МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра «Информационная безопасность»

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие
по изучению дисциплин «Современные технологии информационной безопасности», «Комплексные системы защиты информации»
для студентов очной и очно-заочной форм обучения,
обучающихся по направлению подготовки
10.04.01 «Информационная безопасность» (уровень подготовки – магистр),
10.05.01 «Компьютерная безопасность»

Севастополь
СевГУ
2020

УДК 004.056(075.8)
ББК 32.973.26-018.2я73
С568

Р е ц е н з е н т:
Л.В. Третьякова – д. ф.-м. н., профессор кафедры ВМ института ИТиУТС

Составители: Маслова М.А., Ожиганова М.И.

С568 Современные технологии информационной безопасности : учебно-методическое пособие по изучению дисциплин «Современные технологии информационной безопасности», «Комплексные системы защиты информации», для студентов очной и очно-заочной форм обучения, обучающихся по направлению подготовки 10.04.01 «Информационная безопасность» (уровень подготовки – магистр), 10.05.01 «Компьютерная безопасность» / Сост. М.А. Маслова, М.И. Ожиганова ; Министерство науки и высшего образования Российской Федерации, Севастопольский государственный университет, Институт радиоэлектроники и информационной безопасности, кафедра «Информационная безопасность». – Севастополь : СевГУ, 2020. – 98 с. – Текст : электронный.

Учебно-методическое пособие содержит теоретический материал охватывающий курс лекций, основных законов информационной безопасности, контрольных вопросов для самопроверки и подготовки знаний к экзамену/зачету по дисциплинам «Современные технологии информационной безопасности», «Комплексные системы защиты информации»: 10.04.01 «Информационная безопасность», профиль обучения «Организация и технология защиты информации», 10.05.01 «Компьютерная безопасность» профиль обучения «Информационная безопасность объектов информатизации на базе компьютерных систем».

УДК 004.056(073)
ББК 32.973.26-018.2я73

Рассмотрено и утверждено на заседании кафедры «Информационная безопасность» СевГУ, протокол № 8 от 11 марта 2020 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире защиты информации существует множество отдельных программно-аппаратных, инженерно-технических и криптографических средств защиты информации без которых невозможно обойтись на предприятиях. Но для эффективного использования всех существующих мер защиты информации необходимо четко знать и понимать для чего она используется и в каком направлении, а так же как выбрать и объединить существующие средства и методы для эффективной и постоянной защиты предприятия. Так же необходимо не забывать о человеческом факторе, который играет значимую роль на любом действующем предприятии и может привести к непоправимым последствиям благодаря только маленькой халатности, не беря даже во внимание преднамеренный замысел или преступление. Но необходимо помнить, что для работы предприятия самым важным есть его направление работы и получение прибыли, а создание системы защиты информации является вспомогательным средством. Поэтому при создании системы защиты информации необходимо помнить, что она должна помогать, а не мешать работе предприятия и самое главное оно должно быть экономически выгодным и оправданным, обеспечивая защиту всех важных информационных ресурсов предприятия т всех возможных угроз. Важно помнить, что система должна быть комплексной. В данном учебно-методическом пособии будет рассмотрены все факторы создания системы защиты предприятия и основным нормативные акты для ее работы в сочетании с методами внедрения современных технологий на предприятиях ИБ.

Дисциплина «Современные технологии информационной безопасности» является частью основной образовательной программы высшего профессионального образования направления подготовки 10.04.01 «Информационная безопасность», профиль «Организация и технология защиты информации», квалификация (степень) – магистр.

Цели изучения дисциплины:

- сформировать у студентов знания о структуре комплексной системы защиты информации;
- сформировать у студентов знания о создании политики безопасности для предприятий;
- получение навыков анализа защищаемой информации;
- формирование научного мировоззрения и развитию системного мышления,
- ознакомиться с современными технологиями ИБ и методами их внедрения на предприятиях/организациях.

Задачи освоения дисциплины – дать основы:

– обеспечения и владения основными документами в сфере защиты информации;
– умение определения состава защищаемой информации и ее классификацию по видам;
– процессов сбора, передачи, накопления и просчета необходимой информации;
- овладеть навыками применения современных технологий ИБ,
– определения возможных методов несанкционированного доступа к защищаемой информации.

СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ

СЗИ – система защиты информации
ЗИ – защита информации, защищаемая информация
КСЗИ – комплексная система защиты информации
КС – комплексная система
КТ – коммерческая тайна
ДФ – дестабилизирующие факторы
НСД – несанкционированный доступ
ОС – организационная система, организационная структура
ОУ – объект управления
СУ – субъект управления
ТЭО – технико-экономическое обоснование
ТЗ – техническое задание
ТП – технический проект
ТС – технические средства
СФС – структурно-функциональная схема
СБ – служба безопасности
АСОД – автоматизированная система обработки данных
ИС – информационная система
ГК – гражданский кодекс
ЛПР – лицо, принимающее решения
УР – управленческое решение
ВТ – вычислительная техника
ЧС – чрезвычайная ситуация

ТЕМА 1. СУЩНОСТЬ И ЗАДАЧИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Понятие комплексной системы защиты информации

Работы по защите информации у нас в стране ведутся достаточно интенсивно и уже продолжительное время. Накоплен существенный опыт. Сейчас уже никто не думает, что достаточно провести на предприятии ряд организационных мероприятий, включить в состав автоматизированных систем некоторые технические и программные средства – и этого будет достаточно для обеспечения безопасности.

Главное направление поиска новых путей защиты информации заключается не просто в создании соответствующих механизмов, а представляет собой реализацию регулярного процесса, осуществляемого на всех этапах жизненного цикла систем обработки информации при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и мероприятия, используемые для ЗИ, наиболее рациональным образом объединяются в единый целостный механизм – причём не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала, а также нештатных ситуаций технического характера.

Основной проблемой реализации систем защиты является:

– с одной стороны, обеспечение надёжной защиты, находящейся в системе информации, т.е. исключение случайного и преднамеренного получения информации посторонними лицами, разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;

– с другой стороны, системы защиты не должны создавать заметных неудобств пользователям в ходе их работы с ресурсами системы.

Проблема обеспечения желаемого уровня защиты информации весьма сложная, требующая для своего решения не просто осуществления некоторой совокупности научных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических мероприятий и применения комплекса специальных средств и методов по ЗИ.

На основе теоретических исследований и практических работ в области ЗИ сформулирован системно-концептуальный подход к защите информации.

Под системностью как основной частью системно-концептуального подхода понимается:

а) системность целевая, т.е. защищённость информации рассматривается как основная часть общего понятия качества информации;

б) системность пространственная, предлагающая взаимоувязанное решение всех вопросов защиты на всех компонентах предприятия;

в) системность временная, означающая непрерывность работ по ЗИ, осуществляемых в соответствии планам;

г) системность организационная, означающая единство организации всех работ по ЗИ и управления ими.

Концептуальность подхода предполагает разработку единой концепции как полной совокупности научно обоснованных взглядов, положений и решений, необходимых и

достаточных для оптимальной организации и обеспечения надёжности защиты информации, а также целенаправленной организации всех работ по ЗИ.

Системный подход к построению любой системы включает в себя: прежде всего, изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, её свойств, принципов работы и возможность увеличения её эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца.

Системный подход – это принцип рассмотрения проекта, при котором анализируется система в целом, а не её отдельные части. Его задачей является оптимизация всей системы в совокупности, а не улучшение эффективности отдельных частей. Это объясняется тем, что, как показывает практика, улучшение одних параметров часто приводит к ухудшению других, поэтому необходимо стараться обеспечить баланс противоречий требований и характеристик.

1.2. Сущность комплексной системы защиты информации

Объектами профессиональной деятельности специалиста по защите информации являются методы, средства и мероприятия по обеспечению комплексной системы защиты информации (КСЗИ) на предприятии. А функциями КСЗИ будут функции защиты, то есть совокупность однородных функциональных отношений и мероприятий, регулярно осуществляемых на предприятии с целью создания, поддержания и обеспечения условий, необходимых для защиты информации.

Современное предприятие представляет собой сложную систему, в рамках которой осуществляется защита информации.

Основные особенности такого сложного современного предприятия таковы:

- Сложная организационная структура;
- Многоаспектность функционирования;
- Высокая техническая оснащённость;
- Широкие связи по кооперации;
- Непрерывно расширяющаяся доступность;
- Всё возрастающий удельный вес безбумажной технологии обработки информации.

Кроме того, нахождение информации по местам хранения и обработки, сюда же входят помещения, где разрабатываются программы, обострило ситуацию с ее защитой. Только один пример. Появились в огромных количествах персональные компьютеры и на их основе построены сети ЭВМ (локальные, глобальные, национальные, транснациональные), которые используют различные каналы связи, в том числе спутниковые.

Все это требует постоянного совершенствования, создания и разработки? совокупности методологических, организационных и технических элементов комплексной защиты, взаимообусловленных и взаимоувязанных. Также надо учитывать, что на современном предприятии одновременно присутствуют люди, техника, ЭВМ, т.е. интегрально, комплексная система защиты информации может быть представлена совокупностью трех групп систем:

1. Люди – это биосоциальные системы;

2. Техника – включает в себя технические системы и помещения, в которых они расположены;

3. ЭВМ, т.е. программное обеспечение, которое является интеллектуальным посредником между человеком и техникой (интеллектуальные системы).

Совокупность этих трех групп образует социотехническую систему.

Но максимально эффективной защита информации будет лишь в том случае, когда будут созданы механизмы защиты, и в процессе функционирования комплексной системы будет осуществляться непрерывное управление этими механизмами. Чтобы это было, в КСЗИ должно быть предусмотрено два вида функций защиты, которые являются основополагающими:

I. функция, основной целью которой является создание механизмов защиты, сводящая до минимума возможность воздействия дестабилизирующих факторов на защищаемую информацию;

II. функция, осуществляемая с целью непрерывного и оптимального управления механизмами комплексной защиты.

1. Создание и поддержание таких механизмов защиты, в которых появление дестабилизирующих факторов (ДФ), способных оказать отрицательное воздействие на защищаемую информацию, маловероятно;

2. Предупреждение проявлений дестабилизирующих факторов в случае возникновения благоприятных для них условий;

3. Своевременное обнаружение воздействия дестабилизирующих факторов на информацию, локализация этих факторов и быстрая их ликвидация.

4. Вторая функция, т.е. функция непрерывного и оптимального управления механизмами комплексной защиты.

Здесь управление определяется как элемент, функция организованных систем различной природы (люди, техника, ЭВМ и прочее), обеспечивающая сохранение определенной структуры, поддержание режимов деятельности, реализации их программ и целей.

Но главным направлением поиска путей создания комплексных систем защиты информации на предприятии является повышение системности подхода к самой проблеме организации и эксплуатации КСЗИ.

1.3. Назначение комплексной системы защиты информации

Главным условием создания комплексной системы является ее надежность. Но надежность может быть обеспечена лишь в том случае, если защита является комплексной и системной. Исходя из сказанного, можно дать такое определение:

Система защиты информации (СЗИ) это организованная совокупность органов и объектов (компонентов) защиты информации, использование методов и средств защиты, а также осуществление защитных мероприятий.

Но органы защиты информации с одной стороны являются составной частью системы, с другой стороны - они сами организуют систему, осуществляя защитные мероприятия.

Поскольку система определяется как совокупность взаимосвязанных элементов, то **назначение системы защиты информации** состоит в том, чтобы объединить все составляющие элементы защиты в единое целое, в котором каждый компонент, выполняя свою прямую функцию, одновременно обеспечивает выполнение функций другими компонентами и связан с ними логически и технологически.

При отсутствии отдельных компонентов системы или их несогласованности между собой неизбежны ошибки в технологии защиты информации.

Следовательно, защита должна быть системной, и это является основным условием защиты информации.

Для того чтобы обеспечить надежность защиты информации нужна не только системность защиты, но и ее комплексность.

Комплексность – это один из основополагающих принципов защиты информации.

Комплекс вообще – это совокупность предметов и явлений, составляющих одно целое.

Комплексность имеет три назначения:

Первое назначение состоит в объединении в одно целое локальных СЗИ, при этом они должны функционировать в единой «связке». В качестве локальных СЗИ могут быть рассмотрены, например, виды защиты информации: правовая, организационная, инженерно-техническая.

Второе назначение комплексности обусловлено назначением самой системы. Система должна объединить логически и технологически все составляющие защиты. Но она не рассматривает полноту этих составляющих, не учитывает всех факторов, которые оказывают или могут оказывать влияние на качество защиты.

Например, система включает в себя объекты защиты, а все ли они включены или нет – это уже вне пределов системы. Другой пример. Система предусматривает проведение защитных мероприятий. Но и здесь не рассмотрены вопросы полноты этих мероприятий, учета всех факторов, определяющих состав таких мероприятий. Между тем факторы, влияющие на защиту информации, корректируют не только состав защитных мероприятий, но и объекты, и методы, и средства защиты информации.

Поэтому качество защиты информации, ее надежность зависят не только от видов, составляющих системы, но и от их полноты, которая обеспечивается при учете всех факторов и обстоятельств, влияющих на защиту. Именно полнота всех составляющих системы защиты, базирующаяся на анализе этих факторов и обстоятельств, является вторым назначением комплексности.

При этом должны учитываться все параметры уязвимости информации, потенциально возможные угрозы ее безопасности, охватываться все необходимые объекты защиты, использоваться все возможные виды, методы и средства защиты и необходимые для защиты кадровые ресурсы, осуществляться все вытекающие из целей и задач защитные мероприятия.

Третье назначение комплексности состоит в том, что система должна обеспечивать безопасность всей совокупной информации, подлежащей защите, и при любых обстоятельствах. Это означает, что должны защищаться все носители информации во всех компонентах ее сбора, хранения, передачи и использования, в любое время и при всех режимах функционирования системы обработки информации.

В то же время комплексность не исключает, а наоборот, предполагает дифференцированный подход к защите информации. Здесь дифференцированность зависит от состава ее носителей, видов тайны, к которым отнесена информация, степени ее конфиденциальности, средств хранения и обработки, форм и условий проявления ее уязвимости, каналов и методов несанкционированного доступа к информации.

Таким образом, коротко назначение комплексности защиты информации состоит:

- в объединении локальных систем защиты;
- в обеспечении полноты всех составляющих системы защиты;
- в обеспечении всеохватности защиты информации.

Исходя из этого, можно сформулировать следующее определение КСЗИ:

«Комплексная система защиты информации – это система, полно и всесторонне охватывающая все предметы, процессы и факторы, которые обеспечивают безопасность всей защищаемой информации».

Следовательно, из вышесказанного следует, что только комплексная система может гарантировать достижение максимальной эффективности защиты информации, поскольку системность обеспечивает необходимые составляющие защиты и устанавливает между ними логическую и технологическую связь, а комплексность, требует полноты этих составляющих, всеохватности защиты, обеспечивает ее надежность.

1.4. Принципы построения комплексной системы защиты информации

В процессе развития научных и практических работ по защите информации наряду с конкретными разработками конкретных вопросов защиты формировались и развивались и общеметодологические принципы (общие положения) построения и функционирования КСЗИ. Соблюдение требований выполнения таких принципов в общем случае способствует повышению эффективности защиты информации на предприятии.

