции и технические средства, обеспечивающие защиту информации независимо от их принадлежности к другим системам. Ядро системы защиты образуют силы и средства, основными функциями которых является обеспечение ин формационной безопасности. Однако они составляют лишь часть сил и средств системы защиты информации. Например, в систему защиты информации входят не только структурные подразделения (служба безопасности, отдел режима и секретности, 1-й отдел и др.), предназначенные для защиты информации, но все сотрудники организации, обязанные в меру своей ответственности обеспечивать защиту информации. Следовательно, они также являются элементами системы защиты информации организации. И если какой-либо сотрудник организации нарушит правила обращения с секретными документами, то возможен огромный ущерб, несмотря на безупречную работу других элементов системы защиты. Следовательно, структура (элементы и их взаимосвязь) системы защиты информации государства, ведомства, организации пронизывает структуру государства, ведомства, организации.

Для системы защиты информации очень трудно точно указать места входовr и выходов. Входами любой системы являются силы и воздействия, изменяющие состояние системы. Такими силами и воздействиями являются угрозы. Угрозы могут быть внутренними и внешними, в том числе такие трудно локализуемые как слабая правовая дисциплина сотрудников, некачественная эксплуатация средств обработки информации или наличие в помещении радио и электрических приборов, побочные физические процессы в которых способ-

ствуют несанкционированному распространению защищаемой информации. Источниками угроз могут быть злоумышленники, технические средства внутри организации, сотрудники организации, внутренние и внешние поля, стихийные силы и т. д.

Выходы системы представляют собой реакцию системы на входы. Выходами системы являются меры по защите информации. Однако локализовать в пространстве выходы системы так же сложно, как и входы. Каждый сотрудник, например, в меру своей ответственности обязан заниматься задачами защиты информации и принимать меры по обеспечению ее безопасности. Меры по защите информации также включают разнообразные способы и средства, в том числе документы, определяющие доступ сотрудников к защищаемой информации в конкретном структурном подразделении организации.

Следовательно, **система защиты информации представляет собой модель системы, объединяющей силы и средства организации, обеспечивающие защиту информации.** Она описывается параметрами на рис. 1.

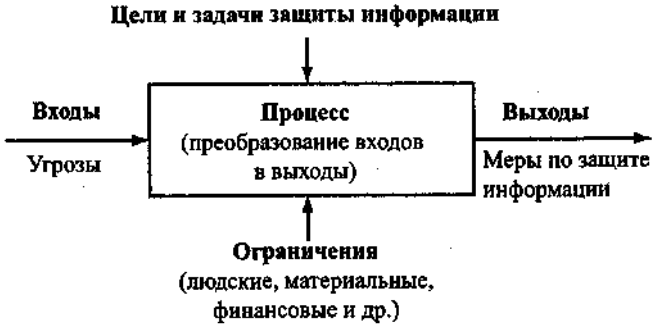

Рис. 1. Параметры системы защиты информации

К параметрам системы, по терминологии, относятся:

- цели и задачи (конкретизированные в пространстве и во времени цели);
- входы и выходы системы;
- ограничения, которые необходимо учитывать при построении (модернизации, оптимизации) системы;
- процессы внутри системы, обеспечивающие преобразование входов в выходы.

Цели представляют собой ожидаемые результаты функционирования системы защиты информации, а **задачи** то, что надо сделать для того, чтобы система могла обеспечить достижение поставленных целей. Возможность решения задач зависит от **ресурса,** выделяемого на защиту информации. Ресурс включает в себя людей, решающих задачи защиты информации, финансовые, технические и другие средства, расходуемые на защиту информации. **Входами** системы защиты информации являются угрозы информации, а **выходами** — меры, которые надо применить для предотвращения угроз или снизив их до допустимого уровня. Наконец, мероприятия, действия и технологии, определяющие меры защиты, соответствующие угрозам, образуют **процесс.**

Так как для слабоформализуемых задач нет методов их точного решения, то процесс представляет собой выбор для угроз на входе системы рациональных вариантов защиты, удовлетворяющих значениям используемых показателей эффективности защиты. Следовательно, процесс выбора должен включать также **показатели эффективности,** по которым производится выбор мер из множества известных. При отсутствии формальных методов решения слабоформализуемых задач в общем случае можно обеспечить лишь выбор рациональных решений, удовлетворяющих определенным требованиям и образующих область решений, внутри которой находится оптимальное решение.

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы, не обеспечивающей требуемый уровень защищенности, в систему с заданным уровнем безопасности информации.

Цели, задачи и ресурсы системы защиты информации

Формулирование целей и задач защиты информации, как любой другой деятельности, представляет начальный и значимый этап обеспечения безопасности информации. Важность этого этапа часто недооценивается и ограничивается целями и задачами, напоминающими лозунги. В то же время специалисты в области системного анализа считают, что от четкости и конкретности целей и постановок задач во многом зависит успех в их достижении и решении. Провал

многих, в принципе полезных, начинаний обусловлен именно неопределенностью и расплывчатостью целей и задач, из которых не ясно, кто, что и за счет какого ресурса предполагает решать продекларированные задачи.

Цели защиты информации сформулированы в ст. 20 Закона РФ «Об информации, информатизации и защите информации»:

- предотвращение утечки, хищения, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в ин

формационные ресурсы и информационные системы, обеспечение правового режима как объекта собственности;

- защита конституционных прав граждан по сохранению личной тайны, конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

В общем виде цель защиты информации определяется как обеспечение безопасности информации, содержащей государственную или иные тайны. Но такая постановка цели содержит неопределенные понятия: **информация** и **безопасность.**

Информация — первичное понятие, используемое в понятийном аппарате информационной безопасности. Предпринимаются многочисленные попытки дать корректное определение понятию «информация», но список попыток пока не закрыт. Учитывая, что любой материальный объект или физическое явление отображаются в виде совокупности признаков (свойств), а человек, кроме того, на основе этих признаков формирует их модели или образы, то информацию