Содержание:

ВВЕДЕНИЕ

Примечательная особенность нынешнего периода — переход от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергетические ресурсы. Ресурсами, как известно, называют элементы экономического потенциала, которыми располагает общество и которые при необходимости могут быть использованы для достижения конкретных целей 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. В при водимой литературе так излагается это понятие: «Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и 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 производства 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 соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий 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.

1. Основные определения и критерии классификации угроз

1.1 Основные понятия об угрозах

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется *атакой*, а тот, кто предпринимает такую попытку - *злоумышленником*. Потенциальные злоумышленники называются *источниками угрозы*.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется *окном опасности*, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест время существования *окна опасности определяются* следующими событиями:

1. должно стать известно о средствах использования пробела в защите;

2. должны быть выпущены соответствующие заплаты;

3. заплаты должны быть установлены в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - как можно более оперативно.

Некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

1.2 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 (рис. 1.1), что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации.

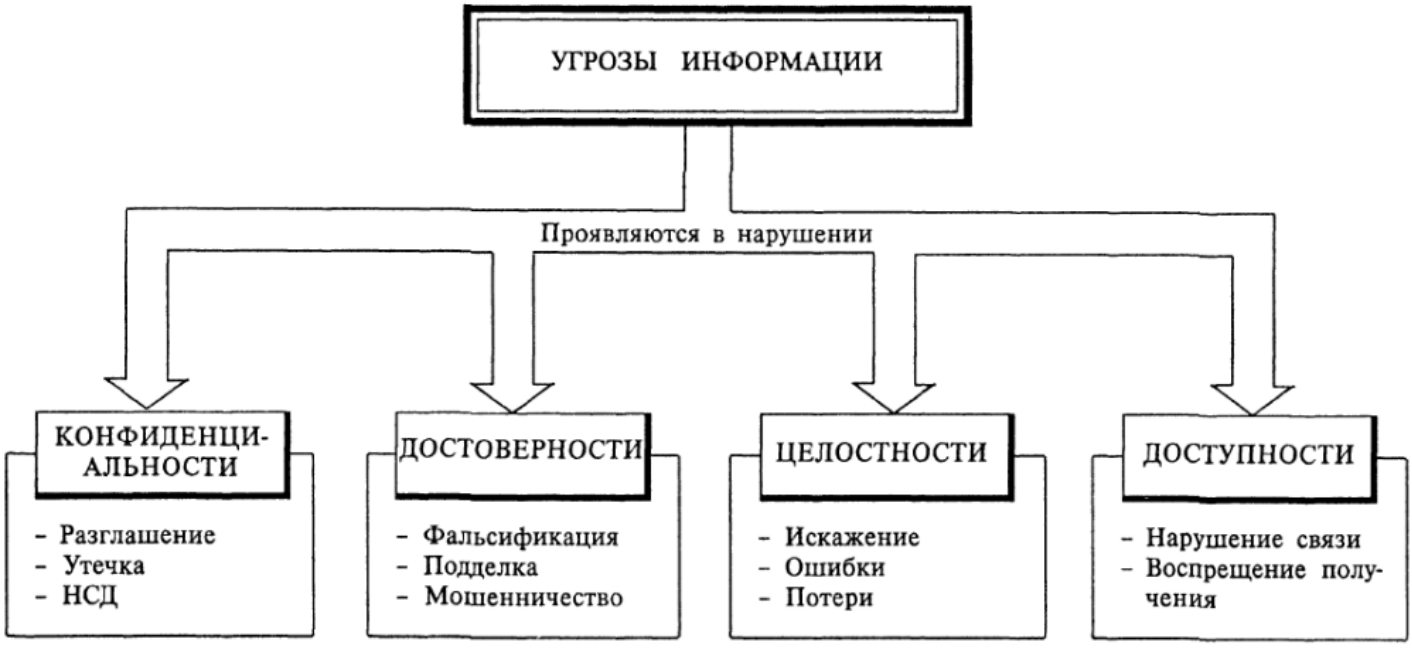

Рис. 1.1

Каждая угроза влечет за собой определенный ущерб — моральный или материальный, а защита и противодействие угрозе призваны 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, (рис. 1.2):