Нижеперечисленные принципы относятся к любому предприятию: государственному, коммерческому, смешанному и другим формам собственности, а также большим, средним, малым. Среди принципов выделяют:

1. **принцип законности**. Здесь меры обеспечения функционирования предприятия разрабатываются на основе и в рамках действующих правовых актов. Правовые акты предприятия не должны противоречить государственным законам и подзаконным актам;

2. **принцип превентивности**, т.е. упреждения. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз. На основе анализа этих угроз вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз, т.е. разрабатываются упреждающие мероприятия;

3. **принцип полноты состава защищаемой информации**. Он заключается в том, что защите подлежит не только информация, содержащая государственную, коммерческую или служебную тайну, но даже часть служебной информации, утрата которой может нанести ущерб ее собственнику;

4. **принцип обоснованности защиты информации**. Выполнение этого принципа заключается в установлении целесообразности засекречивания и защиты той или другой информации с точки зрения экономических и иных последствий такой защиты. Это позволяет расходовать средства на защиту только той информации, утрата или утечка которой может нанести действительный ущерб ее владельцу;

5. **принцип персональной ответственности за защиту информации** заключается в том, что каждый сотрудник предприятия персонально отвечает за сохранность и неразглашение вверенной ему защищаемой информации, а за утрату или распространение такой информации несет уголовную, административную или иную ответственность;

6. **принцип непрерывности**, т.е. защита информации происходит на регулярной основе (постоянно);

7. **принцип гибкости**, т.е. это возможность варьирования и замены элементов системы без нарушения структуры и функционирования;

8. **принцип концептуального единства**. В комплексных системах защиты архитектура, технология, организация и обеспечение функционирования, как в целом, так и в отдельных ее компонентах должны рассматриваться в соответствии с общей концепцией защиты информации и теми требованиями, которые предъявляются для данной системы;

9. **принцип регламентации предоставляемых прав**, т.е. каждый сотрудник предприятия имеет доступ только к определенной информации, которая ему действительно необходима для выполнения своих функций в процессе работы, причем предоставленные права должны быть заранее определены и утверждены в установленном порядке, например, в договоре при приеме на работу;

10. **принцип активности**. Здесь меры противодействия угрозам осуществляются на основе взаимодействия и скоординированности усилий всех подразделений и служб предприятия, отдельных лиц, а также установления необходимых контактов с внешними организациями, способными оказать комплексной защите информации необходимое содействие в обеспечении безопасности предприятия.

11. **принцип плановой основы деятельности предприятия**. Здесь деятельность по обеспечению защиты информации должна строиться на основе комплексной программы обеспечения защиты информации на предприятии, разрабатываются подпрограммы обеспечения этой защиты по основным его видам (экономической, техногенной, научно-технической, экологической, технологической, информационной, психологической, физической, пожарной и другим видам), а также разрабатываются для их исполнения планы работы подразделений предприятия и отдельных сотрудников;

12. **принцип системности**. Этот принцип предполагает учет всех факторов, влияющих на организацию КСЗИ предприятия. При этом должны быть охвачены все этапы и режимы функционирования, задействованы все силы и средства.

Среди рассмотренных принципов едва ли можно выделить более или менее важные. А при построении КСЗИ важно использовать их в совокупности.

1.5. Цели системного подхода к защите информации

Для каждой системы должна быть сформулирована цель, к которой эта система стремится. Чем точнее и конкретнее указано назначение или перечислены функции системы, тем быстрее и правильнее можно выбрать лучший вариант ее построения. Например, цель, сформулированная в самом общем виде как обеспечение безопасности предприятия, заставит его рассматривать варианты создания глобальной системы защиты.

Если же цель уточнить, определив ее, например, как обеспечение безопасности информации, передаваемой по каналам связи внутри здания, то круг возможных технических решений существенного сузится. Следует иметь в виду, что, как правило, глобальная цель достигается через достижение множества менее общих локальных целей (подцелей). Построение такого «дерева целей» значительно облегчает, ускоряет и удешевляет процесс создания системы защиты информации.

Как правило, всегда рассматривается несколько вариантов построения системы, обеспечивающей заданные цели по защите информации. Чтобы оценить, какой из вариантов построения системы лучше, необходимо:

1. определить качество реализации заданных функций, ведущих к цели;

2. учитывать затраты ресурсов, необходимых для выполнения функционального назначения системы (ресурсы это не только деньги, техника, но и люди, и чем они подготовленные, тем меньше затрачивается ресурсов. Например, инженер после института и сотрудник после школы);

3. иметь ясный и однозначный физический смысл;

4. быть связанным с основными характеристиками системы и допускать количественную оценку на всех этапах создания системы.

Таким образом, учитывая многообразие потенциальных угроз информации на предприятии, сложность его структуры, а также участие человека в технологическом процессе обработки информации цели защиты информации могут быть достигнуты только путем создания СЗИ на основе комплексного подхода.

А это одновременно подразумевает, что защита информации – есть непрерывный процесс, который заключается в контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

Учитывая все вышесказанное можно сформулировать четыре пункта постулата системы защиты:

1) система защиты информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты, сочетающая в себе такие направления защиты, как правовая, организационная и инженерно-техническая;

2) никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты;

3) никакую систему защиты нельзя считать абсолютно надежной, т.к. всегда может найтись злоумышленник, который найдет лазейку для доступа к информации (действия злоумышленника всегда носят комплексный характер, т.к. он любыми средствами стремится добыть важную информацию);

4) система защиты должна быть адаптируемой (приспособляющейся) к изменяющимся условиям.

1.6. Стратегии защиты информации

Осознание необходимости разработки стратегических подходов к защите формировалось по мере осознания важности, многоаспектности и трудности защиты и невозможности эффективного ее осуществления простым использованием некоторого набора средств защиты.

Под стратегией понимается общая направленность в организации соответствующей деятельности, разрабатываемая с учётом объективных потребностей в данном виде деятельности, потенциально возможных условий ее осуществления и возможностей организации.

Стратегия включает:

1) план - заранее намеченные в деталях и контролируемые действия на определенный срок, преследующий определенные цели;

2) прием или тактический ход, представляющий собой кратковременную стратегию, имеющую ограниченные цели, могущую меняться, маневр с целью обыграть противника;

3) модель поведения – часто спонтанного, неосознанного, не имеющего конкретных целей;

4) позицию по отношению к другим;

5) перспективу.

Задача стратегии состоит в создании конкурентного преимущества, устранении негативного эффекта нестабильности окружающей среды, обеспечении доходности, уравновешении внешних требований и внутренних возможностей. Через ее призму рассматриваются все деловые ситуации, с которыми предприятие сталкивается в повседневной жизни.

Способность предприятия проводить самостоятельную стратегию во всех областях делает ее более гибкой, устойчивой, позволяет адаптироваться к требованиям времени и обстоятельствам.

Стратегия формируется под воздействием внутренней и внешней среды, постоянно развивается, ибо всегда возникает что-то новое, на что нужно реагировать.

Факторы, которые могут иметь для предприятия решающее значение в будущем, называются стратегическими. По мнению западных специалистов, они, влияя на стратегию любой организации, придают ей специфические свойства. К таким факторам относятся:

1) миссия, отражающая философию предприятия, его предназначения. При пересмотре миссии, происходящем в результате изменения общественных приоритетов;

2) конкурентные преимущества, которыми предприятие обладает в своей сфере деятельности по сравнению с соперниками или к которым стремится (считается, что эти преимущества оказывают на стратегию наибольшее влияние). Конкурентные преимущества любого типа обеспечивают более высокую эффективность использования ресурсов предприятия;

3) характер выпускаемой продукции, особенности ее сбыта, послепродажного обслуживания, рынки и их границы;

4) организационные факторы, среди которых выделяется внутренняя структура предприятия и его ожидаемые изменения, система управления, степень интеграции и дифференциации внутренних процессов;

5) располагаемые ресурсы (материальные, финансовые, информационные, кадровые пр.). Чем они больше, тем масштабнее могут быть инвестиции в будущие проекты. Сегодня для разработки и реализации стратегии огромное значение имеют, прежде всего, структурные, информационные и интеллектуальные ресурсы. Сравнивая значения параметров наличных и требующихся ресурсов, можно определить степень их соответствия стратегии;

6) потенциал развития предприятия, совершенствования деятельности, расширения масштабов, роста деловой активности, инноваций;

7) культура, философия, этические воззрения и компетентность управленцев, уровень их притязаний и предприимчивости, способность к лидерству, внутренний климат в коллективе.

На стратегический выбор влияют: риск, на который готово идти предприятие; опыт реализации действующих стратегий, позиции владельцев, наличие времени.

Рассмотрим особенности стратегических решений. По степени регламентированности они относятся к контурным (предоставляют широкую свободу исполнителям в тактическом отношении), а по степени обязательности следования главным установкам – директивным.

По функциональному назначению такие решения чаще всего бывают организованными или предписывающими способ осуществления в определенных ситуациях тех или иных

действий. С точки зрения предопределенности, это решения незапрограммированные. Они принимаются в новых, неординарных обстоятельствах, когда требуемые шаги трудно заранее точно расписать. С точки зрения важности, стратегические решения кардинальны: касаются основных проблем и направлений деятельности предприятия, определяют основные пути развития ее в целом, отдельных подразделений или видов деятельности на длительную перспективу (не менее 5-10 лет). Они вытекают, прежде всего, из внешних, а не из внутренних условий, должны учитывать тенденции развития ситуации и интересы множества субъектов. Практическая необратимость стратегических решений обусловливает необходимость их тщательной и всесторонней подготовки. Стратегическим решениям присуща комплектность. Стратегия обычно представляет собой не одно, а совокупность взаимосвязанных решений, объединенных общей целью, согласованных между собой по срокам выполнения и ресурсам. Такие решения определяют приоритеты и направления развития предприятия, его потенциала, рынков, способы реакции на непредвиденные события. Практика сформировала следующие требования к стратегическим решениям:

1) Реальность, предполагающая ее соответствие ситуации, целям, техническому и экономическому потенциалу предприятия, опыту и навыкам работников и менеджеров, культуре, существующей системе управления;

2) Логичность, понятность, приемлемость для большинства членов предприятия, внутренняя целостность, непротиворечивость отдельных элементов, поддержка ими друг друга, порождающая синергетический эффект;

3) Своевременность (реализация решения должна успеть приостановить отрицательное развитие ситуации или позволить упустить выгоду);

4) Совместимость со средой, обеспечивающая возможность взаимодействия с ней (стратегия находится под влиянием изменений в окружении предприятия и сама может формировать эти изменения);

5) Направленность на формирование конкурентных преимуществ;

6) Сохранение свободы тактического маневра;

7) Устранение причин, а не следствий существующей проблемы;

8) Четкое распределение по уровням организации работы по подготовке и принятию решений, а также ответственности за них конкретных лиц;

9) Учет скрытых и явных, желательных и нежелательных последствий, которые могут возникнуть при реализации стратегии или отказе от нее для предприятия, его партнеров; от существующего законодательства, этической стороны дела, допустимого уровня риска и пр.

Разработка научно обоснованной системы стратегий предприятия как ключевого условия ее конкурентоспособности и долгосрочного успеха является одной из основных функций ее менеджеров, прежде всего высшего уровня. От них требуется:

– выделять, отслеживать и оценивать ключевые проблемы;

– адекватно и оперативно реагировать на изменения внутри и в окружении предприятия;

– выбирать оптимальные варианты действий с учетом интересов основных субъектов, причастных к ее деятельности;

– создавать благоприятный морально- психологический климат, поощрять предпринимательскую и творческую активность низовых руководителей и персонала.

Исходный момент формирования стратегии – постановка глобальных качественных целей и параметров деятельности, которые предприятие, должно достичь в будущем. В

результате увязки целей и ресурсов формируются альтернативные варианты развития, оценка которых позволяет выбрать лучшую стратегию. Единых рецептов выработки стратегий не существует. В одном случае целесообразно стратегическое планирование (программирование); в другом - ситуационный подход.

Исходя их большого разнообразия условий, при которых может возникнуть необходимость защиты информации, общая целевая установка на решение стратегических вопросов заключалась в разработке множества стратегий защиты, и выбор такого минимального их набора, который позволял бы рационально обеспечивать требуемую защиту в любых условиях.

В соответствии с наиболее реальными вариантами сочетаний значений рассмотренных факторов выделено **три стратегии защиты**:

1)оборонительная - защита от уже известных угроз, осуществляемая автономно, т.е. без оказания существенного влияния на информационно - управляющую систему;

2) наступательная - защита от всего множества потенциально возможных угроз, при осуществлении которой в архитектуре информационно – управляющей системы и технологии ее функционирования должны учитываться условия, продиктованные потребностями защиты;

3) упреждающая – создание информационной среды, в которой угрозы информации не имели бы условия для проявления.

1.7. Разработка политики безопасности предприятия

Прежде чем предлагать какие-либо решения по организации системы защиты информации, предстоит разработать политику безопасности. Политика безопасности - набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Политика безопасности реализуется при помощи организационных мер и программно- технических средств, определяющих архитектуру системы защиты, а также при помощи средств управления механизмами защиты. Для конкретной организации политика безопасности должна быть индивидуальной, зависимой от конкретной технологии обработки информации, используемых программных и технических средств, расположения предприятия и т.д.

Организационная политика безопасности описывает порядок представления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система защиты информации окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения организационной политики безопасности- это внесение в описание объекта структуры ценностей и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. Прежде всего необходимо составить детализированное описание общей цели построения системы безопасности объекта, выражаемое через совокупность факторов или критериев, уточняющих цель. Совокупность факторов служит базисом для определения требований к системе (выбор альтернатив). Факторы безопасности, в свою очередь, могут разделяться на правовые, технологические, технические и организационные.

Разработка политики безопасности предприятия, как формальной, так и неформальной, - безусловно, нетривиальная задача. Эксперт должен не только владеть соответствующими стандартами и хорошо разбираться в комплексных подходах к обеспечению защиты информации предприятия, но и, например, проявлять детективные способности при выявлении особенностей построения информационной системы и существующих мер по организации защиты информации. Аналогичная проблема возникает в дальнейшем при необходимости анализа соответствия рекомендаций политики безопасности реальному положению вещей: необходимо по некоторому критерию отобрать своего рода «контрольные точки» и сравнить их практическую реализацию с эталоном, задаваемым политикой безопасности.

В общем случае можно выделить следующие процессы, связанные с разработкой и реализацией политики безопасности.

1. Комплекс мероприятий, связанных с проведением анализа рисков. К этой группе можно отнести:

– учет материальных или информационных ценностей;

– моделирование угроз информации системы;

– собственно анализ рисков с использованием того или иного подхода - например, стоимостной анализ рисков.

2. Мероприятия по оценке соответствия мер по обеспечению защиты информации системы некоторому эталонному образцу: стандарту, профилю защиты и т.п.

3. Действия, связанные с разработкой разного рода документов, в частности отчетов, диаграмм, профилей защиты, заданной по безопасности.

4. Действия, вязанные со сбором, хранением и обработкой статистики по событиям безопасности для предприятия.

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название этого способа, как правило, определяет название политики безопасности.

Для изучения свойств способа управления доступом создается его формальное описание - математическая модель. При этом модель должна отражать состояние всей системы, ее переходы из одного состояния в другое, а также учитывать, какие состояния и переходы можно считать безопасными в смысле данного управления. Без этого говорить о каких–либо свойствах системы, и тем более гарантировать их, по меньшей мере, некорректно. Отметим лишь, что для разработки моделей применяется широкий спектр математических методов (моделирования, теории информации, графов и др.).

В настоящее время лучше всего изучены два вида политики безопасности: избирательная и полномочная, основанные, соответственно, на избирательном и полномочном способах управления доступом.

Кроме того, существует набор требований, усиливающих действие этих политик и предназначений для управления информационными потоками в системе. Следует отметить, что средства защиты, предназначенные для реализации какого – либо из названных способов управления доступом, только предоставляют возможности надежного управления доступом или информационными потоками.

Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:

– все субъекты и объекты системы должны быть идентифицированы;

– права доступа субъекта к объекту системы определяются на основании некоторого правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа, иногда ее называют матрицей контроля доступа. Такая модель получила название матричной. Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменения этих правил также является задачей матрицы доступа.

Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно избирательное управление доступом реализует принцип « что не разрешено, то запрещено», предполагающий явное разрешение доступа субъекта к объекту. Матрица доступа – наиболее простой подход к моделированию систем доступа.

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость и небольшие накладные расходы.

Основу полномочной политики безопасности составляет **полномочное управление доступом**, которое подразумевает, что

– все субъекты и объекты системы должны быть однозначно идентифицированы;

– каждому объекту системы присвоена метка критичности, определяющая ценность содержащей в нем информации;

– каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру, и, таким образом, в системе можно реализовать иерархически восходящий поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Основное назначение полномочной политики безопасности - регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии в нижние, а также блокирование возможного проникновения с нижних уровней в верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Выбор политики безопасности – это прерогатива руководителя системы защиты информации. Но какой бы она ни была, важно, чтобы внедренная системы защиты информации отвечала ряду требований, которые будут рассмотрены в следующим разделе.