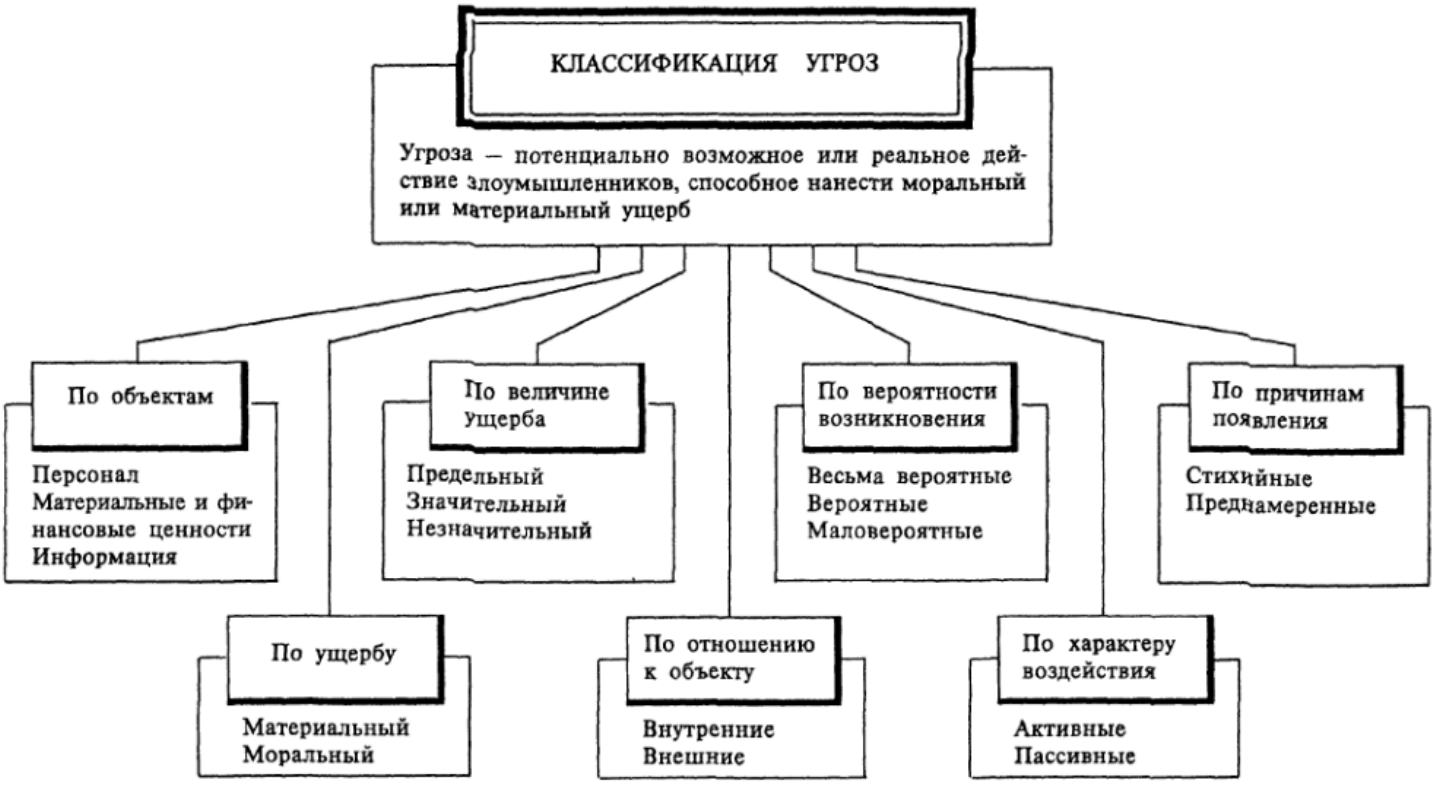

Рис. 1.2

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 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.

1.3 Угрозы информационной безопасности

Угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации. Классификация угроз представлена на рисунке 3.

Рис. 1.3

Основной целью защиты информации является обеспечение заданного уровня её безопасности.

Под *заданным уровнем безопасности информации* понимается такое состояние защищенности информации от угроз, при котором обеспечивается допустимый риск её уничтожения, изменения и хищения (не обеспечивается конфиденциальность, целостность и доступность.

При этом под уничтожением информации понимается не только её физическое уничтожение, но и стойкое блокирование санкционированного доступа к ней.

В общем случае при блокировке информации в результате неисправности замка или утери ключа сейфа, забывания пароля компьютера, искажения кода загрузочного сектора винчестера или дискеты и других факторах информация не искажается и не похищается и при определенных усилиях доступ к ней может быть восстановлен. Следовательно, блокирование информации прямой угрозы ее безопасности не создаст. При этом под уничтожением информации понимается не только её физическое уничтожение, но и стойкое блокирование санкционированного доступа к ней. При невозможности доступа к ней в нужный момент её пользователь теряет информацию так же, как если бы она были уничтожена.

Угроза может быть реализована с различной вероятностью. Вероятность реализации утраты безопасности информации определяет риск ее владельца.

Допустимость риска означает, что ущерб в результате реализации угроз не приведет к серьезным последствиям для собственника информации.

Ущерб может проявляться в разнообразных формах:

- неполучение прибыли, ожидаемой от информации при её материализации в новой продукции или принятии более обоснованного решения;
- дополнительные затраты на замену образцов техники, характеристики которой стали известны конкуренту;
- и другие.

По некоторым оценкам, например, попадание к конкуренту около 20% объёма конфиденциальной информации фирмы может привести к ее банкротству.

Риск владельца информации зависит от уровня инженерно-технической защиты информации, который, в свою очередь, определяется ресурсами системы.

Ресурс может быть определен в виде количества людей, привлекаемых к защите информации, в виде инженерных конструкций и технических средств, применяемых для защиты, денежных сумм для оплаты труда людей, строительства, разработки и покупки технических средств, их эксплуатации и других расходов.

2. Организационные источники и каналы утечки информации

2.1 Основы теории информации. Коммуникационный процесс

Чтобы дать исчерпывающую характеристику реального состояния объекта информационной безопасности в конкретный момент времени, необходимо описать не только сущность, виды и основы формирования угроз его информационной безопасности, но и возможные каналы утечки конфиденциальной информации.

В первую очередь необходимо рассмотреть основные понятия и некоторые основополагающие принципы теории информации.

Теория информации изучает количественные меры информации и способность различных систем передавать, хранить и обрабатывать информацию. Главная задача теории информации заключается в обнаружении математических закономерностей, управляющих системами, разработанными для связи и манипулирования информацией. Сходный круг вопросов исследует теория связи, однако она ориентирована больше на фундаментальные ограничения в области обработки и передачи информации, чем на сущность и порядок функционирования используемых средств и устройств. Теория информации может служить основой для изучения коммуникационного процесса с точки зрения различных проявлений негативного воздействия на передаваемую (обрабатываемую) в рамках этого процесса информацию, в особенности на информацию, подлежащую защите.

Предлагаемые для рассмотрения основные понятия теории информации неразрывно связаны с элементами структуры системы связи, а в некоторых случаях они сами являются этими элементами. Сравнение и сопоставление элементов поможет представить систему передачи конфиденциальной информации в форме некоторого коммуникационного процесса.

Источник информации — объект, осуществляющий выбор из всей совокупности информационных сообщений одного сообщения, подлежащего передаче по каналу связи адресату. В нашем случае источником информации может быть сотрудник предприятия, в установленном порядке допущенный к конфиденциальной

информации, работающий с документами или иными ее носителями. В процессе разработки (формирования) документа осуществляется преобразование информации в форму сообщения.

Сообщение — набор знаков (текст документа), с помощью которых сведения могут быть переданы другому объекту и восприняты им. В отдельных случаях в целях исключения (существенного уменьшения) вероятности овладения посторонним лицом (злоумышленником) охраняемой информацией преобразование информации в текст документа осуществляется с использованием криптографических или программно-аппаратных средств защиты.

Отправитель сообщения — объект, осуществляющий непосредственную передачу документа, содержащего конфиденциальную информацию, адресату. В роли отправителя документа может выступать сотрудник режимно-секретного подразделения (службы безопасности) предприятия, осуществляющий непосредственную отправку (доставку) документа по назначению (в соответствии с указанным адресом). Также отправителем может быть оператор (сотрудник структурного подразделения), осуществляющий передачу документа с использованием технических средств передачи и обработки информации (технических средств связи).

Передатчик — устройство, выполняющее функцию обработки сообщения в соответствии с выбранным алгоритмом и формирования сигнала для непосредственной его передачи по каналу связи (информационному каналу).

Канал распространения (информационный канал или канал связи) — среда, используемая для передачи сообщения (информации) от передатчика к приемнику. Иными словами, канал представляет собой пространство между отправителем сообщения и его получателем, характеризуемое определенным расстоянием. При этом *информационный канал* — среда передачи сообщения в документированном (текстовом) виде, а канал связи служит для обмена информацией, представленной в речевой (звуковой, символьной и т. п.) форме. Во время передачи по каналу связи (информационному каналу) передаваемый сигнал и сообщение, содержащее конфиденциальную информацию, могут быть подвергнуты определенному воздействию. На сигнал воздействуют помехи, он может искажаться при передаче по каналу связи. Воздействие на сообщение может представлять собой попытки овладения содержащейся в нем информацией со стороны злоумышленника (противника, недоброжелателя, конкурента).

Приемник — элемент, выполняющий функцию, обратную функции передатчика. Иными словами, приемник преобразует принятый сигнал и восстанавливает по нему первоначальное сообщение. В рамках системы информационного обмена (в том числе документированной информацией) приемник можно представить в форме объекта, выполняющего также функцию доставки сообщения его получателю.

Получатель информации — объект (лицо), осуществляющий фактический прием, обработку (приведение к документальному виду) и подготовку сообщения для его непосредственного доведения до сведения адресата.

В роли получателя сообщения может выступить работник службы безопасности (режимно-секретного подразделения), функционально отвечающий за получение, учет, регистрацию и доведение до сведения конкретного адресата сообщения, преобразованного в форму документа.

Адресат — должностное лицо (сотрудник предприятия), для которого предназначается передаваемая и принимаемая информация.

При выполнении элементами коммуникационного процесса своих функций возникают объективные возможности негативного воздействия со стороны злоумышленника на передаваемую и принимаемую (обрабатываемую, преобразуемую) информацию. Вследствие этого воздействия появляются каналы утечки конфиденциальной информации независимо от формы ее представления и состояния (существует ли она в форме сообщения или находится в открытом, уже преобразованном для использования виде, обработана или находится в стадии подготовки для доведения до сведения адресата и т.д.).

2.2. Источники конфиденциальной информации и каналы ее утечки

Основными *источниками конфиденциальной информации* являются:

- персонал предприятия, допущенный к конфиденциальной информации;
- носители конфиденциальной информации (документы, изделия);
- технические средства, предназначенные для хранения и обработки информации;
- средства коммуникации, используемые в целях передачи информации;

- передаваемые по каналам связи сообщения, содержащие конфиденциальную информацию.

Способы обмена конфиденциальной информацией (например, между сотрудниками предприятия) могут носить как непосредственный (личный) характер, так и характер передачи формируемых на основе информации сообщений посредством технических средств и средств коммуникаций (различных средств и систем связи).

Из существующих способов обмена конфиденциальной информацией необходимо выделить о*рганизационные каналы передачи и обмена информацией*:

- конфиденциальное делопроизводство (защищенный документооборот);
- совместные работы, выполняемые предприятием по направлениям его производственной и иной деятельности;
- совещания (конференции), в ходе которых обсуждаются вопросы конфиденциального характера;
- рекламная и издательская (публикаторская) деятельность;
- различные мероприятия в области сотрудничества с иностранными государствами (их представителями и организациями), связанные с обменом информацией;
- научные исследования, деятельность диссертационных и иных советов учреждений и организаций;
- передача сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекторские и надзорные органы.

Организационные каналы передачи и обмена конфиденциальной информацией в ходе их функционирования могут быть подвергнуты негативному воздействию со стороны злоумышленников, направленному на получение этой информации. Данное воздействие, в свою очередь, может привести к возникновению каналов утечки конфиденциальной информации и потребовать от руководства предприятия, руководителей структурных подразделений и персонала принятия мер по защите конфиденциальной информации, направленных на недопущение ее утечки и несанкционированного распространения (утраты носителей конфиденциальной информации).

Для определения необходимых мер по защите информации. Нужно провести классификацию всех возможных каналов утечки информации в зависимости от направлений и специфики деятельности предприятия, видов конфиденциальной информации, особенностей функционирования системы защиты информации и

иных факторов.

Организационные каналы утечки конфиденциальной информации, возникающие в процессе деятельности предприятия, подразделяйся следующим образом:

- по источникам угроз защищаемой информации (внешние и утренние);
- по видам конфиденциальной информации или тайн (государственная, коммерческая, служебная или иная тайна; персональные данные сотрудников предприятия);
- по источникам конфиденциальной информации (персонал, носители информации, технические средства хранения и обработки информации, средства коммуникации, передаваемые или принимаемые сообщения и т.п.);
- по способам или средствам доступа к защищаемой информации (применение технических средств, непосредственная и целее направленная работа с персоналом предприятия, осуществление непосредственного доступа к информации, получение доступа к защищаемой информации агентурным путем);
- по характеру взаимодействия с партнерами (каналы утечки, возникающие в отсутствие взаимодействия, при осуществлении взаимодействия, в условиях конкурентной борьбы);
- по продолжительности или времени действия (каналы утечки постоянного, кратковременного, а также периодического или эпизодического действия);
- по направлениям деятельности предприятия (каналы утечки, возникающие в обычных условиях или при повседневной деятельности предприятия, при выполнении совместных работ, осуществлении международного сотрудничества, проведении совещаний, выезде персонала за границу, в ходе рекламной и публикаторской или издательской деятельности, при проведении научных исследований или командировании сотрудников предприятия);
- по причинам возникновения каналов утечки информации Действия злоумышленников, ошибки персонала, разглашение конфиденциальной информации, случайные обстоятельства);

Далее по тексту термин «защита информации» распространяется только на информацию, в установленном порядке отнесенную к конфиденциальной информации, если иное не оговорено особо.