1.8. Основные требования, предъявляемые к комплексной системе защиты информации

Поскольку комплексная система защиты информации предназначена обеспечивать безопасность всей защищаемой информации, к ней должны предъявляться следующие требования:

– она должна быть привязана к целям и задачам защиты информации на конкретном предприятии;

– она должна быть целостной : содержать все ее составляющие, иметь структурные связи между компонентами, обеспечивающие ее согласованное функционирование;

– она должна быть всеохватывающей, учитывающей все объекты и составляющие их компоненты защиты, все обстоятельства и факторы, влияющие на безопасность информации, и все виды, методы и средства защиты;

– она должна быть достаточной для решения поставленных задач и надежной во всех элементах защиты, т.е. базироваться на принципе гарантированного результата;

– она должна быть « вмонтированной» в технологические схемы сбора, хранения, обработки, передачи и использования информации;

– она должна быть компонентно, логически, технологически и экономически обоснованной;

– она должна быть реализуемой, обеспеченной всеми необходимыми ресурсами;

– она должна быть простой и удобной в эксплуатации и управлении, а также в использовании законными потребителями;

– она должна быть непрерывной;

– она должна быть достаточно гибкой, способной к целенаправленному приспособлению при изменении компонентов ее составных частей, технологии обработки информации, условий защиты.

Таким образом, обеспечение безопасности информации есть непрерывный процесс, который заключается в контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты:

– безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты;

– никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты;

– никакую систему защиты нельзя считать абсолютно надежной, т.к. всегда может найтись злоумышленник, который найдет лазейку для доступа к информации.

1.9 СТР-К

1.9.1 Общие положения

1. Настоящий документ устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации на территории Российской Федерации и является основным руководящим документом в этой области для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, предприятий, учреждений и организаций (далее - учреждения и предприятия) независимо от их организационно-правовой формы и формы собственности, должностных лиц и граждан Российской Федерации, взявшим на себя обязательства либо обязанными по статусу исполнять требования правовых документов Российской Федерации по защите информации.

2. Требования и рекомендации настоящего документа распространяются на защиту:

– конфиденциальной информации - информации с ограниченным доступом, за исключением сведений, отнесенных к государственной тайне и персональным данным, содержащейся в государственных (муниципальных) информационных ресурсах, накопленной за счет государственного (муниципального) бюджета и являющейся собственностью государства (к ней может быть отнесена информация, составляющая служебную тайну и другие виды тайн в соответствии с законодательством Российской Федерации, а также сведения конфиденциального характера в соответствии с "Перечнем сведений конфиденциального характера", утвержденного Указом Президента Российской Федерации от 06.03.97 №188), защита которой осуществляется в интересах государства (далее - служебная тайна);

– информации о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющей идентифицировать его личность (персональные данные) *(В соответствии с Федеральным законом "Об информации, информатизации и защите информации" режим защиты персональных данных должен быть определен федеральным законом. До его введения в действие для установления режима защиты такой информации следует руководствоваться настоящим документом., за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.)*

3. Для защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (например, информации, составляющей коммерческую, банковскую тайну и т.д.) (далее - коммерческая тайна), данный документ носит рекомендательный характер.

4. Документ разработан на основании федеральных законов "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", Указа Президента Российской Федерации от 06.03.97г. № 188 "Перечень сведений конфиденциального характера", "Доктрины информационной безопасности Российской Федерации", утвержденной Президентом Российской Федерации 09.09.2000г. № Пр.-1895, "Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти", утвержденного постановлением Правительства Российской Федерации от 03.11.94г. № 1233, других нормативных правовых актов по защите информации (приложение № 8), а также опыта

реализации мер защиты информации в министерствах и ведомствах, в учреждениях и на предприятиях.

5. Документ определяет следующие основные вопросы защиты информации:

– организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;

– состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;

– требования и рекомендации по защите речевой информации при осуществлении переговоров, в том числе с использованием технических средств;

– требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;

– порядок обеспечения защиты информации при эксплуатации объектов информатизации;

– особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;

– порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования.

Порядок разработки, производства, реализации и использования средств криптографической защиты информации определяется "Положением о порядке разработки, производства (изготовления), реализации, приобретения и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" (Положение ПКЗ-99), а также "Инструкцией по организации и обеспечению безопасности хранения, обработки и передачи по техническим каналам связи конфиденциальной информации в Российской Федерации с использованием сертифицированных ФАПСИ криптографических средств".

6. Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в установленном настоящим документом порядке в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации.

7. Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в АС.

Защищаемыми объектами информатизации являются:

– средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы,

системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации;

– технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);

– защищаемые помещения.

8. Защита информации должна осуществляться посредством выполнения комплекса мероприятий и применение (при необходимости) средств ЗИ по предотвращению утечки информации или воздействия на нее по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

9. При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

– акустическое излучение информативного речевого сигнала;

– электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы КЗ;

– виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

– несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

– воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;

– побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;

– наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

– радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;

– радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;

– радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

– прослушивание ведущихся телефонных и радиопереговоров;

– просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

– хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

10. Перехват информации или воздействие на нее с использованием технических средств могут вестись:

– из-за границы КЗ из близлежащих строений и транспортных средств;

– из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;

– при посещении учреждения (предприятия) посторонними лицами;

– за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

11. В качестве аппаратуры перехвата или воздействия на информацию и технические средства могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта защиты либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства перехвата информации "закладки", размещаемые внутри или вне защищаемых помещений.

12. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

– непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;

– случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;

– некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;

– просмотра информации с экранов дисплеев и других средств ее отображения.

13. Выявление и учет факторов воздействующих или могущих воздействовать на защищаемую информацию (угроз безопасности информации) в конкретных условиях, в соответствии с ГОСТ Р 51275-99, составляют основу для планирования и осуществления мероприятий, направленных на защиту информации на объекте информатизации.

Перечень необходимых мер защиты информации определяется по результатам обследования объекта информатизации с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности информации и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрытия ее содержания.

14. Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности информации реализуются без применения сложных технических средств перехвата информации:

– речевой информации, циркулирующей в защищаемых помещениях;

– информации, обрабатываемой средствами вычислительной техники, от несанкционированного доступа и несанкционированных действий;

– информации, выводимой на экраны видеомониторов;

– информации, передаваемой по каналам связи, выходящим за пределы КЗ.

15. Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России и/или ФАПСИ на право оказания услуг в области защиты информации.

16. Для защиты информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства обработки и передачи информации, технические и программные средства защиты информации.

При обработке документированной конфиденциальной информации на объектах информатизации в органах государственной власти Российской Федерации и органах государственной власти субъектов Российской Федерации, других государственных органах, предприятиях и учреждениях средства защиты информационных систем подлежат обязательной сертификации.

17. Объекты информатизации должны быть аттестованы на соответствие требованиям по защите информации *(Здесь и далее под аттестацией понимается комиссионная приемка объекта информатизации силами предприятия с обязательным участием специалиста по защите информации.)*

18. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителей учреждений и предприятий, эксплуатирующих объекты информатизации.

ТЕМА 2. МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Основные понятия теории защиты информации

Дадим определение и сформулируем основные понятия теории защиты информации. **Теория защиты информации** определяется как система основных идей, относящихся к защите информации, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся и развивающаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

В приведенном определении уже содержатся общие сведения о задачах теории защиты.

В более же развернутом виде **теория защиты должна:**

1) предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты;

2) полно и адекватно отображать структуру и содержание взаимосвязей с родственными и смежными областями знаний;

3) аккумулировать опыт предшествующих исследований, разработок и практического решения задач защиты информации;

4) ориентировать исследователей в направлении наиболее эффективного решения основных задач защиты и предоставлять необходимые для этого научно-методологические и инструментальные средства (какие конкретно методы, способы и средства используются для эффективной защиты информации);

5) формировать научно обоснованные перспективные направления развития теории и практики защиты информации.

Сформулированные назначения теории защиты предопределяют ее состав, общее содержание и свидетельствуют о ее многоаспектности.

Составляющими частями ее, очевидно, должны быть:

1) полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;

2) систематизированные результаты анализа развития теоретических исследований и разработок, а также результаты опыта практического решения задач защиты (метод экспериментальных оценок, метод мозгового штурма, метод психоинтеллектуальной генерации);

3) научно обоснованная постановка задач защиты информации в современных системах ее обработки, полно и адекватно учитывающая текущие и перспективные концепции построения систем и технологий обработки, потребности в защите информации и объективные предпосылки их удовлетворения;

4) общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;

5) методы, необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные прикладные методы решения;

6) методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства для решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;

7) научно обоснованные предложения по организации и обеспечению работ по защите информации;

8) научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

Приведенный перечень составных частей свидетельствует о большом объеме и многоаспектности теории защиты, что, естественно, порождает значительные трудности ее формирования. Эти трудности усугубляются еще тем, что по мере развития исследований, разработок и практической их реализации появляются новые направления исследований, формирующиеся на стыке с другими науками. Например, для оценки влияния на безопасность информации основного ее носителя, человека, надо владеть навыками психологического анализа личности. Отсюда следует, что защита информации представляется все более системной и комплексной и все более масштабной проблемой. Кроме того, существенным фактором является повышенное влияние на процессы защиты случайных трудно предсказуемых (слабоструктурированных) событий, особенно тех из них, которые связаны со злоумышленными действиями людей или возникновением чрезвычайных ситуаций.

Всем изложенным предопределяется настоятельная необходимость выбора и обоснования методологических принципов формирования самой теории защиты.

Общеметодологические принципы формирования теории, методы решения задач и методологический базис в совокупности составляют научно методологическую основу теории защиты информации.

Методологический базис – это методологические принципы формирования самой теории защиты.

2.2 Методология защиты информации как теоретический базис комплексной системы защиты информации

Главная цель создания СЗИ это достижение максимальной эффективности защиты за счет одновременного использования всех необходимых ресурсов, методов и средств, исключающих несанкционированный доступ к защищаемой информации и обеспечивающих физическую сохранность ее носителей.

Организация – это совокупность элементов (людей, органов, подразделений) объединенных для достижения какой-либо цели, решения какой-либо задачи на основе разделения труда, распределения обязанностей и иерархической структуры.

СЗИ относится к системам организационно-технологического (социотехнического) типа, т.к. общую организацию защиты и решение значительной части задач осуществляют люди (организационная составляющая), а защита информации осуществляется параллельно с технологическим процессами ее обработки (технологическая составляющая).

Серьезным побудительным мотивом к проведению перспективных исследований в области защиты информации послужили те постоянно нарастающие количественные и качественные изменения в сфере информатизации, которые имели место в последнее время и которые, безусловно, должны быть учтены в концепциях защиты информации.

Постановка задачи защиты информации на современном этапе приобретает целый ряд особенностей: **во-первых**, ставится вопрос о комплексной (в современной интерпретации)

защите информации; **во-вторых**, защита информации становится все более актуальной для массы объектов (больших и малых, государственной и негосударственной принадлежности), **в-третьих**, резко расширяется разнообразие подлежащей защите информации (государственная, промышленная, коммерческая, персональная и т.п.). Осуществление мероприятий по защите информации носит массовый характер, занимается этой проблемой большое количество специалистов различного профиля. Но успешное осуществление указанных мероприятий при такой их масштабности возможно только при наличии хорошего инструментария в виде методов и средств решения соответствующих задач. Разработка такого инструментария требует наличия развитых научно-методологических основ защиты информации.

Под научно-методологическими основами комплексной защиты информации (как решения любой другой проблемы) **понимается совокупность принципов, подходов и методов** (научно-технических направлений), необходимых и достаточных для анализа (изучения, исследования) проблемы комплексной защиты, построения оптимальных механизмов защиты и управления механизмами защиты в процессе их функционирования. Уже из приведенного определения следует, что основными компонентами научно-методологических основ являются принципы, подходы и методы. При этом под принципами понимается основное исходное положение какой-либо теории, учения, науки, мировоззрения; под подходом - совокупность приемов, способов изучения и разработки какой-либо проблемы; под методом - способ достижения какой-либо цели, решения конкретной задачи. Например, при реализации принципа разграничения доступа в качестве подхода можно выбрать моделирование, а в качестве метода реализации – построение матрицы доступа.

Общее **назначение методологического базиса заключается**:

1. В формировании обобщенного взгляда на организацию и управление КСЗИ, отражающего наиболее существенные аспекты проблемы;
2. В формировании полной системы принципов, следование которым обеспечивает наиболее полное решение основных задач;
3. В формировании совокупности методов, необходимых и достаточных для решения всей совокупности задач управления.

Предмет нашего исследования – рассмотрение различных аспектов обеспечения безопасности социотехнической системы, характерным примером которой является современный объект информатизации.

Поэтому состав научно-методологических основ можно определить следующим образом:

– т.к. речь идет об организации и построении КСЗИ, то общеметодологической основой будут выступать основные положения теории систем;

– т.к. речь идет об управлении, то в качестве научно-методической основы будут выступать общие законы кибернетики (как науки об управлении в системах любой природы);

– т.к. процессы управления связаны с решением большого количества разноплановых задач, то в основе должны быть принципы и методы моделирования больших систем и процессов их функционирования.

Состав научно-методологических основ комплексной системы защиты информации представлен на рис. 2.1.

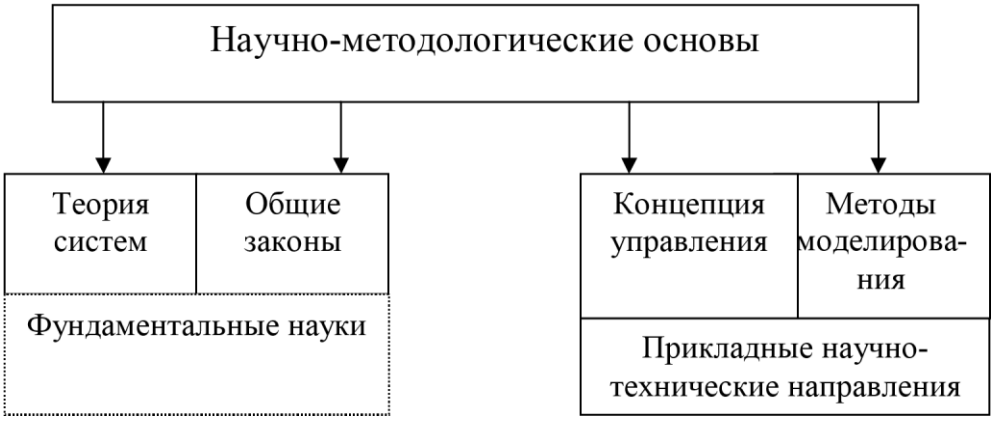

Рисунок 2.1. Состав научно-методологических основ КСЗИ

ТЕМА 3. ОПРЕДЕЛЕНИЕ СОСТАВА ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

3.1. Методика определения состава защищаемой информации

Определение состава защищаемой информации – это первый шаг на пути построения системы защиты. От того насколько он будет точно выполнен, зависит результат функционирования разрабатываемой системы. Общий подход состоит в том, что защите подлежит вся конфиденциальная информация, т.е. информация, составляющая государственную тайну (секретная информация), информация, составляющая коммерческую тайну и определяемая собственником(владельцем) часть открытой информации. При этом конфиденциальная информация должна защищаться от утечки и утраты, а открытая только от утраты.

Часто высказывается мнение, что любая открытая информация не может быть предметом защиты, а также не все согласны с включением информации, отнесенной к государственной тайне, в состав конфиденциальной.

Поэтому рассмотрим эти вопросы подробнее.

Защита открытой информации существовала всегда и производилась путем регистрации ее носителей, учета их движения и местонахождения, т.е. создавались безопасные условия хранения. Открытость информации не умаляет ее ценности, а ценная информация нуждается в защите от утраты. Эта защита не должна быть направлена на ограничение общедоступности информации, т.е. не может быть отказа в доступе к информации, но доступ должен осуществляться с соблюдением требований по ее сохранности в соответствии с требованиями обработки и использования (например, библиотека).

Теперь что касается разделения информации с ограниченным доступом на конфиденциальную и составляющую государственную тайну. Термин «конфиденциальный» переводится с латинского как «секретный», «доверительный». Но информацию, отнесенную к государственной тайне, принято называть секретной. Возможно, что разделение информации на секретную и конфиденциальную было вызвано стремлением вписаться в ранее принятые нормативные акты.

В «Конвенции о запрещении разработки, производства, накопления и применения химического оружия и его уничтожения», к которой присоединилась и Россия, речь идет об информации, составляющей государственную тайну, но она называется конфиденциальной

В Законе «О международном информационном обмене» информация, отнесенная к государственной тайне, поставлена в один ряд с «иной конфиденциальной информацией» (ст. 8).

Таким образом, к конфиденциальной информации должна быть отнесена вся информация с ограниченным доступом, составляющая любой вид тайны.