- по каналам коммуникации, используемым для передачи, приема или обработки конфиденциальной информации (каналы утечки, возникающие при хранении, приеме-передаче, обработке или преобразовании информации, а

также в канале связи, по которому передается информация);
- по месту возникновения каналов утечки информации (каналы утечки, возникающие за пределами территории предприятия или на территории предприятия — в служебных помещениях, на объектах информатизации, объектах связи и в других местах);
- по используемым способам и методам защиты информации (каналы утечки, возникающие при нарушении установленных требований по порядку отнесения информации к категории конфиденциальной, обращения с носителями информации, ограничения круга допускаемых к информации лиц, непосредственного доступа к информации персонала предприятия или командированных лиц, а также по причине нарушения требований пропускного или внутриобъектового режимов).

Задачи по исключению возможных каналов утечки конфиденциальной информации решаются как отдельными должностными лицами (персоналом), так и структурными подразделениями предприятия, создаваемыми и функционирующими по различным направлениям защиты информации. Успешное решение этих задач невозможно без применения совокупности средств и методов защиты информации. Классификация сил, средств, способов и методов защиты информации, а также порядок их применения (использования) рассмотрены в соответствующих главах учебника.

Для более полного представления о системе защиты информации предприятия, силах, средствах, способах, методах защиты информации, мероприятиях, планируемых и проводимых в целях обеспечения информационной безопасности, необходимо рассмотреть основы организационной составляющей системы защиты конфиденциальной информации предприятия как наиболее важного направления деятельности предприятия по защите информации.

3. Организационные основы защиты информации на предприятии

3.1 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, понимания 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, в том числе правовых и инженерно-технических, 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 на рис. 3.1.

Рис. 3.1

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.

3.2 Источники конфиденциальной информации и каналы ее утечки

Основными источниками конфиденциальной информации являются:

- персонал предприятия, допущенный к конфиденциальной информации;
- носители конфиденциальной информации (документы, изделия);
- технические средства, предназначенные для хранения и обработки информации;
- средства коммуникации, используемые в целях передачи информации;
- передаваемые по каналам связи сообщения, содержащие конфиденциальную информацию.

Способы обмена конфиденциальной информацией (например, между сотрудниками предприятия) могут носить как непосредственный (личный) характер, так и характер передачи формируемых на основе информации сообщений посредством технических средств и средств коммуникаций (различных средств и систем связи).

Из существующих способов обмена конфиденциальной информацией необходимо выделить организационные каналы передачи и обмена информацией:

- конфиденциальное делопроизводство (защищенный документооборот);
- совместные работы, выполняемые предприятием по направлениям его производственной и иной деятельности;

- совещания (конференции), в ходе которых обсуждаются вопросы конфиденциального характера;
- рекламная и издательская (публикаторская) деятельность;
- различные мероприятия в области сотрудничества с иностранными государствами (их представителями и организациями), связанные с обменом информацией;
- научные исследования, деятельность диссертационных и иных советов учреждений и организаций;
- передача сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекторские и надзорные органы.

Организационные каналы передачи и обмена конфиденциальной информацией в ходе их функционирования могут быть подвергнуты негативному воздействию со стороны злоумышленников, направленному на получение этой информации. Данное воздействие, в свою очередь, может привести к возникновению каналов утечки конфиденциальной информации и потребовать от руководства предприятия, руководителей структурных подразделений и персонала принятия мер по защите конфиденциальной информации, направленных на недопущение ее утечки и несанкционированного распространения (утраты носителей конфиденциальной информации).

Для определения необходимых мер по защите информации. Нужно провести классификацию всех возможных каналов утечки информации в зависимости от направлений и специфики деятельности предприятия, видов конфиденциальной информации, особенностей функционирования системы защиты информации и иных факторов.

Организационные каналы утечки конфиденциальной информации, возникающие в процессе деятельности предприятия, подразделяйся следующим образом:

- по источникам угроз защищаемой информации (внешние и утренние);
- по видам конфиденциальной информации или тайн (государственная, коммерческая, служебная или иная тайна; персональные данные сотрудников предприятия);
- по источникам конфиденциальной информации (персонал, носители информации, технические средства хранения и обработки информации, средства коммуникации, передаваемые или принимаемые сообщения и т.п.);
- по способам или средствам доступа к защищаемой информации (применение технических средств, непосредственная и целее направленная работа с

персоналом предприятия, осуществление непосредственного доступа к информации, получение доступа к защищаемой информации агентурным путем);
- по характеру взаимодействия с партнерами (каналы утечки, возникающие в отсутствие взаимодействия, при осуществлении взаимодействия, в условиях конкурентной борьбы);
- по продолжительности или времени действия (каналы утечки постоянного, кратковременного, а также периодического или эпизодического действия);
- по направлениям деятельности предприятия (каналы утечки, возникающие в обычных условиях или при повседневной деятельности предприятия, при выполнении совместных работ, осуществлении международного сотрудничества, проведении совещаний, выезде персонала за границу, в ходе рекламной и публикаторской или издательской деятельности, при проведении научных исследований или командировании сотрудников предприятия);
- по причинам возникновения каналов утечки информации Действия злоумышленников, ошибки персонала, разглашение конфиденциальной информации, случайные обстоятельства);

Далее по тексту термин «защита информации» распространяется только на Формацию, в установленном порядке отнесенную к конфиденциальной информации, если иное не оговорено особо.

- по каналам коммуникации, используемым для передачи, приема или обработки конфиденциальной информации (каналы утечки, возникающие при хранении, приеме-передаче, обработке или преобразовании информации, а также в канале связи, по которому передается информация);
- по месту возникновения каналов утечки информации (каналы утечки, возникающие за пределами территории предприятия или на территории предприятия — в служебных помещениях, на объектах информатизации, объектах связи и в других местах);
- по используемым способам и методам защиты информации (каналы утечки, возникающие при нарушении установленных требований по порядку отнесения информации к категории конфиденциальной, обращения с носителями информации, ограничения круга допускаемых к информации лиц, непосредственного доступа к информации персонала предприятия или командированных лиц, а также по причине нарушения требований пропускного или внутриобъектового режимов).

Задачи по исключению возможных каналов утечки конфиденциальной информации решаются как отдельными должностными лицами (персоналом), так и структурными подразделениями предприятия, создаваемыми и функционирующими по различным направлениям защиты информации. Успешное решение этих задач невозможно без применения совокупности средств и методов защиты информации. Классификация сил, средств, способов и методов защиты информации, а также порядок их применения (использования) рассмотрены в соответствующих главах учебника.

Для более полного представления о системе защиты информации предприятия, силах, средствах, способах, методах защиты информации, мероприятиях, планируемых и проводимых в целях обеспечения информационной безопасности, необходимо рассмотреть основы организационной составляющей системы защиты конфиденциальной информации предприятия как наиболее важного направления деятельности предприятия по защите информации.

4. ОРГАНИЗАЦИЯ АНАЛИТИЧЕСКОЙ РАБОТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

4.1 Основные направления аналитической работы. Функции аналитического подразделения

Анализ состояния защиты информации — это комплексное изучение фактов, событий, процессов, явлений, связанных с проблемами защиты информации, в том числе данных о состоянии работы по выявлению возможных каналов утечки информации, о причинах и обстоятельствах, способствующих утечке и нарушениям режима секретности (конфиденциальности) в ходе повседневной деятельности предприятия.

Основное предназначение аналитической работы — выработка эффективных мер, предложений и рекомендаций руководству предприятия, направленных на недопущение утечки конфиденциальной информации о деятельности предприятия и проводимых работах. Аналитическая работа должна включать элементы прогнозирования возможных действий противника по получению важной

защищаемой информации.

Основные *направления аналитической работы* на предприятии следующие:

- анализ объекта защиты;
- анализ внутренних и внешних угроз информационной без опасности предприятия;
- анализ возможных каналов несанкционированного доступа к информации;
- анализ системы комплексной безопасности объектов;
- анализ имеющих место нарушений режима конфиденциальности информации;
- анализ предпосылок к разглашению информации, а также к утрате носителей конфиденциальной информации.

Функции анализа на предприятии возлагаются на специально создаваемое в его структуре аналитическое подразделение, которое комплектуется квалифицированными специалистами в области защиты информации. Вместе с тем, данные специалисты должны в полной мере владеть информацией по всем направлениям деятельности предприятия: знать виды, характер и последовательность выполнения производственных работ, взаимодействующие организации, специфику деятельности структурных подразделений предприятия и т.д. Как правило, аналитическое подразделение включается в состав службы безопасности предприятия.

Аналитическое подразделение должно обеспечивать руководство предприятия достоверной и аналитически обработанной информацией, необходимой для принятия эффективных управленческих решений по всем направлениям защиты информации. Основными функциями аналитического подразделения являются:

- обеспечение своевременного поступления достоверных и всесторонних сведений по проблемам защиты информации;
- учет, обобщение и постоянный анализ материалов о состоянии дел в системе защиты информации предприятия (его филиалов и представительств);
- анализ возможных угроз защите информации, моделирование реального сценария возможных действий конкурентов (злоумышленников), затрагивающих интересы предприятия;
- обеспечение эффективности работы по анализу имеющейся информации, исключение дублирования при ее сборе, обработке и распространении;

- мониторинг ситуации на рынке продукции, товаров и услуг, а также во внешней среде в целях выявления событий и фактов, которые могут иметь значение для деятельности предприятия;
- обеспечение безопасности собственных информационных ресурсов, ограничение доступа сотрудников предприятия к аналитической информации;
- подготовка выводов и предложений, направленных на повышение эффективности планируемых и принимаемых мер по защите информации, а также уточнение (корректировку) организационно-планирующих документов предприятия и его структурных подразделений;
- выработка рекомендаций по внесению изменений и дополнений в методические документы, регламентирующие алгоритм действий сотрудников предприятия по защите информации (стандарты предприятия).

Наличие постоянной аналитической работы, ее характер и результаты определяют необходимость, основы организации, структуру и содержание системы комплексной защиты информации, требования к ее эффективности и направления ее развития и совершенствования. Анализ состояния системы защиты информации существенно влияет на количество, состав и структуру подразделений предприятия, непосредственно решающих эти задачи (служба безопасности предприятия, служба охраны, режимно-секретное подразделение и др.). От эффективности и качества ведения на предприятии аналитической работы в полной мере зависит состояние защищенности информационных ресурсов предприятия, отнесенных к категории охраняемых, а также своевременность и обоснованность принятия мер по исключению утечки конфиденциальной информации и утрат носителей информации. Эффективность аналитической работы и ее результаты служат основой для принятия руководством предприятия управленческих решений по вопросам организации защиты информации. С учетом результатов аналитической работы могут вырабатываться следующие основные меры:

- уточнение (доработка) планов работы предприятия по защите информации, включение в них дополнительных мероприятий;
- уточнение распределения задач и функций между структурными подразделениями предприятия;
- переработка (уточнение) должностных (функциональных) обязанностей сотрудников предприятия, в том числе руководящего звена, совершенствование систем пропускного и внутри-объектового режимов;

- ограничение круга лиц, допускаемых к конфиденциальной информации по различным направлениям деятельности предприятия;
- пересмотр степени конфиденциальности сведений и их носителей;
- усиление системы охраны предприятия и его объектов, применение особых мер защиты информации на отдельных объектах (в служебных помещениях);
- принятие решений об ограничении публикации в открытой печати, использования в рекламной и издательской деятельности отдельных материалов (материалов по отдельным темам), доступа командированных лиц, об исключении рассмотрения этих мате риалов на конференциях, семинарах, встречах и т.д.

Ведение эффективной аналитической работы возможно лишь при наличии необходимой информации. Для ее получения нужна четко сформулированная цель, определяющая конкретные источники информации. Аналитическая работа на предприятии должна вестись последовательно и непрерывно, представлять собой в полной мере целостное исследование.

В аналитической работе можно выделить следующие основные этапы:

1) формулирование целей аналитической работы, разработка программы исследований, формулирование предварительных гипотез (результатов аналитической работы);

2) отбор и анализ источников информации, сбор и обобщение информации;

3) полноценный анализ имеющейся информации и подготовка выводов.

Основная форма ведения аналитической работы — аналитические исследования.

Проведение аналитических исследований требует четкой организации процесса, оценки имеющихся ресурсов для выполнения исследований и достижения необходимого результата. Итогом исследования должны быть выводы, предложения и рекомендации по совершенствованию системы защиты информации.