Но изложенный общий подход устанавливает лишь границы защищаемой информации, в пределах которых должен определяться ее состав. При решении вопроса об отнесении конкретной информации к защищаемой нужно руководствоваться определенными **критериями, т.е. признаками, при наличии которых информация может быть отнесена к защищаемой.**

Очевидно, что общей основой для отнесения информации к защищаемой является ценность информации, поскольку именно ценность информации диктует необходимость ее защиты. Поэтому критерии отнесения информации к защищаемой являются по существу критериями определения ее ценности.

Применительно к открытой информации такими критериями могут быть:

1) необходимость информации для правового обеспечения деятельности предприятия. Это относится к документированной информации, регламентирующей статус предприятия, права, обязанности и ответственность его работников;

2) необходимость информации для производственной деятельности (это касается информации, относящейся к научно-исследовательской, проектной, конструкторской, технологической, торговой и другим сферам производственной деятельности);

3) необходимость информации для управленческой деятельности, сюда относится информация, требующая для принятия управленческих решений, а также для организации производственной деятельности и обеспечения ее функционирования;

4) необходимость информации для финансовой деятельности;

5) необходимость информации для обеспечения функционирования социальной сферы;

6) необходимость информации как доказательного источника на случай возникновения конфликтных ситуаций;

7) важность информации как исторического источника, раскрывающего направления и особенности деятельности предприятия.

Эти критерии обусловливают необходимость защиты открытой информации от утраты. Они же вызывают потребность в защите от утраты и конфиденциальной информации. Однако основным, определяющим критерием отнесения информации к конфиденциальной и защиты ее от утечки является возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам. Этот критерий имеет как бы две составляющие: неизвестность информации третьим лицам и получение преимуществ в силу этой неизвестности. Данные составляющие взаимосвязаны и взаимообусловлены, поскольку, с одной стороны, неизвестность информации третьим лицам сама по себе ничего не значит, если не обеспечивает получение преимуществ, с другой – преимущества можно получить только за счет такой неизвестности информации.

Преимущества от использования информации, не известной третьим лицам, могут состоять в получении выгоды или предотвращении ущерба, иметь, в зависимости от областей и видов деятельности, политические, военные, экономические, моральные и другие характеристики, выражаться количественными и качественными показателями.

3.2. Классификация информации по видам тайны и степеням конфиденциальности

Понятие государственной тайны является одним из важнейших в системе защиты государственных секретов в любой стране. От ее правильного определения зависит и политика руководства страны в области защиты секретов.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

В соответствии с Указом Президента РФ от 30.11.1995 г. № 1203 к государственной тайне относят «сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности государства, распространение которых может нанести ущерб безопасности Российской Федерации, а также наименования федеральных органов исполнительной власти и других

организаций (далее именуются государственными органами), наделенных полномочиями по распоряжению этими сведениями».

Главный документ, в соответствии с которым осуществляется работа по защите государственной тайне, — это Закон о государственной тайне.

В соответствии с Указом Президента РФ от 06.03.1997 г. № 118 в перечень сведений конфиденциального характера включены:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2. Сведения, составляющие тайну следствия и судопроизводства;

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду; информация, составляющая коммерческую тайну – научно-техническая, технологическая, производственная, финансово экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Таким образом: сведения, составляющие коммерческую тайну, могут быть в любой сфере экономической деятельности; состав сведений, относимых к коммерческой тайне, должен определяться обладателем коммерческой тайны или, согласно договору, конфидентом коммерческой тайны; защита информации, составляющей коммерческую тайну, должна осуществляться ее обладателем.

3.3. Определение объектов защиты

Информация не существует сама по себе, она фиксируется в определенных материальных объектах, которые могут ее сохранять, накапливать, передавать с их же помощью осуществляется и использование информации. Эти материальные объекты выступают в роли носителей информации.

Носителями информации могут быть физическое лицо или другие материальные объекты, в том числе физическое поле, в которых информация находит свое отображение в

виде символов, образов, сигналов, технических решений и процессов, создавая тем самым возможность для ее накопления, хранения, передачи и использования.

Как видим, материальные объекты – это не только то, что можно увидеть и пощупать, но и физические поля (электромагнитное поле, оптическое, ультрафиолетовое, инфракрасное, рентгеновское и др.), которые являются формой материи.

Информация отображается не только символами, например, программы, но и образами в виде рисунков, графиков, карт, чертежей, схем и других знаковых моделей, а также техническими решениями в изделиях, технологическими процессами при изготовлении продукции.

Для записи секретной и несекретной информации используются одни и те же носители.

Как правило, носители секретной и конфиденциальной информации охраняются собственником этой информации.

Носители защищаемой информации можно классифицировать по следующим признакам: документы письменные и электронные; изделия или предметы; вещества и материалы; различные виды поля и излучения (электромагнитные поля, тепловые излучения, радиационные поля, акустические и другие виды излучения и поля).

Но особым носителем информации – является человек, мозг которого представляет исключительно сложную систему, хранящую и перерабатывающую информацию, поступающую из внешнего мира. Свойство мозга отражать и познавать внешний мир, накапливать в памяти колоссальные объемы информации ставят человека на особое место как носителя информации. Человек обладает возможностью генерировать новую информацию. И как носитель информации он может иметь позитивные и негативные черты.

Позитивные, т. е. положительные черты - без согласия человека, как носителя защищаемой информации из его памяти, как правило, никакая информация не может быть извлечена. Он может оценивать важность имеющейся у него информации. Может ранжировать и потребителей защищаемой информации, т.е. знать, кому и какую информацию он может доверить.

Негативные, т. е. отрицательные черты – он может заблуждаться в отношении истинности потребителя защищаемой информации или умышленно не сохранять доверенную ему информацию: измена или просто разболтать.

Раскроем смысл перечисленных выше видов носителей защищаемой информации.

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими его идентифицировать. По форме документы могут быть разные: бумага, кинофотопленка, магнитные ленты, диски, дискеты, флэшки и т. д.

На документе-носителе защищаемой информации указывается **гриф секретности**. Недостатком документа как носителя защищаемой информации является: документом может воспользоваться любой человек, в том числе и недобросовестный потребитель, документ может быть утрачен: похищен, или уничтожен, испорчен и т. д.

Следующим видом носителя информации является **выпускаемая продукция**, т. е. конкретные изделия, предметы. Здесь информация отображается в виде технических решений, например, в виде образцов вооружения, военной и др. техники; оборудования; приборов; комплектующих элементов и т.п. Эти изделия выполняют свое прямое назначение и являются носителем защищаемой информации.

Носителями информации являются также **технологические процессы**, отражающие в себе технологию производства продукции и применяемые при ее изготовлении компоненты (средства производства): оборудование, приборы, материалы, вещества, сырье, топливо,

термостойкие покрытия космических кораблей и другое. Информация отображается в виде технических процессов (первая составляющая) и технических решений (вторая составляющая).

К **веществам**, которые могут нести информацию, относятся отходы предприятий, а также вода, воздух (радиационный фон), пробы грунта (химический состав) и т.п.

Следующим видом носителей являются **магнитные носители**: аудиокассеты (аудио плёнки) для магнитофонов и диктофонов; видеокассеты (видеопленки) для видеомагнитофонов и некоторых видеокамер; жесткие (твердые) диски, дискеты, магнитные ленты для ЭВМ. В этих носителях информация фиксируется (наносится) с помощью магнитного накопления (записи сигналов), осуществляемого магнитным устройством, а отображается в виде символов. Воспроизведение (считывание) информации осуществляется также магнитным устройством посредством восстановления сигналов.

Магнитооптические и оптические носители (лазерные диски, компакт-диски). Запись данных в них выполняется лазерным лучом (в магнитооптическое и магнитное поле), информация отображается в виде символов, а ее считывание (воспроизведение) осуществляется посредством лазерного луча.

3.4. Хранилища носителей информации как объект защиты

Объектами хранения носителей защищаемой информации являются:

- хранилища письменных и видовых носителей информации;
- средства транспортировки письменных и видовых носителей информации;
- средства обработки и передачи информации;
- системы обеспечения производственной деятельности;
- технические средства защиты информации;
- здания, территория внутри и по периметру предприятия.

К хранилищам письменных и видовых носителей информации относятся:

а) помещения службы защиты информации, в которых постоянно хранятся и обрабатываются носители информации (документы, изделия). Эти помещения должны обязательно защищаться от несанкционированного физического проникновения в них;

б) помещения, в которых работает персонал с носителями информации. Сюда же относятся помещения для проведения закрытых мероприятий, производственные участки по выпуску продукции. Эти помещения во время нахождения в них носителей должны защищаться не только от несанкционированного физического проникновения к носителям, но и от визуального наблюдения. Кроме того, комнаты исполнителей, как и помещения для проведения закрытых заседаний должны защищаться от прослушивания информации.

Следующий объект защиты — это средства транспортировки письменных и видовых носителей информации, которые одновременно могут рассматриваться и как временное хранилище информации. Например, автомобиль, поезд, самолет. Они должны защищаться от физического проникновения к носителям или от их уничтожения.

Объектами защиты информации во время её обработки и передачи техническими средствами **должны быть:**

а) ЭВМ, которые должны защищаться от несанкционированного подключения, заражения вирусом, визуального наблюдения, вывода из строя и нарушения режима работы;

б) электрические и автоматические пишущие машинки и копировально-множительная техника (ксероксы). Они также должны защищаться от визуального наблюдения во время обработки информации;

в) средства видео-, звукозаписывающей и воспроизводящей техники - должны защищаться от прослушивания и визуального наблюдения;

г) средства радио и кабельной связи, радиовещания и телевидения - защищаются от прослушивания, вывода из строя, нарушения режима работы.

Технические средства защиты информации и контроля за ними. Защищаются от визуального наблюдения (злоумышленник не должен видеть аппаратуру) и от несанкционированного физического доступа к ним.

Здания предприятий, их территория внутри и по периметру предприятия.

Защищаются от несанкционированного физического проникновения в них. Здание является уязвимым, прежде всего из-за наличия дверей, окон, световых окон в потолке и других проёмов. Эти части здания в наибольшей степени нуждаются в установке сигнализации, предупреждающей о проникновении. Кроме этого, все окна и другие проёмы должны быть оборудованы металлическими запорами, в первую очередь решетками. Окна, желательно, делать непроницаемыми для обозрения. Периметр должен быть оснащен такой системой сигнализации, которая позволяла бы охране мгновенно реагировать на попытку его преодоления. Стены здания, которые частично или полностью являются периметром или линией защиты в случае наличия ограды, подлежат оснащению системной сигнализацией.

3.5. Методы оценки защищенности предприятия

В настоящее время существует ряд методик, позволяющих провести оценку защищенности объекта. Среди них можно отметить следующие пять:

1) анализ анкет-опросников (анкетный метод);

2) экспертная оценка отдельных составляющих системы защиты (экспертный метод);

3) проведение испытаний с использованием специального оборудования и аппаратуры (метод испытаний);

4) использование методик современной психологии и психофизиологии;

5) моделирование на объекте угрожающей ситуации.

При использовании анкетного метода привлекаются несколько руководителей предприятия. Заполненные анкеты обрабатываются на ЭВМ с использованием специальных программ. На основе полученных результатов готовятся развернутое заключение и конкретные рекомендации по совершенствованию системы безопасности как предприятия, так и его руководителей.

Второй метод (экспертный метод) предполагает проведения оценки качества системы безопасности путем анализа ее отдельных составляющих, а именно:

– правильность построения системы охраны;

– стойкость объекта против проникновения со взломом;

– возможность вывода из строя или нейтрализации охранной сигнализации и контрольных устройств;

– определение «мертвых зон» в системе наблюдения;

– правильность построения защиты от пожара и других стихийных бедствий.

Третий метод с использованием специальной аппаратуры является достаточно трудоемким и требует наличия сложной аппаратуры. Однако его следует применять, когда необходимо:

– определить максимальное расстояние, с которого возможен устойчивый перехват информации с экрана ПЭВМ, расположенной на указанном месте;

– проверить наличие подслушивающих устройств в конкретных помещениях после проведения в них ремонтно-строительных работ;

– определить, возможен ли съем речевой информации с оконных стекол конкретного кабинета из точек, расположенных вне здания на расстоянии прямой видимости;

– проверить подозрения, не заложены ли средства негласного наблюдения и передачи видеоинформации из здания в какой-нибудь пункт, расположенный поблизости.

Однако при проведении таких работ необходимо соблюдать требования Указа Президента РФ № 21 от 9 января 1996 г. и постановления Правительства РФ № 770 от 1 июля 1996 г., определяющего, кто и как может выполнять подобную работу.

Четвертый метод касается проверки обслуживающего персонала на его лояльность и способность выполнять возложенные функции. Здесь используются методики психологии и психофизиологии. Они оказываются эффективными в тех случаях, когда:

– необходимо дать оценку надежности и лояльности персонала;

– определить степень правдивости показаний при расследовании происшествий;

– проверить сотрудника при приеме его на работу;

– определить способность должностного лица выполнять предписанные ему функции в различных ситуациях.

В настоящее время такие методы разработаны на достаточно хорошем уровне.

В качестве примера можно привести систему: аппаратно-программный комплекс компьютерного психосемантического анализа. Время тестирования – 15 минут. Суть тестирования состоит в маскированном предъявлении тестовых стимулов (слов), записи времен реакций в ответ на предъявление стимулов и математической обработке результатов с выдачей конечного протокола. Система реализована на базе ПК.

Пятый метод моделирования является весьма эффективным и позволяет выявить слабые места в системе защиты. Для его проведения необходимо разработать модель операции, условно угрожающей жизнедеятельности объекта (вооруженное нападение, проникновение со взломом, тайное проникновение с нейтрализацией средств защиты, внедрение на объекты «закладок» и др.).

3.6 СТР-К 2.7

Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в АС.

Защищаемыми объектами информатизации являются:

– средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема,

передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации;

– технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);

– защищаемые помещения.

ТЕМА 4. ИСТОЧНИКИ, СПОСОБЫ И РЕЗУЛЬТАТЫ ДЕСТАБИЛИЗИРУЮЩЕГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИЮ

4.1. Оценка угроз безопасности информации

Говорить о безопасности объекта (системы) можно, лишь подразумевая, что с помощью этого объекта или над этим объектом совершаются какие-то действия. В этом смысле, если объект бездействует, а именно не функционирует (не используется, не развивается и т.д.), или, говоря другими словами, не взаимодействует с внешней средой, то и рассматривать его безопасность бессмысленно. Следовательно, объект необходимо рассматривать в динамике и во взаимодействии с внешней средой.

В некоторых случаях можно говорить о безопасности системы при ее сохраняемости. Но даже при сохраняемости системы взаимодействие с внешней средой неизбежно.

При функционировании объекта всегда преследуются определенные цели. Совокупность действий, совершаемых объектом, для достижения некоторой цели реализуется в виде результатов, имеющих значение для самого объекта.

Если цель операции или совокупность целенаправленных действий достигнута, то безопасность информации, циркулирующей в системе, обеспечена.

Проблема исследования критических ситуаций и факторов, которые могут представлять определенную опасность для информации, а также поиска и обоснования мер и средств по их исключению или снижению, характеризуется следующими особенностями:

а) большим количеством факторов опасных ситуаций и необходимостью выявления источников и причин их возникновения.

б) необходимостью выявления и изучения полного спектра возможных мер и средств парирования опасных факторов с целью обеспечения безопасности.

С другой стороны, существует угроза защищаемой информации. В литературе определение угрозы сформулировано следующим образом: «Угроза защищаемой информации это есть совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации». То есть угроза информации обусловлена вполне определенными факторами, совокупностью явлений и условий, которые могут сложиться в конкретной ситуации.

По отношению к информационной системе все множество угроз можно разбить на **две группы:** внешние и внутренние, каждая из которых, в свою очередь, делиться на умышленные и случайные угрозы, которые могут быть явными и скрытыми.

Выявления и анализ угроз защищаемой информации является ответственным этапом при построении системы защиты информации на предприятии. Большинство специалистов употребляют термин «угрозы безопасности информации». Но безопасность информации- это состояние защищенности информации от воздействий, нарушающих ее статус. Следовательно, безопасность информации означает, что информация находится в таком защищенном виде, который способен противостоять любым дестабилизирующим воздействиям.