На первом этапе аналитического исследования формулируются цели и задачи исследования, разрабатывается программа исследования, которая составляет научную основу сбора, обобщения, обработки и анализа всей полученной информации. Типовая программа исследований включает следующие основные разделы:

- цели и задачи аналитического исследования;
- предметы и объекты исследования;
- сроки (период) проведения аналитического исследования;
- методики проведения исследования;
- ожидаемые результаты и предполагаемые выводы.

При формулировании целей и задач исследования нужно учитывать, кто является его организатором и непосредственным исполнителем, какие силы и средства могут быть задействованы для его проведения, какие будут использоваться источники информации, способы и методы ее сбора, обработки и анализа, какие существуют возможности для реализации предложений и рекомендаций, которые будут выработаны в ходе исследований.

В зависимости от поставленных целей и задач определяются конкретные методы и технологии исследования, а также процедуры сбора и обработки информации.

Наиболее типичны следующие задачи аналитического исследования:

- получение данных о состоянии системы защиты информации на предприятии (его конкретных объектах, в филиалах, представительствах);
- выявление возможных каналов утечки информации, подлежащей защите;
- определение обстоятельств, причин и факторов, способствующих возникновению каналов утечки и созданию предпосылок для утечки информации;
- подготовка для руководства предприятия (филиала, представительства) и его структурных подразделений конкретных рекомендаций по закрытию выявленных каналов утечки.

Под объектом исследования понимается все то, что изучается и анализируется в ходе исследования. Предмет исследования — та сторона объекта, которая непосредственно подлежит изучению в ходе аналитического исследования.

Особое значение на первом этапе аналитической работы имеет формулирование предварительных гипотез (версий). Предварительные гипотезы должны объяснить роль и место выводов аналитических исследований в логической последовательности происходящих событий в сфере защиты охраняемой информации.

Построение предварительные гипотез проводится в следующем порядке. Сначала формируется полный список сведений, которые предполагается исследовать

(проанализировать). Вошедшие в список сведения систематизируются и располагаются по степени важности. Далее из всего объема иуформации выделяется группа наиболее значимых сведений, роль которых особенно очевидна в ситуации, подлежащей анализу и оценке. Выбранные сведения классифицируются по актуальности, способу получения и степени достоверности источника. Наиболее актуальные сведения анализируются в первую очередь.

Затем проводится выбор предварительных гипотез, объясняющих проявления тех или иных событий (появление тех или иных сведений). Причем в отношении одного события осуществляется проверка нескольких гипотез (версий). При последовательной проверке гипотез особое внимание уделяется наиболее реальным. Эти гипотезы фиксируются. Наименее реальные гипотезы отклоняются.

Таким образом последовательно выбираются и формулируются наиболее вероятные предположения, объясняющие появление тех или иных конкретных событий (возникновение сведений). Возможные противоречия в полученных выводах о предполагаемых версиях происходящих событий устраняются путем всесторонней последовательной проверки реальности гипотез.

Результатом работы по формулированию предварительных гипотез является выбор версии, которая наиболее точно по сравнению с другими версиями объясняет причину возникновения конкретной ситуации, связанной с появлением возможного канала утечки конфиденциальной информации, и характеризует состояние системы защиты информации, в том числе — действия соответствующих должностных лиц, качество выполнения мероприятий и т.д.

На втором этапе проводится отбор и анализ источников информации, сбор и обобщение данных в целях выявления канала несанкционированного доступа к сведениям конфиденциального характера, исключения возможности возникновения такого канала. Для этого осуществляется постоянный контроль объектов защиты (информационных ресурсов), а также степени защищенности, обрабатываемой (циркулирующей) в них информации, проводится анализ данных, получаемых из различных источников.

Для решения конкретной задачи аналитического исследования в рамках второго этапа из всех имеющихся в распоряжении аналитического подразделения источников информации отбираются те, из которых поступает информация, наиболее близкая к исследуемым проблемам, и в то же время достаточно достоверная.

Аналитическое исследование источников информации предусматривает проведение следующих основных мероприятий:

- формирование исчерпывающего перечня источников конфиденциальной информации на предприятии;
- формирование и своевременное уточнение перечня и состава конфиденциальной информации, реально циркулирующей (обрабатываемой) на объектах предприятия, с указанием конкретных носителей, на которых она хранится;
- организация и ведение учета осведомленности сотрудников предприятия в конфиденциальной информации, накопление данных об их ознакомлении с конкретными сведениями конфиденциального характера с указанием носителей этих сведений;
- изучение и оценка соответствия степени конфиденциальности, присвоенной информации, реальной ценности этой информации;
- изучение внутренних и внешних угроз каждому имеющемуся на предприятии источнику конфиденциальной информации1;
- выявление предприятий, заинтересованных в получении конфиденциальной информации (фирм-конкурентов), а также отдельных лиц-злоумышленников и их систематизация (классификация);
- анализ полноты и качества мер по защите конфиденциальной информации, принимаемых (принятых) в конкретных ситуациях. Учет и анализ попыток представителей фирм-конкурентов, а также других злоумышленников получить конфиденциальную информацию;
- учет и анализ контактов сотрудников предприятия с представителями фирм-конкурентов вне зависимости от того, касались ли они вопросов конфиденциального характера или нет.

В ходе изучения и исследования источников информации производится их оценка с точки зрения надежности и достоверности получаемой из них информации. Оценка источников информации осуществляется методом ранжирования (классификации) самих источников, поступающей из них информации и способов ее получения. В большинстве случаев может использоваться система экспертной оценки (непосредственно аналитиком) надежности и достоверности полученных данных. Уровень подготовки и практические навыки позволяют сотруднику аналитического подразделения наиболее точно оценить собственно информацию, ее источник и способ ее получения.

При проведении оценки указанных элементов, как правило, используются следующие критерии:

1. Оценка источника:

- надежный источник;
- обычно надежный источник;
- довольно надежный источник;
- не всегда надежный источник;
- ненадежный источник;
- источник неустановленной надежности.

2. Оценка полученной информации:

- информация, подтвержденная другими фактами;
- информация, подтвержденная другими источниками;
- информация, с высокой степенью вероятности соответствующая действительности;
- информация, возможно соответствующая действительности;
- сомнительная информация;
- неправдоподобная информация;
- информация, установить (подтвердить) достоверность которой не представляется возможным.

3. Оценка способа получения информации источником:

- информация получена источником самостоятельно;
- информация получена источником из другого постоянного источника информации (например, открытого источника);
- информация получена источником из другого «разового» источника (например, в ходе переговоров, неформального общения).

В ходе оценки достоверности информации и ее источника необходимо учитывать возможность преднамеренной дезинформации, а также получения непреднамеренно искаженной информации. В обоих случаях необходимо проведение дополнительной проверки и более подробного всестороннего анализа полученной информации для принятия решения о ее использовании в ходе аналитических исследований.

С учетом результатов оценки полученной информации, а также источников и способов ее получения осуществляются сбор и обобщение (систематизация) необходимых для проведения полноценного анализа сведений.

В ходе третьего этапа аналитической работы проводится полноценный анализ полученной информации и, на основе его результатов, — всесторонний анализ состояния системы защиты информации, вырабатываются эффективные меры по ее совершенствованию. На этом этапе оформляются результаты аналитических исследований, готовятся выводы, рекомендации и предложения в области защиты охраняемой информации.

Анализ состояния системы защиты информации включает изучение возможных каналов утечки информации, оценку эффективности мер по их закрытию, оценку действий персонала предприятия по решению задач в области защиты информации, определение основных направлений деятельности по защите информации.

4.2 Содержание и основные виды аналитических отчетов

Основной формой представления результатов аналитических исследований является аналитический отчет. Отчеты могут оформляться в письменном виде, также они могут быть представлены в устной форме, сопровождаться графиками, диаграммами, рисунками, таблицами, поясняющими или отражающими результаты проведенной работы.

Основные разделы аналитического отчета следующие:

- цели и задачи аналитического исследования (цели и задачи аналитического исследования, пути решения поставленных задач, вопросы, подлежащие анализу и оценке; предполагаемые результаты исследования);
- источники информации, степень достоверности полученной информации (оценки полученной информации, источников и способов ее получения, результаты анализа степени достоверности полученной с использованием этих источников аналитической информации);
- обобщение полученной информации (алгоритм сбора и обобщения необходимой для проведения полноценного анализа информации — из всего объема полученной и обработанной информации выделяются наиболее

значимые факты);
- основные и альтернативные версии или гипотезы (мотивированное деление версий, объясняющих или характеризующих исследуемые события и факты, на основную и дополнительные или альтернативные);
- недостающая информация (дополнительная информация, необходимая для подтверждения основной версии, ее источники и способы ее получения);
- заключение, выводы (результаты анализа и оценки поставленных вопросов, выводы о степени важности полученной и обработанной информации, значение этой информации для принятия конкретных решений в области защиты конфиденциальной информации, взаимосвязь результатов данного аналитического исследования с другими направлениями аналитической работы в сфере защиты информации, возможные угрозы защищаемой информации, а также возможные последствия воздействия негативных факторов);
- предложения и рекомендации по совершенствованию работы в области защиты информации (конкретные предложения и рекомендации руководству предприятия и руководителям структурных подразделений по совершенствованию работы в области защиты конфиденциальной информации; выработанные на основе проведенного анализа полученной информации, а также различных событий и фактов конкретные меры, принятие которых необходимо для закрытия возможных каналов утечки информации и предотвращения потенциальных угроз защищаемой информации).

В отдельных случаях, на основе результатов проведения более глубокого анализа состояния системы защиты информации вырабатываются алгоритм и способы действий персонала предприятия в конкретных ситуациях.

В зависимости от предназначения используются следующие основные виды аналитических отчетов:

- оперативный (тактический) отчет;
- перспективный (стратегический) отчет;
- периодический отчет.

Оперативные (тактические) отчеты отражают результаты аналитических исследований, проводимых для подготовки и принятия какого-либо оперативного (экстренного) решения по вопросу кратковременного (срочного) характера. В ходе проведения таких исследований анализу и оценке подвергается информация, как

правило, небольшого объема.

Перспективные (стратегические) отчеты содержат информацию, более полную по содержанию. Анализ этой информации не ограничен по сроку (времени) его проведения. В такие отчеты, как правило, включается информация, содержащая более полный анализ предпосылок конкретных ситуаций, фактов, событий. В отчетах излагаются прогнозы и перспективы развития этих ситуаций. Отчеты этого вида соответствуют постоянным направлениям аналитических исследований.

Периодические отчеты предназначены для анализа состояния системы защиты информации (отдельных направлений защиты информации) в соответствии с разработанным и утвержденным руководством предприятия графиком. Эти отчеты не зависят от происходящих событий (возникновения различных ситуаций), связанных с защитой информации. Такие отчеты готовятся по проблемам (направлениям), являющимся объектами постоянного внимания со стороны службы безопасности предприятия (его аналитического подразделения).

К составлению отчетов, независимо от формы их представления, предъявляются общие требования, такие, как наличие глубокого анализа событий (фактов, полученной информации), простота, четкость и грамотность изложения материала, логичность приводимых рассуждений и выводов, соответствие отчетов установленной форме.

Одно из наиболее важных требований, предъявляемых к отчетам, заключается в том, что их содержание и уровень подготовки аналитического материала должны отвечать запросам конкретных потребителей аналитической информации — руководителей структурных подразделений или отдельных сотрудников предприятия.

4.3 Классификация методов анализа информации

Полнота и качество проведения аналитических исследований, достоверность полученных результатов и эффективность выработанных предложений и рекомендаций в полной мере зависят от тех методов анализа информации, которые были выбраны и использовались сотрудниками аналитического подразделения непосредственно в ходе проведения исследований.

Применяемые в ходе аналитических исследований методы анализа информации делятся на три группы:

1) общенаучные (качественные) методы;

2) количественные методы;

3) частнонаучные методы.

Основные методы анализа, относящиеся к первой группе, включают метод выдвижения гипотез, метод интуиции, метод наблюдения, метод сравнения, метод эксперимента.

Из количественных методов наиболее распространен метод статистических исследований.

К третьей группе относятся методы письменного и устного опроса, метод индивидуальной беседы и метод экспертной оценки.

Метод выдвижения гипотез состоит в процедуре отделения известного от неизвестного и вычленения в неизвестном отдельных, наиболее важных элементов и фактов (событий).