Любая угроза не сводится к чему-то однозначному, она состоит из определенных взаимосвязанных компонентов, каждый из которых сам по себе не создает угрозу, но является неотъемлемой частью ее, угроза же возникает лишь при совокупном их взаимодействии.

Угрозы защищаемой информации связаны с ее уязвимостью, т.е. неспособностью информации самостоятельно противостоять дестабилизирующим воздействиям, нарушающим ее статус. Реализация угроз приводит, в зависимости от их характера, к одной или нескольким формам проявления уязвимости информации. При этом каждой из форм проявления уязвимости(или нескольким из них) присущи определенные, имеющие отношение только к ним угрозы с набором соответствующих компонентов, т.е. структура конкретной угрозы предопределяет конкретную форму. Однако должна существовать и общая, как бы типовая структура угроз, составляющая основу конкретных угроз. Эта общая структура должна базироваться на определенных признаках, характерных для угрозы защищаемой информации.

4.2. Явления, факторы и условия дестабилизирующего воздействия на защищаемую информацию

Прежде всего, угроза должна иметь какие-то сущностные проявления. А любое проявление, обнаружение чего-то принято называть явлением. Следовательно, одним из признаков и вместе с тем одной из составляющих угрозы должны быть явления.

Но в основе любого явления лежат соответствующие причины, которые являются его движущей силой и которые, в свою очередь, обусловлены определенными обстоятельствами или предпосылками. Эти причины и обстоятельства (предпосылки) относятся к факторам, создающим возможность дестабилизирующего воздействия на информацию. Таким образом, факторы являются еще одним признаком и второй составляющей угрозы.

Вместе с тем факторы могут стать побудительной силой для явления, а последние могут «сработать» лишь при наличии определенных условий (обстановки) для этого. Наличие условий для дестабилизирующего воздействия на информацию является третьим признаком и еще одной составляющей угрозы.

Определяющим признаком угрозы является ее направленность, результат, к которому может привести дестабилизирующее воздействие на информацию. Этим результатом во всех случаях реализации угрозы является нарушение статуса информации.

Таким образом, угроза защищаемой информации – это совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

К явлениям, т. е. сущностным проявлениям угрозы, относятся:

а) Источники дестабилизирующего воздействия на информацию (от кого или от чего исходит дестабилизирующее воздействие)

б) Виды дестабилизирующего воздействия на информацию (каким образом, по каким направлениям происходит дестабилизирующее воздействие)

в) Способы дестабилизирующего воздействия на информацию (какими приемами, действиями осуществляется (реализуется) виды дестабилизирующего воздействия).

К факторам, помимо причин и обстоятельств, следует отнести наличие каналов и методов несанкционированного доступа к конфиденциальной информации для воздействия на информацию со стороны лиц, не имеющих к ней разрешенного доступа.

Что касается состава структурных частей угрозы, то необходимо подчеркнуть: стержневыми, исходными являются источники дестабилизирующего воздействия на информацию, от их состава зависят и виды, и способы, и конечный результат воздействия. Хотя состав других структурных частей угрозы также играет существенную роль, он в отличие от источников не носит определяющего характера и прямо зависит от источников.

Вместе с тем еще раз следует отметить, что источники сами по себе не являются угрозой, если от них не происходит тех или других воздействий.

Рассмотрим **источники дестабилизирующего воздействия на информацию**. К ним относятся:

1) Люди.
2) Технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи.
3) Системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации.
4) Технологические процессы отдельных категорий промышленных объектов.
5) Природные явления.

4.3. Источники дестабилизирующего воздействия на информацию

Самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются **люди**, которые делятся на следующие **категории:**

а) сотрудники данного предприятия;

б) лица, не работающие на предприятии, но имеющие доступ к защищаемой информации предприятия в силу служебного положения (из вышестоящих, смежных, в том числе посреднических, предприятий, контролирующих органов государственной и муниципальной власти и др.);

в) сотрудники государственных органов разведки других стран и разведывательных служб конкурирующих отечественных и зарубежных предприятий;

г) лица из криминальных структур, хакеры.

В части соотношения с видами и способами дестабилизирующего воздействия на информацию эти категории людей подразделяются на две группы: имеющие доступ к носителям данной защищаемой информации, техническим средствам ее отображения, хранения, обработки, воспроизведения, передачи и системам обеспечения их функционирования и не имеющие такового.

Отличия в конкретно применяемых видах и методах дестабилизирующего воздействия на информацию между названными группами людей (при однотипности видов и методов) обусловлены преследуемыми целями. Основной целью второй группы людей является несанкционированное получение(хищение) информации, являющееся конфиденциальной. Уничтожение, искажение, блокирование информации стоят на втором плане, а нередко и не являются целью. Дестабилизирующее воздействие со стороны этой группы людей в подавляющем большинстве случаев является преднамеренным (умышленным, сознательным). К тому же, для того чтобы осуществить дестабилизирующее воздействие на конфиденциальную информацию, людям, входящим в эту группу, нужно иметь канал несанкционированного доступа к ней.

Для первой группы людей несанкционированное получение конфиденциальной информации вообще не является целью в силу наличия у них доступа к такой информации. Целями дестабилизирующего воздействия со стороны этой группы являются разглашение, несанкционированное уничтожение, блокирование, искажение информации (перечислены в последовательности, соответствующей степени интенсивности воздействия, от большей к меньшей). Хищение информации также присуще для данной группы, но оно является не

целью, а средством для осуществления уничтожения или разглашения информации. Предметом воздействия со стороны этой группы является не только конфиденциальная информация (хотя она в первую очередь), но и защищаемая часть открытой информации. Воздействие со стороны людей, включенных в данную группу, может быть как преднамеренным, так и непреднамеренным (ошибочным, случайным). Т.е. по объектам доступа эта группа неоднородна по своему составу. В нее входят люди, имеющие доступ и к носителям защищаемой информации, и к средствам отображения, хранения, обработки, воспроизведения и передачи информации (ко всем или части из них), и к системам обеспечения функционирования этих средств; люди, имеющие доступ только к информации и (иногда или) к средствам ее обработки (всем либо отдельным); люди, допущенные только к системам обеспечения функционирования средств.

Самым многообразным этот источник является потому, что, во-первых, он самый массовый, во-вторых, воздействие со стороны носит не эпизодический, постоянный характер, в-третьих, как уже отмечалось, его воздействие может быть не только непреднамеренным, как со стороны других источников, но и преднамеренным, и, в четвертых, оказываемое им воздействие может привести ко всем формам проявления уязвимости информации (со стороны остальных источников- к отдельным формам).

Технические средства отображения, хранения, обработки, воспроизведения, передачи информации и средства связи являются **вторым по значению источником дестабилизирующего воздействия** на защищаемою информацию в силу их многообразия, а так же существующих с их стороны способов дестабилизирующего воздействия. К этому источнику относятся:

а) электронно-вычислительная техника;

б) электрические и автоматические пишущие машинки и копировально-множительная техника;

в) средства видео- и звукозаписывающей и воспроизводящей техники;

г) средства телефонной, телеграфной, факсимильной, громкоговорящей передачи информации;

д) средства радиовещания и телевидения;

е) средства радио и кабельной связи.

Третий источник дестабилизирующего воздействия на информацию включает системы электроснабжения водоснабжения, теплоснабжения, кондиционирования.

К четвертому источнику относятся технологические процессы объектов ядерной энергетики, химической промышленности, радиоэлектроники, а также объектов по изготовлению некоторых видов вооружения и военной техники, которые изменяют естественную структуру окружающей объект среды.

Пятый источник — это природные явления. Составляющими их являются стихийные бедствия и атмосферные явления.

4.4. Виды и способы дестабилизирующего воздействия на информацию со стороны людей

В зависимости от источника и вида воздействия оно может быть непосредственным на защищаемую информацию либо опосредственным, через другой источник воздействия.

Со стороны людей возможны следующие виды воздействия:

1. непосредственное воздействие на носители защищаемой информации;

2. несанкционированное распространение конфиденциальной информации;

3. вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи;

4. нарушение режима работы перечисленных средств и технологии обработки информации;

5. вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Способами непосредственного воздействия на носители защищаемой информации могут быть:

а) физическое разрушение носителя (поломка, разрушение и др.);

б) создание аварийных ситуаций для носителей (поджог, искусственное затопление, взрыв и т.д.);

в) удаление информации с носителей;

г) создание искусственных магнитных полей для размагничивания носителей;

д) внесение фальсифицированной информации в носители.

Этот вид дестабилизирующего воздействия приводит к реализации трех форм проявления уязвимости информации: уничтожению, искажению и блокированию.

К непосредственному воздействию на носители защищаемой информации можно с оговоркой отнести и непреднамеренное оставление их в неохраняемой зоне, чаще всего в общественном транспорте, магазине, на рынке, что приводит к потери носителей.

Несанкционированное распространение конфиденциальной информации может осуществляться путем:

а) словесной передачи (сообщения) информации;

б) передачи копий (снимков) носителей информации;

в) показа носителей информации;

г) ввода информации в вычислительные сети;

д) опубликования информации в открытых публичных выступлениях, в том числе по радио, телевидению.

К несанкционированному распространению может привести и потеря носителей информации. Этот вид дестабилизирующего воздействия приводит к разглашению конфиденциальной информации.

К способам вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи можно отнести:

а) неправильный монтаж средств;

б) поломку (разрушение) средств, в том числе разрыв (повреждение) кабельных линий связи;

в) создание аварийных ситуаций для средств (поджог, искусственное затопление, взрыв и др.);

г) отключение средств от сетей питания;

д) вывод из строя или нарушение режима работы систем обеспечения функционирования средств;

е) вмонтирование в ЭВМ разрушающих радио- и программных закладок.

Этот вид дестабилизирующего воздействия приводит к реализации **трех форм** проявления уязвимости информации: уничтожению, искажению и блокированию.

Способами нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передачи информации, средств связи и технологии обработки информации могут быть:

а) повреждение отдельных элементов средств;

б) нарушение правил эксплуатации средств;

в) внесение изменений в порядок обработки информации;

г) заражение программ обработки информации;

д) выдача неправильных программных команд;

е) превышение расчетного числа запросов;

ж) создание помех в радиоэфире с помощью дополнительного звукового или шумового фона, изменения (наложения) частот передачи информации;

з) передача ложных сигналов;

и) подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;

к) нарушение (изменение) режима работы систем обеспечения функционирования средств.

Данный вид дестабилизирующего воздействия также приводит к уничтожению, искажению и блокированию информации.

К способам вывода из строя и нарушения режима работы систем обеспечения, функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации следует отнести:

а) неправильный монтаж систем;

б) поломку (разрушение) систем или их элементов;

в) создание аварийных ситуаций для систем (поджог, искусственное затопление, взрыв и т.д.);

г) отключение систем от источников питания;

д) нарушение правил эксплуатации систем.

Этот вид дестабилизирующего воздействия приводит к тем же результатам, что и два предыдущих вида.

4.5. Виды и способы дестабилизирующего воздействия на информацию со стороны технических средств, технологических процессов и природных явлений

К видам дестабилизирующего воздействия на защищаемую информацию со стороны второго источника воздействия – технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи относятся:

- вывод средств из строя;
- сбои в работе средств;
- создание электромагнитных излучений.

Вывод средств из строя, приводящий к невозможности выполнения операций, может происходить путем:

а) технической поломки, аварии (без вмешательства людей);

б) возгорания, затопления (без вмешательства людей);

в) выхода из строя систем обеспечения функционирования средств;

г) воздействия природных явлений;

д) воздействия измененной структуры окружающего магнитного поля;

е) заражения программ обработки информации вредоносными программами (путем размножения последних или с заражением дискет);

ж) разрушения или повреждения носителя информации, в том числе размагничивания магнитного слоя диска (ленты) из-за осыпания магнитного порошка.

Этот вид дестабилизирующего воздействия приводит к реализации трех форм проявления уязвимости информации: уничтожению, искажению, блокированию.

Сбои в работе средств, приводящие к неправильному выполнению операций (ошибкам), могут осуществляться посредством:

а) возникновения технических неисправностей элементов средств;

б) заражения программ обработки информации вредоносными программами (путем размножения последних или с зараженных дискет);

в) воздействия природных явлений;

г) воздействия окружающего магнитного поля;

д) частичного размагничивания магнитного слоя диска (ленты) из-за осыпания магнитного порошка;

е) нарушения режима функционирования средств.

Данный вид дестабилизирующего воздействия приводит к реализации **четырех форм проявления уязвимости информации**: уничтожению, искажению, блокированию, разглашению (пример последней - соединение с номеров телефона не того абонента, который набирался или слышимость разговора других лиц из-за неисправности в цепях коммуникации телефонной станции). Электромагнитные излучения, в том числе побочные, образующиеся в процессе эксплуатации средств, приводят к хищению информации.

Третий источник дестабилизирующего воздействия на информацию- системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации- включает два вида воздействия:

1. Выход систем из строя.

2. Сбои в работе систем.

Выход систем из строя может происходить путем:

а) поломки, аварии (без вмешательства людей);

б) возгорания, затопления (без вмешательства людей);

в) выхода из строя источников питания;

г) воздействия природных явлений.

Этот вид дестабилизирующего воздействия приводит к реализации **трех форм проявления уязвимости информации**: уничтожению, блокированию, искажению. Сбои в работе систем могут осуществляться посредством:

а) появления технических неисправностей элементов систем;

б) воздействия природных явлений;

в) нарушения режима работы источников питания.

Результатом дестабилизирующего воздействия также являются уничтожение, блокирование, искажение информации. Видом дестабилизирующего воздействия на информацию со стороны **технологических процессов** отдельных промышленных объектов является изменение структуры окружающей среды. Это воздействие осуществляется путем:

а) изменения естественного радиационного фона окружающей среды, происходящего при функционировании объектов ядерной энергетики;

б) изменения химического состава окружающей среды, происходящего при функционировании объектов химической промышленности;

в) изменения локальной структуры магнитного поля, происходящего вследствие деятельности объектов радиоэлектроники и по изготовлению некоторых видов вооружения и военной техники.

Этот вид дестабилизирующего воздействия в итоге приводит к хищению конфиденциальной информации. Пятый источник дестабилизирующего воздействия на информацию – **природные явления,** как уже отмечалось, включает стихийные бедствия и атмосферные явления (колебания).

К стихийным бедствиям и одновременно видам воздействия следует отнести: землетрясение, наводнение, извержение вулканов, ураган(смерч), шторм, оползни, лавины; к атмосферным явлениям (видам воздействия): грозу, дождь, снег, перепады температуры и влажность воздуха, магнитные бури.

Способами воздействия со стороны и стихийных бедствий, и атмосферных явлений могут быть разрушения (поломка), землетрясение, сожжение носителей информации, средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи, систем обеспечения функционирования этих средств, нарушение режима работы средств и систем, а так же технологии обработки информации, создание паразитных наводок (грозовые разряды).

Эти виды воздействия приводят к пяти проявлениям уязвимости информации: потере, уничтожению, искажению, блокированию и хищению.

При рассмотрении признаков и составляющих угрозы защищаемой информации было сказано, что в основе любого дестабилизирующего воздействия лежат определенные причины, побудительные мотивы, которые обуславливают появление того или другого вида и способа воздействия. Вместе с тем и причины имеют под собой основания- обстоятельства или предпосылки, которые вызывают данные причины, способствуют их появлению. Однако наличие источников, видов, способов, причин и обстоятельств (предпосылок) дестабилизирующего воздействия на информацию представляет потенциально существующую опасность, которая может быть реализована только при наличии определенных условий для этого.

4.6. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию со стороны людей

Поскольку виды и способы дестабилизирующего воздействия зависят от источников воздействия, то и причины, обстоятельства (предпосылки) и условия должны быть привязаны к источникам воздействия.

Применительно к людям причины, обстоятельства и условия в большинстве случаев увязаны еще и с характером воздействия− преднамеренным или непреднамеренным.

К причинам, вызывающим преднамеренное дестабилизирующее воздействие, следует отнести:

а) стремление получить материальную выгоду (подработать);

б) стремление нанести вред (отомстить) руководству или коллеге по работе, а иногда и государству;

в) стремление оказать бескорыстную услугу приятелю из конкурирующей фирмы;

г) стремление продвинуться по службе;

д) стремление обезопасить себя, родных и близких от угроз, шантажа, насилия;

е) стремление показать свою значимость.

Обстоятельствами (предпосылками), способствующими появлению этих причин, могут быть:

а) тяжелое материальное положение, финансовые затруднения;

б) корыстолюбие, алчность;

в) склонность к развлечениям, пьянству, наркотикам;

г) зависть, обида;

д) недовольство государственным строем, политическое или научное инакомыслие;

е) личные связи с представителями конкурента;

ж) недовольство служебным положением, карьеризм;

з) трусость, страх;

и) тщеславие, самомнение, завышенная самооценка, хвастовство.

К условиям, создающим возможность для дестабилизирующего воздействия на информацию, можно отнести:

а) недостаточность мер, принимаемых для защиты информации, в том числе из-за недостатка ресурсов;

б) недостаточное внимание и контроль со стороны администрации вопросам защиты информации;

в) принятие решений по производственным вопросам без учета требований по защите информации;

г) плохие отношения между сотрудниками и сотрудников с администрацией.

Причинами непреднамеренного дестабилизирующего воздействия на информацию со стороны людей могут быть:

а) неквалифицированное выполнение операций;

б) халатность, безответственность, недисциплинированность, недобросовестное отношение к выполняемой работе;

в) небрежность, неосторожность, неаккуратность;

г) физическое недомогание (болезни, переутомление, стресс, апатия).

К обстоятельствам (предпосылкам) появления этих причин можно отнести:

а) низкий уровень профессиональной подготовки;

б) излишнюю болтливость, привычку делиться опытом, давать советы;

в) незаинтересованность в работе (вид работы, ее временный характер, зарплата), отсутствие стимулов для ее совершенствования;

г) разочарованность в своих возможностях и способностях;

д) перезагруженность работой, срочность ее выполнения, нарушение режима работы;

е) плохое отношение со стороны администрации.

Условиями для реализации непреднамеренного дестабилизирующего воздействия на информацию могут быть:

а) отсутствие или низкое качество правил работы с защищаемой информацией;

б) незнание или нарушение правил работы с информацией исполнителями;

в) недостаточный контроль со стороны администрации за соблюдением режима конфиденциальности;

г) недостаточное внимание со стороны администрации условиям работы, профилактики заболеваний, повышению квалификации.

4.7. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию со стороны технических средств, технологических процессов и природных явлений

Причинами дестабилизирующего воздействия ни информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи могут быть:

а) недостаток или плохое качество средств;

б) низкое качество режима функционирования средств;

в) перезагруженность средств;

г) низкое качество технологии выполнения работ;

д) дестабилизирующее воздействие на средства со стороны других источников воздействия.

К обстоятельствам (предпосылкам), вызывающим эти причины, следует отнести:

а) недостаточность финансовых ресурсов, выделяемых на приобретение и эксплуатацию средств;

б) плохой выбор средств;

в) старение (износ) средств;

г) конструктивные недоработки или ошибки при монтаже средств;

д) ошибки при разработке технологии выполнения работ, в том числе программного обеспечения;

е) дефекты используемых материалов;

ж) чрезмерный объем обрабатываемой информации;

з) причины, лежащие в основе дестабилизирующего воздействия на средства со стороны других источников воздействия.

Условиями, обеспечивающими реализацию дестабилизирующего воздействия на информацию со стороны технических средств, могут являться:

а) недостаточное внимание к составу и качеству средств со стороны администрации, нередко из-за недопонимания их значения;

б) нерегулярный профилактический осмотр средств;

в) низкое качество обслуживания средств.

Причины, обстоятельства (предпосылки) и условия дестабилизирующего воздействия на информацию со стороны систем обеспечения функционирования средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи «вписываются» в причины и обстоятельства воздействия со стороны самих средств.

Причиной дестабилизирующего воздействия на информацию со стороны технологических процессов отдельных промышленных объектов является специфика технологии, обстоятельством - необходимость такой технологии, а условием - отсутствие возможностей противодействия изменению структуры окружающей среды.

В основе дестабилизирующего воздействия на информацию со стороны природных явлений заложены внутренние причины и обстоятельства, неподконтрольные людям, а следовательно, и не поддающиеся нейтрализации или устранению.

Взаимосвязь причин, условий, а также обстоятельств и источников дестабилизирующего воздействия на информацию представлена в табл. 4.1.

Таблица 4.1 – Виды и способы дестабилизирующего воздействия на защищаемую информацию

Виды воздействия	Способы дестабилизирующего воздействия	Результат воздействия на информацию
1. Со стороны людей		
Непосредственное воздействие на носители защищаемой информации	- физическое разрушение; создание аварийных ситуаций для носителей; - удаление информации с носителей; - создание искусственных магнитных полей для размагничивания носителей; - внесение фальсифицированной информации в носители.	Уничтожение, искажение, блокирование
Несанкционированное распространение конфиденциальной информации	- словесная передача (сообщение) информации; - передача копий(снимков) носителей информации; - показ носителей информации; - ввод информации в вычислительные сети; - опубликование информации в открытой печати; - использование информации в публичных выступлениях.	разглашение
Вывод из строя технических средств (ТС) при работе с информацией и средств связи	- неправильный монтаж ТС; - поломка (разрушение) ТС. В т.ч. разрыв (повреждение) кабельных линий связи; - создание аварийных ситуаций для ТС; - отключение ТС от сетей питания; - вывод из строя систем обеспечения функционирования ТС; - вмонтирование в ЭВМ разрушающих радио и программных закладок.	Уничтожение, искажение, блокирование
Нарушение режима работы ТС и технологии обработки информации	- повреждение отдельных элементов ТС; - нарушение правил эксплуатации ТС; - внесение изменений в порядок обработки информации; - заражение программ обработки информации вредоносными вирусами; - выдача неправильных программных команд;	Уничтожение, искажение, блокирование

	- превышение расчетного числа запросов; - создание помех в радиоэфире с помощью дополнительного звукового или шумового фона; - передача ложных сигналов; - подключение подавляющих фильтров в информационные цепи, цепи питания и заземления; - нарушение, изменение режима работы систем обеспечения функционирования ТС.	
Вывод из строя и нарушение режима работы систем обеспечения функционирования ТС	- неправильный монтаж систем; - поломка, разрушение систем или их элементов; - создание аварийных ситуаций для систем; - отключения систем от источников питания; - нарушение правил эксплуатации систем.	Уничтожение, искажение, блокирование
2. Со стороны технических средств при работе с информацией и средств связи		
Выход ТС из строя	- техническая поломка, авария (без вмешательства людей); - возгорание, затопление (без вмешательства людей); - выход из строя систем обеспечения функционирования ТС; - воздействие природных явлений; - воздействие измененной структуры окружающего магнитного поля; - заражение программ обработки носителя информации, в том числе размагничивание магнитного слоя диска(ленты) из-за осыпания магнитного порошка.	Уничтожение, искажение, блокирование
Создание электромагнитных излучений	- запись электромагнитных излучений.	Хищение
3. Со стороны систем обеспечения функционирования ТС при работе с информацией		
Выход систем из строя	- техническая поломка, авария (без вмешательства людей); - возгорание, затопление (без вмешательства людей); - выход из строя источников питания; - воздействие природных явлений.	Уничтожение, искажение, блокирование

Сбои в работе систем	- появление технических неисправностей элементов систем; - воздействие природных явлений; - нарушение режима работы источников питания.	Уничтожение, искажение, блокирование
4. Со стороны технологических процессов отдельных промышленных объектов		
Изменение структуры окружающей среды	- изменение естественного радиационного фона окружающей среды при функционировании объектов ядерной энергетики; изменение естественного химического состава окружающей среды при функционировании объектов химической промышленности; - изменения локальной структуры магнитного поля из-за деятельности объектов радиоэлектроники и изготовлению некоторых видов вооружения и военной техники.	Хищение
5. Со стороны природных явлений		
Землетрясение, наводнение, ураган(смерч), шторм, оползни, лавины, извержения вулканов	- разрушение (поломка), затопление, сожжение носителей информации, ТС работы с информацией, кабельных средств связи, систем обеспечения функционирования ТС; - нарушение режима работы ТС и систем обеспечения функционирования ТС; - нарушение технологии обработки.	Потеря, уничтожение, искажение, блокирование, хищение
Гроза,дождь,снег,перепады температуры и влажности воздуха. Магнитные бури		

4.8. СТР-К 3 организация работ по защите информации

1. Организация и проведение работ по технической защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами Гостехкомиссии России.

2. Организация работ по защите информации возлагается на руководителей учреждений и предприятий, руководителей подразделений, осуществляющих разработку проектов объектов информатизации и их эксплуатацию, а методическое руководство и

контроль за эффективностью предусмотренных мер защиты информации на руководителей подразделений по защите информации (служб безопасности) учреждения (предприятия).

3. Научно-техническое руководство и непосредственную организацию работ по созданию (модернизации) СЗИ объекта информатизации осуществляет его главный конструктор или другое должностное лицо, обеспечивающее научно-техническое руководство созданием объекта информатизации.

4. Разработка СЗИ может осуществляться как подразделением учреждения (предприятия), так и специализированным предприятием, имеющим лицензии Гостехкомиссии России и/или ФАПСИ на соответствующий вид деятельности в области защиты информации.

В случае разработки СЗИ или ее отдельных компонент специализированным предприятием, в учреждении (на предприятии), для которого осуществляется разработка (предприятие-заказчик), определяются подразделения (или отдельные специалисты), ответственные за организацию и проведение (внедрение и эксплуатацию) мероприятий по защите информации в ходе выполнения работ с использованием конфиденциальной информации.

Разработка и внедрение СЗИ осуществляется во взаимодействии разработчика со службой безопасности предприятия-заказчика, которая осуществляет методическое руководство и участвует в разработке конкретных требований по защите информации, аналитическом обосновании необходимости создания СЗИ, согласовании выбора средств вычислительной техники и связи, технических и программных средств защиты, организации работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации, в аттестации объектов информатизации.

5. Организация работ по созданию и эксплуатации объектов информатизации и их СЗИ определяется в разрабатываемом на предприятии "Руководстве по защите информации" или в специальном "Положении о порядке организации и проведения работ по защите информации" и должна предусматривать:

- порядок определения защищаемой информации;
- порядок привлечения подразделений предприятия, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и СЗИ, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;
- порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
- порядок разработки, ввода в действие и эксплуатацию объектов информатизации;
- ответственность должностных лиц за своевременность и качество формирования требований по технической защите информации, за качество и научно-технический уровень разработки СЗИ.

6. В учреждении (на предприятии) должен быть документально оформлен перечень сведений конфиденциального характера (приложение № 6), подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведениям.

7. Устанавливаются следующие стадии создания системы защиты информации:

- предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание;

− стадия проектирования (разработки проектов) и реализации объекта информатизации, включающая разработку СЗИ в составе объекта информатизации;

− стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации.

8. На предпроектной стадии по обследованию объекта информатизации:

− устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;

− определяется перечень сведений конфиденциального характера, подлежащих защите от утечки по техническим каналам;

− определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;

− определяются условия расположения объектов информатизации относительно границ КЗ;

− определяются конфигурация и топология автоматизированных систем и систем связи в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

− определяются технические средства и системы, предполагаемые к использованию в разрабатываемой АС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;

− определяются режимы обработки информации в АС в целом и в отдельных компонентах;

− определяется класс защищенности АС;

− определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;

− определяются мероприятия по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

9. По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗИ.

На основе действующих нормативных правовых актов и методических документов по защите конфиденциальной информации, в т.ч. настоящего документа, с учетом установленного класса защищенности АС задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗИ.

10. Предпроектное обследование в части определения защищаемой информации должно базироваться на документально оформленных перечнях сведений конфиденциального характера.

Перечень сведений конфиденциального характера составляется заказчиком объекта информатизации и оформляется за подписью соответствующего руководителя.

11. Предпроектное обследование может быть поручено специализированному предприятию, имеющему соответствующую лицензию, но и в этом случае анализ информационного обеспечения в части защищаемой информации целесообразно выполнять представителям предприятия-заказчика при методической помощи специализированного предприятия.

Ознакомление специалистов этого предприятия с защищаемыми сведениями осуществляется в установленном на предприятии-заказчике порядке.

12. Аналитическое обоснование необходимости создания СЗИ должно содержать:

− информационную характеристику и организационную структуру объекта информатизации;

− характеристику комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;

− возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;

− перечень предлагаемых к использованию сертифицированных средств защиты информации;

− обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;

− оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;

− ориентировочные сроки разработки и внедрения СЗИ;

− перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем предпроектного обследования, согласовывается с главным конструктором (должностным лицом, обеспечивающим научно-техническое руководство создания объекта информатизации), руководителем службы безопасности и утверждается руководителем предприятия-заказчика.

13. Техническое (частное техническое) задание на разработку СЗИ должно содержать:

− обоснование разработки;

− исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах;

− класс защищенности АС;

− ссылку на нормативные документы, с учетом которых будет разрабатываться СЗИ и приниматься в эксплуатацию объект информатизации;

− конкретизацию требований к СЗИ на основе действующих нормативно-методических документов и установленного класса защищенности АС;

− перечень предполагаемых к использованию сертифицированных средств защиты информации;

− обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;

− состав, содержание и сроки проведения работ по этапам разработки и внедрения;

− перечень подрядных организаций-исполнителей видов работ;

− перечень предъявляемой заказчику научно-технической продукции и документации.

14. Техническое (частное техническое) задание на разработку СЗИ подписывается разработчиком, согласовывается со службой безопасности предприятия-заказчика, подрядными организациями и утверждается заказчиком.

15. В целях дифференцированного подхода к защите информации производится классификация АС по требованиям защищенности от НСД к информации.

Класс защищенности АС от НСД к информации устанавливается совместно заказчиком и разработчиком АС с привлечением специалистов по защите информации в соответствии с требованиями руководящего документа (РД) Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация

автоматизированных систем и требования по защите информации" и раздела 5 настоящего документа и оформляется актом.

Пересмотр класса защищенности АС производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен.

16. На стадии проектирования и создания объекта информатизации и СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

- разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) объекта информатизации в соответствии с требованиями технического (частного технического) задания на разработку СЗИ;
- разработка раздела технического проекта на объект информатизации в части защиты информации;
- строительно-монтажные работы в соответствии с проектной документацией, утвержденной заказчиком, размещением и монтажом технических средств и систем;
- разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, либо их сертификация;
- закупка сертифицированных технических, программных и программно-технических (в т.ч. криптографических) средств защиты информации и их установка;
- разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;
- организация охраны и физической защиты помещений объекта информатизации, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;
- разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;
- определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;
- выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;
- разработка эксплуатационной документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);
- выполнение других мероприятий, специфичных для конкретных объектов информатизации и направлений защиты информации.

17. Задание на проектирование оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности предприятия-заказчика в части достаточности мер по технической защите информации и утверждается заказчиком.

Мероприятия по защите информации от утечки по техническим каналам являются основным элементом проектных решений, закладываемых в соответствующие разделы проекта, и разрабатываются одновременно с ними.

18. На стадии проектирования и создания объекта информатизации оформляются также технический (техно-рабочий) проект и эксплуатационная документация СЗИ, состоящие из:

- пояснительной записки с изложением решений по комплексу организационных мер и программно-техническим (в том числе криптографическим) средствам обеспечения безопасности информации, состава средств защиты информации с указанием их соответствия требованиям ТЗ;
- описания технического, программного, информационного обеспечения и технологии обработки (передачи) информации;
- плана организационно-технических мероприятий по подготовке объекта информатизации к внедрению средств и мер защиты информации;
- технического паспорта объекта информатизации;
- инструкций и руководств по эксплуатации технических и программных средств защиты для пользователей, администраторов системы, а также для работников службы защиты информации.

19. На стадии ввода в действие объекта информатизации и СЗИ осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком;
- аттестация объекта информатизации по требованиям безопасности информации.

20. На этой стадии оформляются:

- акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний;
- предъявительский акт к проведению аттестационных испытаний;
- заключение по результатам аттестационных испытаний.

При положительных результатах аттестации на объект информатизации оформляется "Аттестат соответствия" требованиям по безопасности информации (форма "Аттестата соответствия" для АС приведена в приложении № 2, для ЗП в приложении № 3)

21. Кроме вышеуказанной документации в учреждении (на предприятии) оформляются приказы, указания и решения:

- о проектировании объекта информатизации, создании соответствующих подразделений разработки и назначении ответственных исполнителей;
- о формировании группы обследования и назначении ее руководителя;
- о заключении соответствующих договоров на проведение работ;
- о назначении лиц, ответственных за эксплуатацию объекта информатизации;
- о начале обработки в АС (обсуждения в защищаемом помещении) конфиденциальной информации.