Метод интуиции заключается в использовании аналитиком своей способности к непосредственному постижению истины (достижению требуемого результата) без предварительного логического рассуждения. Во многом этот метод основывается наличном опыте аналитика.

Метод наблюдения заключается в непосредственном исследовании (обследовании) конкретного объекта (источника информации, события, действия, факта), в самостоятельном описании аналитиком каких-либо фактов (событий, процессов), а также их логических связей в течение определенного времени.

Цель метода сравнения состоит в более глубоком изучении процессов (событий), происходящих на предприятии и имеющих отношение к вопросам защиты охраняемой информации. Сравниваются различные факторы, обусловливающие причины и обстоятельства, приводящие к утечке конфиденциальной информации или к возникновению предпосылок к ее утечке. При использовании метода; сравнения в обязательном порядке соблюдаются следующие основные условия: сравниваемые объекты (действия, явления, события) должны быть сопоставимы по своим качественным особенностям; сравнение должно определить не только

элементы сходства, но и элементы различия между исследуемыми объектами.

Метод эксперимента используется для проверки результатов деятельности по конкретному направлению защиты информации или для поиска новых решений, совершенствования системы ее защиты.

Роль количественных методов анализа заключается в информационном, статистическом обеспечении качественных методов. Наиболее характерен метод статистических исследований, который заключается в проведении количественного анализа отдельных сторон исследуемого явления (факта, события). В ходе этого анализа накапливаются цифровые данные о состоянии и динамике нарушений режима конфиденциальности (секретности) в ходе проводимых работ, об эффективности решения службой безопасности (режимно-секретным подразделением) задач по их недопущению, о тенденциях развития ситуации в области информационной безопасности и т.д.

Методы письменного и устного опроса заключаются в получении путем анкетирования (или иным способом) необходимой информации от сотрудников предприятия, руководителей подразделений, а также лиц, допускающих нарушения установленного режима секретности (конфиденциальности информации). При этом в анкете указываются несколько возможных вариантов ответов на каждый поставленный вопрос.

Метод индивидуальной беседы отличает от метода письменного и устного опроса необходимость личного общения с сотрудником предприятия. Использование этого метода позволяет в динамично развивающейся беседе получить конкретную информацию в зависимости от целей аналитического исследования.

Метод экспертной оценки включает учет и анализ различных мнений по определенному кругу вопросов, излагаемых специалистами в той или иной области деятельности предприятия, связанной с конфиденциальной информацией.

Выбор конкретных методов анализа при проведении аналитических исследований в области защиты конфиденциальной информации зависит от целей и задач исследований, а также от специфики деятельности предприятия, состава и структуры службы безопасности и ее аналитического подразделения.

ЗАКЛЮЧЕНИЕ

При рассмотрении угроз информационной безопасности объекта особое внимание необходимо уделить классификации подлежащих защите объектов информационной безопасности предприятия. В соответствии с приведенной ранее классификацией угроз по виду объекта воздействия они подразделяются на угрозы собственно информации, угрозы персоналу объекта и угрозы деятельности по обеспечению информационной безопасности объекта. При более детальном рассмотрении угрозы собственно информации можно подразделить на угрозы носителям конфиденциальной информации, местам их размещения (расположения), каналам передачи (системам информационного обмена), а также собственно информации, хранящейся в документированном (электронном) виде на различных носителях.

Таким образом, можно сделать вывод о том, что действие угроз информационной безопасности объекта направлено на создание возможных каналов утечки защищаемой информации (предпосылок к ее утечке) и непосредственно на утечку информации. Одно из ключевых понятий в оценке эффективности проявления угроз объекту информационной безопасности — ущерб, наносимый этому объекту (предприятию) в результате воздействия угроз.

По своей сути любой ущерб, его определение и оценка имеют ярко выраженную экономическую основу. Не является исключением и ущерб, наносимый информационной безопасности объекта (предприятия).

С позиции экономического подхода общий ущерб информационной безопасности предприятия складывается из двух составных частей: прямого и косвенного ущерба.

Прямой ущерб информационной безопасности предприятия возникает вследствие утечки конфиденциальной информации. Косвенный ущерб — потери, которые несет предприятие в связи с ограничениями на распространение информации, в установленном порядке отнесенной к категории конфиденциальной.

Описание ущерба, наносимого предприятию в результате утечки конфиденциальной информации, основывается на его количественных и качественных показателях, которые базируются на одном из принципов засекречивания информации (отнесения ее к категории конфиденциальной) — принципе обоснованности. Он заключается в установлении (путем экспертных

оценок) целесообразности засекречивания конкретных сведений (отнесения содержащейся в них информации к категории конфиденциальной), а также вероятных последствий этих действий, с учетом решаемых предприятием задач и поставленных целей.

Введение ограничений на распространение информации (в связи с ее засекречиванием или отнесением к категории конфиденциальной) приводит и к позитивным, и к негативным последствиям. К основным позитивным последствиям следует отнести предотвращение возможного прямого ущерба информационной безопасности предприятия из-за утечки защищаемой информации. Негативные последствия связаны с наличием (вероятным возрастанием) косвенного ущерба или издержек в виде затрат на защиту информации и величины упущенной выгоды, которая может быть получена при ее открытом распространении.

Общий ущерб безопасности предприятия от утечки конфиденциальной информации определяют следующим образом.

Проводят классификацию всех имеющихся на предприятии сведений по степени их важности. С этой целью методом экспертной оценки с привлечением специалистов структурных подразделений предприятия, участвующих в выполнении работ по различным направлениям его деятельности, разрабатывают единую шкалу сведений, содержащих конфиденциальную информацию — так называемый рейтинг важности информации. В рейтинге отражаются все сведения, включенные в перечни информации, подлежащей защите.

Методической основой для разработки такого рейтинга служит метод экспертного анализа в совокупности с методом объективного количественного оценивания. На основе рейтинга важности информации сопоставляют (соотносят) включенные в него сведения с количественными показателями возможного ущерба, определяемого расчетным или экспертным путем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИОКОВ

1. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.
2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2-е изд.- 2004. - 544 с.
3. Интернет курс «Информационная безопасность», Денисов Д.В.
4. Интернет-портал по вопросам информационной безопасности - http://all-ib.ru/

5. Интернет-портал по вопросам информационной безопасности - https://cyberpedia.su/