22. Для объектов информатизации, находящихся в эксплуатации до введения в действие настоящего документа, может быть предусмотрен по решению их заказчика

(владельца) упрощенный вариант их доработки (модернизации), переоформления организационно-распорядительной, технологической и эксплуатационной документации.

Программа аттестационных испытаний такого рода объектов информатизации определяется аттестационной комиссией.

Необходимым условием является их соответствие действующим требованиям по защите информации.

23. Эксплуатация объекта информатизации осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в разделах 4-6 настоящего документа.

24. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность технических средств в учреждении (на предприятии), проводится периодический (не реже одного раза в год) контроль состояния защиты информации.

Контроль осуществляется службой безопасности учреждения (предприятия), а также отраслевыми и федеральными органами контроля (для информации, режим защиты которой определяет государство) и заключается в оценке:

- соблюдения нормативных и методических документов Гостехкомиссии России;
- работоспособности применяемых средств защиты информации в соответствии с их эксплутационной документацией;
- знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

25. Собственник или владелец конфиденциальной информации имеет право обратиться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах.

26. При необходимости по решению руководителя предприятия в ЗП и в местах размещения средств обработки информации могут проводиться работы по обнаружению и изъятию "закладок", предназначенных для скрытого перехвата защищаемой информации.

27. Такие работы могут проводиться организациями, имеющими соответствующие лицензии ФАПСИ или ФСБ России на данный вид деятельности.

ТЕМА 5. КАНАЛЫ И МЕТОДЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

5.1. Методика выявления каналов несанкционированного доступа к информации

Для того чтобы осуществить дестабилизирующее воздействие на защищаемую (конфиденциальную) информацию, людям, не имеющим разрешенного доступа к ней, необходимо его получить. Такой доступ называется несанкционированным(НСД). Как правило, несанкционированный доступ бывает преднамеренным и имеет целью оказать сознательное дестабилизирующее воздействие на защищенную информацию.

Несанкционированный доступ, даже преднамеренный, не всегда является противоправным. Чаще всего он, конечно, бывает незаконным, но нередко не носит криминального характера.

Несанкционированный доступ, осуществляется через существующий или специально создаваемый канал доступа, который определяется как путь, используя который, можно получить неразрешенный доступ к защищаемой информации.

К методам несанкционированного доступа к защищаемой информации относятся:

1. Установление контакта с лицами, имеющими или имевшими доступ к защищаемой информации;
2. Вербовка и (или) внедрение агентов;
3. Организация физического проникновения к носителям защищаемой информации;
4. Подключение к средствам отображение, хранения, обработки, воспроизведения и передачи информации, средствам связи;
5. Прослушивание речевой конфиденциальной информации;
6. Визуальный съем конфиденциальной информации;
7. Перехват электромагнитных излучений;
8. Исследование выпускаемой продукции, производственных отходов и отходов процессов обработки информации;
9. Изучение доступных источников информации;
10. Подключение к системам обеспечения производственной деятельности предприятия;
11. Замеры и взятие проб окружающей объект среды;
12. Анализ архитектурных особенностей некоторых категорий объектов.

Состав реальных для конкретного предприятия каналов несанкционированного доступа к защищаемой информации и степень их опасности зависят от вида деятельности предприятия, категорий носителей, способов обработки информации, системы ее защиты, а также от устремлений и возможностей конкурентов. Однако даже если соперники известны, определить их намерения и возможности практически не удается, поэтому защита должна предусматривать перекрытие всех потенциально существующих для конкретного предприятия каналов.

5.2. Определение возможных методов несанкционированного доступа к защищаемой информации

Использование того или другого канала осуществляется с помощью определенных, присущих конкретному каналу методов и технологий несанкционированного доступа.

Самым распространенным, многообразным по методам несанкционированного доступа, а потому и самым опасным каналом является **установление контакта с лицами, имеющими или имевшими доступ к защищаемой информации.**

В первую группу входят лица, работающие на данном предприятии, а также не работающие на нем, но имеющие доступ к информации предприятия в силу служебного положения (из органов власти, вышестоящих, смежных предприятий и др.). Вторая группа включает уволенных или отстраненных от данной защищаемой информации лиц, в том числе продолжающих работать на предприятии, а также эмигрантов и «перебежчиков». Эта группа наиболее опасна, поскольку нередко имеет дополнительные причины для разглашения информации (обида за увольнение, недовольство государственным устройством и др.).

Контакт с этими людьми может быть установлен различными путями, например на семинарах, выставках, конференциях и других публичных мероприятиях. Опосредованный контакт, осуществляемый через посредников (без прямого общения, диалога), устанавливается через коллег, родственников, знакомых, которые и выступают в роли посредников.

Использование данного канала может иметь целью **уничтожение или искажение информации** с помощью лиц, имеющих к ней доступ, или для получения защищаемой информации. При этом применяются различные методы несанкционированного доступа к информации.

Наиболее распространенным методом является **выведывание информации под благовидным предлогом** («использование собеседника втемную»). Это может осуществляться в неофициальных беседах на публичных мероприятиях и т. д. с включением в них пунктов, касающихся защищаемой информации.

Широко используется метод **переманивания сотрудников конкурирующих предприятий** с тем, чтобы, помимо использования их знаний и умения, получить интересующую защищаемую информацию, относящуюся к прежнему месту их работы.

При использовании метода **покупки защищаемой информации** активно ищут недовольных заработком, руководством, продвижением по службе.

Следующий метод – **принуждение к выдаче защищаемой информации** шантажом, различного рода угрозами, применением физического насилия как к лицу, владеющему информацией, так и к его родственникам и близким.

Можно использовать **склонение к выдаче защищаемой информации** убеждением, лестью, посылами, обманом, в том числе с использованием национальных, политических, религиозных факторов.

С ростом промышленного шпионажа все более опасным каналом становится вербовка и внедрение агентов. Отличие агентов от лиц, осуществляющих разовые продажи защищаемой информации, состоит в том, что агенты работают на постоянной основе, занимаются систематическим сбором защищаемой информации и могут оказывать на нее другое дестабилизирующее воздействие.

С помощью агентов разведывательные службы обычно стремятся получить доступ к такой информации, которую нельзя добыть через другой, менее опасный канал. И хотя агентурная разведка, именуемая в уголовном праве шпионажем, сурово карается, она

практикуется в широких масштабах, поскольку агенты могут получать не только защищаемую информацию, относящуюся к их служебной деятельности, но и иную, используя различные методы несанкционированного доступа к ней, а также оказывать другое дестабилизирующее воздействие на информацию.

Третий метод - это организация физического проникновения к носителям защищаемой информации сотрудников разведывательных служб — используется сравнительно редко, поскольку он связан с большим риском и требует знаний о месте хранения носителей и системе защиты информации, хотя уровень защиты информации в некоторых государственных и многих частных структурах дает возможность получать через этот канал необходимую информацию.

Физическое проникновение лиц, не работающих на объекте, включает **два этапа:** проникновение на территорию (в здания) охраняемого объекта и проникновение к носителям защищаемой информации.

При проникновении на территорию объекта возможно применение следующих методов:

а) использование подложного, украденного или купленного (в том числе и на время) пропуска;

б) маскировка под другое лицо, если пропуск не выдается на руки;

в) проход под видом внешнего обслуживающего персонала;

г) проезд спрятанным в автотранспорте;

д) отвлечение внимания охраны для прохода незамеченным (путем создания чрезвычайных ситуаций, с помощью коллеги и т. д.);

е) изоляция или уничтожение охраны (в редких, чрезвычайных обстоятельствах);

ж) преодоление заграждающих барьеров (заборов), минуя охрану, в том числе и за счет вывода из строя технических средств охраны.

Проникновение к носителям защищаемой информации может осуществляться путем взлома дверей хранилищ и сейфов (шкафов) или их замков, через окна, если проникновение производится в нерабочее время, с отключением (разрушением) сигнализации, телевизионных средств наблюдения (при необходимости), или, при проникновении в рабочее время, путем прохода в комнаты исполнителей, работающих с защищаемыми документами, в производственные и складские помещения для осмотра технологических процессов и продукции, а также в помещения, в которых производится обработка информации.

Проникновение к носителям защищаемой информации осуществляется и во время их транспортировки с использованием, в зависимости от вида, условий и маршрута транспортировки, соответствующих методов.

Целью проникновения является, как правило, получение защищаемой информации, но она может состоять и в оказании на информацию дестабилизирующих воздействий, приводящих к ее уничтожению, искажению, блокированию.

Подключение к средствам отображения, хранения, обработки, воспроизведения и передачи информации, средства связи (четвертый метод несанкционированного доступа к конфиденциальной информации) может осуществляться лицами, находящимися на территории объекта и вне его.

Несанкционированное подключение, а следовательно, и несанкционированный доступ к защищаемой информации может производиться:

а) с персонального компьютера с использованием телефонного набора или с несанкционированного терминала со взломом парольно-ключевых систем защиты или без взлома с помощью маскировки под зарегистрированного пользователя;

б) с помощью программных и радиоэлектронных закладных устройств;

в) с помощью прямого присоединения к кабельным линиям связи, в том числе с использованием параллельных телефонных аппаратов;

г) за счет электромагнитных наводок на параллельно проложенные провода или методов высокочастотного навязывания.

Пятый метод это прослушивание речевой информации — всегда широко использовался, его опасность увеличивается по мере появления новых технических средств прослушивания. При этом речь идет о прослушивании не агентами, находящимися внутри помещения, а лицами, расположенными вне задания, иногда на значительном расстоянии от него. Такое прослушивание чаще всего осуществляется по двум направлениям:

а) подслушивание непосредственных разговоров лиц, допущенных к данной информации;

б) прослушивание речевой информации, зафиксированной на носителе, с помощью подключения к средствам ее звуковоспроизведения.

Шестой метод это визуальный съем защищаемой информации. Может осуществляться следующими способами:

а) чтением документов на рабочих местах пользователей (в том числе с экранов дисплеев, с печатающих устройств) в присутствии пользователей и при их отсутствии;

б) осмотром продукции, наблюдением за технологическим процессом изготовления продукции;

в) просмотром информации, воспроизводимой средствами видеовоспроизводящей техники и телевидения;

г) чтением текста, печатаемого на машинке и размножаемого множительными аппаратами;

д) наблюдением за технологическими процессами изготовления, обработки, размножения информации;

е) считыванием информации в массивах других пользователей, в том числе чтением остаточной информации.

Перехват электромагнитных излучений (седьмой метод) включает в себя перехват техническими средствами как функциональных сигналов, так и особенно побочных, создаваемых техническими средствами отображения, хранения, обработки, воспроизведения, передачи информации, средствами связи, охранной и пожарной сигнализации, системами обеспечения функционирования этих средств, техническими средствами технологических процессов некоторых промышленных объектов, образцами вооружения и военной техники, вспомогательными электрическими и радиоэлектронными средствами (электрическими часами, бытовыми магнитофонами, видеомагнитофонами, радиоприемниками, телевизорами).

Методами перехвата являются поиск сигналов, выделение из них сигналов, несущих защищенную информацию, съем с них информации, ее обработка и анализ.

Этот канал имеет, по сравнению с другими каналами, преимущества: большой объем и высокая достоверность получаемой информации, оперативность ее получения, возможность съема в любое время, скрытность получения, возможность обнародования без угрозы перекрытия канала.

Восьмой метод заключается в исследовании выпускаемой продукции, производственных отходов и отходов процессов обработки информации. Суть этого метода может состоять из:

а) приобретения и разработки (расчленения, выделения отдельных составных частей, элементов) выпускаемых изделий, их химический и физический анализ (обратный инжиниринг) с целью исследования конструкции, компонентов и других характеристик;

б) сбора и изучения поломанных изделий, макетов изделий, бракованных узлов, блоков, устройств, деталей, созданных на стадии опытно-конструкторских разработок, а также руды и шлаков, позволяющих определить состав материалов, а нередко и технологию изготовления продукции;

в) сбора и прочтения черновиков и проектов конфиденциальных документов, копировальной бумаги, красящей ленты печатающих устройств, прокладок, испорченных магнитных дискет.

Следует отметить, что восьмой метод возможен, как правило, при нарушении требований по хранению носителей защищаемой информации и обращению с ними.

Использование **девятого метода** заключается в изучении доступных источников информации, из которых можно получить, защищаемые сведения. Реализация этого метода возможна следующем путем:

а) изучения научных публикаций, содержащихся в специализированных журналах (сборниках);

б) просмотра (прослушивания) средств массовой информации (газет, журналов, теле-и радиопередач);

в) изучения проспектов и каталогов выставок;

г) прослушивания публичных выступлений на семинарах, конференциях и других публичных мероприятиях;

д) изучения формируемых специализированными коммерческими структурами банков данных о предприятиях.

Целью изучения является не только получение прямой конфиденциальной информации, но и накопление, обобщение, сопоставление открытой информации, собранной из различных источников и за определенный промежуток времени, что позволяет «вывести» конфиденциальную информацию. Несмотря на кажущийся парадокс (в открытых источниках закрытая информация), такой анализ даст возможность получить значительное количество конфиденциальной информации.

5.3. СТР-К 4. Требования и рекомендации по защите речевой информации

5.3.1. Общие положения

1. Требования и рекомендации настоящего раздела направлены на исключение (существенное затруднение) возможности перехвата конфиденциальной речевой информации, циркулирующей в ЗП, в системах звукоусиления (СЗУ) и звукового сопровождения кинофильмов (СЗСК), при осуществлении её магнитной звукозаписи и передачи по каналам связи.

2. Требования настоящего раздела, если не оговорено специально, являются обязательными на всех стадиях проектирования, строительства, оснащения, эксплуатации ЗП и размещенных в них ОТСС и ВТСС, для систем СЗУ и СЗСК.

3. При проведении мероприятий с использованием конфиденциальной речевой информации и технических средств ее обработки возможна утечка информации за счет:

а) акустического излучения информативного речевого сигнала;

б) виброакустических сигналов, возникающих посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические системы ЗП;

в) прослушивания разговоров, ведущихся в ЗП, по информационным каналам общего пользования (городская телефонная сеть, сотовая, транкинговая и пейджинговая связь, радиотелефоны) за счет скрытного подключения оконечных устройств этих видов связи;

г) электрических сигналов, возникающих в результате преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющихся по проводам и линиям передачи информации, выходящих за пределы КЗ;

д) побочных электромагнитных излучений информативного сигнала от обрабатывающих конфиденциальную информацию технических средств, в т.ч. возникающих за счет паразитной генерации, и линий передачи информации;

е) электрических сигналов, наводимых от обрабатывающих конфиденциальную информацию технических средств и линий ее передачи, на провода и линии, выходящих за пределы КЗ;

ж) радиоизлучений, модулированных информативным сигналом, возникающим при работе различных генераторов, входящих в состав технических средств, установленных в ЗП, или при наличии паразитной генерации в их узлах (элементах);

з) радиоизлучений, электрических или инфракрасных сигналов, модулированных информативным сигналом, от специальных электронных устройств перехвата речевой информации "закладок", внедренных в ЗП и установленные в них технические средства.

Также следует учитывать возможность хищения технических средств с хранящейся в них информацией или отдельных носителей информации.

5.3.2. Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях

1. В учреждении (предприятии) должен быть документально определен перечень ЗП и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации, а также составлен технический паспорт на ЗП (форма технического паспорта приведена в приложении № 4).

2. Защищаемые помещения должны размещаться в пределах КЗ. При этом рекомендуется размещать их на удалении от границ КЗ, обеспечивающем эффективную защиту, ограждающие конструкции (стены, полы, потолки) не должны являться смежными с помещениями других учреждений (предприятий).

Не рекомендуется располагать ЗП на первых этажах зданий.

Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

3. Защищаемые помещения рекомендуется оснащать сертифицированными по требованиям безопасности информации ОТСС и ВТСС либо средствами, прошедшими специальные исследования и имеющими предписание на эксплуатацию.

Эксплуатация ОТСС, ВТСС должна осуществляться в строгом соответствии с предписаниями и эксплуатационной документацией на них.

4. Специальная проверка ЗП и установленного в нем оборудования с целью выявления возможно внедренных в них электронных устройств перехвата информации "закладок" проводится, при необходимости, по решению руководителя предприятия.

5. Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи, переносных магнитофонов и других средств аудио и видеозаписи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также аппаратов с автоматическим определителем номера, следует отключать их из сети на время проведения этих мероприятий.

6. Для исключения возможности утечки информации за счет электроакустического преобразования рекомендуется использовать в ЗП в качестве оконечных устройств телефонной связи, имеющих прямой выход в городскую АТС, телефонные аппараты (ТА), прошедшие специальные исследования, либо оборудовать их сертифицированными средствами защиты информации от утечки за счет электроакустического преобразования.

7. Для исключения возможности скрытного проключения ТА и прослушивания ведущихся в ЗП разговоров не рекомендуется устанавливать в них цифровые ТА цифровых АТС, имеющих выход в городскую АТС или к которой подключены абоненты, не являющиеся сотрудниками учреждения (предприятия).

В случае необходимости, рекомендуется использовать сертифицированные по требованиям безопасности информации цифровые АТС либо устанавливать в эти помещения аналоговые аппараты.

8. Ввод системы городского радиотрансляционного вещания на территорию учреждения (предприятия) рекомендуется осуществлять через радиотрансляционный узел (буферный усилитель), размещаемый в пределах контролируемой зоны.

При вводе системы городского радиовещания без буферного усилителя в ЗП следует использовать абонентские громкоговорители в защищенном от утечки информации исполнении, а также трехпрограммные абонентские громкоговорители в режиме приема 2-й и 3-й программы (с усилителем).

В случае использования однопрограммного или трехпрограммного абонентского громкоговорителя в режиме приема первой программы (без усиления) необходимо их отключать на период проведения конфиденциальных мероприятий.

9. В случае размещения электрочасовой станции внутри КЗ использование в ЗП электровторичных часов (ЭВЧ) возможно без средств защиты информации

При установке электрочасовой станции вне КЗ в линии ЭВЧ, имеющие выход за пределы КЗ, рекомендуется устанавливать сертифицированные средства защиты информации.

10. Системы пожарной и охранной сигнализации ЗП должны строиться только по проводной схеме сбора информации (связи с пультом) и, как правило, размещаться в пределах одной с ЗП контролируемой зоне.

В качестве оконечных устройств пожарной и охранной сигнализации в ЗП рекомендуется использовать изделия, сертифицированные по требованиям безопасности информации, или образцы средств, прошедшие специальные исследования и имеющие предписание на эксплуатацию.

11. Звукоизоляция ограждающих конструкций ЗП, их систем вентиляции и кондиционирования должна обеспечивать отсутствие возможности прослушивания ведущихся в нем разговоров из-за пределов ЗП.

Проверка достаточности звукоизоляции осуществляется аттестационной комиссией путем подтверждения отсутствия возможности разборчивого прослушивания вне ЗП разговоров, ведущихся в нем.

При этом уровень тестового речевого сигнала должен быть не ниже используемого во время штатного режима эксплуатации помещения.

Для обеспечения необходимого уровня звукоизоляции помещений рекомендуется оборудование дверных проемов тамбурами с двойными дверями, установка дополнительных рам в оконных проемах, уплотнительных прокладок в дверных и оконных притворах и применение шумопоглотителей на выходах вентиляционных каналов.

Если предложенными выше методами не удается обеспечить необходимую акустическую защиту, следует применять организационно-режимные меры, ограничивая на период проведения конфиденциальных мероприятий доступ посторонних лиц в места возможного прослушивания разговоров, ведущихся в ЗП.

12. Для снижения вероятности перехвата информации по виброакустическому каналу следует организационно-режимными мерами исключить возможность установки посторонних (нештатных) предметов на внешней стороне ограждающих конструкций ЗП и выходящих из них инженерных коммуникаций (систем отопления, вентиляции, кондиционирования).

Для снижения уровня виброакустического сигнала рекомендуется расположенные в ЗП элементы инженерно-технических систем отопления, вентиляции оборудовать звукоизолирующими экранами.

13. В случае, если указанные выше меры защиты информации от утечки по акустическому и виброакустическому каналам недостаточны или нецелесообразны, рекомендуется применять метод активного акустического или виброакустического маскирующего зашумления.

Для этой цели должны применяться сертифицированные средства активной защиты.

14. При эксплуатации ЗП необходимо предусматривать организационно-режимные меры, направленные на исключение несанкционированного доступа в помещение:

- двери ЗП в период между мероприятиями, а также в нерабочее время необходимо запирать на ключ;
- выдача ключей от ЗП должна производиться лицам, работающим в нем или ответственным за это помещение;
- установка и замена оборудования, мебели, ремонт ЗП должны производиться только по согласованию и под контролем подразделения (специалиста) по защите информации учреждения (предприятия).

5.3.3. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов

1. В качестве оборудования систем звукоусиления, предназначенных для обслуживания проводимых в ЗП закрытых мероприятий, и систем звукового сопровождения кинофильмов, содержащих конфиденциальные сведения, необходимо использовать оборудование, удовлетворяющее требованиям стандартов по электромагнитной совместимости России, Европейских стран, США (например, ГОСТ 22505-97). В случае необходимости, для повышения уровня защищенности рекомендуется применять оборудование, сертифицированное по требованиям безопасности информации или прошедшее специальные исследования и имеющее предписание на эксплуатацию.

2. Системы звукоусиления должны выполняться по проводной схеме передачи информации экранированными проводами и располагаться в пределах КЗ.

С целью уменьшения побочных электромагнитных излучений целесообразно использовать систему звукоусиления с рассредоточенной системой звукоизлучателей, т.е. следует отдавать предпочтение системам с большим количеством оконечных устройств малой мощности перед системами с малым количеством оконечных устройств большой мощности.

В качестве оконечных устройств рекомендуется использовать звуковые колонки, выпускаемые в защищенном исполнении.

Можно использовать выпускаемые в обычном исполнении громкоговорители с экранированными магнитными цепями (например: 0,5ГДШ-5, 0,5ГД-54, 1ГДШ-2, 1ГДШ-6, 1ГДШ-28, 2ГДШ-3, 2ГДШ-4, 3ГДШ-1) или укомплектованные ими звуковые колонки (например: 2КЗ-7, 6КЗ-8, 12КЗ-18).

В этом случае звуковые колонки (громкоговорители) следует заэкранировать по электрическому полю с помощью металлической сетки с ячейкой не более 1 мм2, заземляемой через экранирующую оплетку подводящего кабеля.

3. В системах звукоусиления рекомендуется применять аппаратуру с симметричными входными и выходными цепями. В случае использования аппаратуры с несимметричным выходом, линии оконечных устройств следует подключать к оконечным усилителям через симметрирующие трансформаторы, устанавливаемые в непосредственной близости от оконечных усилителей.

4. В качестве усилительного оборудования рекомендуется использовать усилители в металлических экранах с возможностью их заземления.

5. Коммутационное и распределительное оборудование (распределительные, входные и выходные щитки подключения) следует размещать в металлических шкафах (коробках). На корпусах шкафов (коробок) необходимо предусмотреть клеммы (винты) для их заземления и приспособления для опечатывания.

6. Усилительное и оконечное оборудование СЗУ, СЗСК следует размещать на возможно большем расстоянии относительно границы контролируемой зоны.

7. Система электропитания и заземления должна соответствовать требованиям "Правил устройства электроустановок (ПУЭ)".

Рекомендуется электропитание и заземление аппаратуры СЗУ и СЗСК осуществлять от подстанции и на заземлитель, расположенные в пределах КЗ.

5.3.4. Защита информации при проведении звукозаписи

1. Запись и воспроизведение конфиденциальной речевой информации аппаратурой звукозаписи разрешается производить только в ЗП.

2. Для записи (воспроизведения) конфиденциальной информации должны применяться магнитофоны (диктофоны), удовлетворяющие требованиям стандартов по электромагнитной совместимости России, Европейских стран, США (например, ГОСТ 22505-97). Для повышения уровня защищенности информации рекомендуется использовать магнитофоны (диктофоны), сертифицированные по требованиям безопасности информации или прошедшие специальные исследования и имеющие предписание на эксплуатацию.

3. Носители информации (магнитные ленты, кассеты) должны учитываться и храниться в подразделениях учреждения (предприятия) в порядке, установленном для конфиденциальной информации.

В учреждении (предприятии) должно быть назначено должностное лицо, ответственное за хранение и использование аппаратуры звукозаписи конфиденциальной информации, и обеспечено хранение и использование этой аппаратуры, исключающее несанкционированный доступ к ней.

5.3.5. Защита речевой информации при её передаче по каналам связи

Передача конфиденциальной речевой информации по открытым проводным каналам связи, выходящим за пределы КЗ, и радиоканалам должна быть исключена.

При необходимости передачи конфиденциальной информации следует использовать защищенные линии связи (например, защищенные волоконно-оптические), устройства скремблирования или криптографической защиты.

Используемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

ТЕМА 6. СТР-К 5 - ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

6.1. Общие требования и рекомендации

1. Система (подсистема) защиты информации, обрабатываемой в автоматизированных системах различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических и, при необходимости, криптографических средств и мер по защите информации при ее автоматизированной обработке и хранении, при ее передаче по каналам связи.

2. Основными направлениями защиты информации являются:

- обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки за счет НСД и специальных воздействий;
- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3. В качестве основных мер защиты информации рекомендуются:

- документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений;
- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;
- ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей АС и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;
- учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;
- использование СЗЗ, создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки;
- необходимое резервирование технических средств и дублирование массивов и носителей информации;
- использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
- использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
- использование сертифицированных средств защиты информации;
- размещение объектов защиты на максимально возможном расстоянии относительно границы КЗ;

- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ;
- развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- электромагнитная развязка между линиями связи и другими цепями ВТСС, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация;
- использование защищенных каналов связи (защищенных ВОЛС и криптографических средств ЗИ;
- размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации;
- организация физической защиты помещений и собственно технических средств с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри контролируемой зоны технических средств разведки или промышленного шпионажа;
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи (при необходимости, определяемой особенностями функционирования конкретных АС и систем связи);
- предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок.

Обязательность тех или иных мер для защиты различных видов конфиденциальной информации конкретизирована в последующих подразделах документа.

4. В целях дифференцированного подхода к защите информации, обрабатываемой в АС различного уровня и назначения, осуществляемого в целях разработки и применения необходимых и достаточных мер и средств защиты информации, проводится классификация автоматизированных систем (форма акта классификации АС приведена в приложении № 1).

5. Классифицируются АС любого уровня и назначения. Классификация АС осуществляется на основании требований РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" и настоящего раздела документа.

6. Классификации подлежат все действующие, но ранее не классифицированные, и разрабатываемые АС, предназначенные для обработки конфиденциальной информации.

7. Если АС, классифицированная ранее, включается в состав вычислительной сети или системы и соединяется с другими техническими средствами линиями связи различной физической природы, образуемая при этом АС более высокого уровня классифицируется в целом, а в отношении АС нижнего уровня классификация не производится.

Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС, за исключением случаев их объединения посредством межсетевого экрана, когда каждая из объединяющихся АС может сохранять свой класс защищенности. Требования к используемым при этом межсетевым экранам изложены в подразделе 5.9.

8. При рассмотрении и определении режима обработки данных в АС учитывается, что индивидуальным (монопольным) режимом обработки считается режим, при котором ко всей

обрабатываемой информации, к программным средствам и носителям информации этой системы допущен только один пользователь.

Режим, при котором различные пользователи, в т.ч. обслуживающий персонал и программисты, работают в одной АС, рассматривается как коллективный. Коллективным режимом работы считается также и последовательный во времени режим работы различных пользователей и обслуживающего персонала.

9. В случае, когда признаки классифицируемой АС (п. 1.7. РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации") не совпадают с предложенными в РД (п. 1.9) группами по особенностям обработки информации в АС, то при классификации выбирается наиболее близкая группа защищенности с предъявлением к АС соответствующих дополнительных требований по защите информации. (Например, однопользовательская АС с информацией различного уровня конфиденциальности по формальным признакам не может быть отнесена к 3 группе защищенности. Однако, если дополнительно реализовать в такой системе управление потоками информации, то необходимый уровень защиты будет обеспечен).

10. Конкретные требования по защите информации и мероприятия по их выполнению определяются в зависимости от установленного для АС класса защищенности. Рекомендуемые классы защищенности АС, СЗЗ, средств защиты информации по уровню контроля отсутствия недекларированных возможностей, а также показатели по классам защищенности СВТ и МЭ от несанкционированного доступа к информации.

11. Лица, допущенные к автоматизированной обработке конфиденциальной информации, несут ответственность за соблюдение ими установленного в учреждении (на предприятии) порядка обеспечения защиты этой информации.

Для получения доступа к конфиденциальной информации они должны изучить требования настоящего документа, других нормативных документов по защите информации, действующих в учреждении (на предприятии) в части их касающейся.

6.2. Основные требования и рекомендации по защите служебной тайны и персональных данных

При разработке и эксплуатации АС, предполагающих использование информации, составляющей служебную тайну, а также персональных данных должны выполняться следующие основные требования.

1. Организация, состав и содержание проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны отвечать определенным требованиям;

2. В учреждении (на предприятии) должны быть документально оформлены перечни сведений, составляющих служебную тайну, и персональных данных, подлежащих защите. Эти перечни могут носить как обобщающий характер в области деятельности учреждения (предприятия), так и иметь отношение к какому-либо отдельному направлению работ. Все исполнители должны быть ознакомлены с этими перечнями в части их касающейся.

3. В соответствии с РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального характера:

- АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;
- АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.

4. Для обработки информации, составляющей служебную тайну, а также для обработки персональных данных следует использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

5. Для передачи информации по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы.

6. Носители информации на магнитной (магнитно-оптической) и бумажной основе должны учитываться, храниться и уничтожаться в подразделениях учреждений (предприятий) в порядке, установленном для служебной информации ограниченного распространения, с пометкой "Для служебного пользования".

7. Доступ к информации исполнителей (пользователей, обслуживающего персонала) осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям конфиденциального характера, действующей в учреждении (на предприятии).

8. При необходимости указанный минимальный набор рекомендуемых организационно-технических мер защиты информации по решению руководителя предприятия может быть расширен.

6.3. Основные рекомендации по защите информации, составляющей коммерческую тайну

При разработке и эксплуатации АС, предполагающих использование сведений, составляющих коммерческую тайну, рекомендуется выполнение следующих основных организационно-технических мероприятий:

1. На предприятии следует документально оформить "Перечень сведений, составляющих коммерческую тайну". Все исполнители должны быть ознакомлены с этим "Перечнем".

2. При организации разработки и эксплуатации АС с использованием таких сведений следует ориентироваться на порядок, приведенный в разделе 3. Оформить порядок разработки и эксплуатации таких АС документально.

3. Рекомендуется относить АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам 3Б, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования).

4. Рекомендуется для обработки информации, составляющей коммерческую тайну, использовать средства вычислительной техники, удовлетворяющие требованиям стандартов

Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

5. Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации.

6. Следует установить на предприятии порядок учета, хранения и уничтожения носителей информации на магнитной (магнитно-оптической) и бумажной основе в научных, производственных и функциональных подразделениях, а также разработать и ввести в действие разрешительную систему допуска исполнителей документам и сведениям, составляющим коммерческую тайну.

Указанный минимальный набор рекомендуемых организационно-технических мероприятий по решению руководителя предприятия может быть расширен.

Решение о составе и содержании мероприятий, а также используемых средств защиты информации принимается руководителем предприятия по результатам обследования создаваемой (модернизируемой) АС с учетом важности (ценности) защищаемой информации.

6.4. Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС

1. Организация эксплуатации АС и СЗИ в ее составе осуществляется в соответствии с установленным в учреждении (на предприятии) порядком, в том числе технологическими инструкциями по эксплуатации СЗИ НСД для пользователей, администраторов АС и работников службы безопасности.

2. Для обеспечения защиты информации в процессе эксплуатации АС рекомендуется предусматривать соблюдение следующих основных положений и требований:

- допуск к защищаемой информации лиц, работающих в АС (пользователей, обслуживающего персонала), должен производиться в соответствии с установленным разрешительной системой допуска порядком;
- на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с санкции руководителя учреждения (предприятия) или руководителя службы безопасности;
- в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;
- по окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;

- изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;
- при увольнении или перемещении администраторов АС руководителем учреждения (предприятия) по согласованию со службой безопасности должны быть приняты меры по оперативному изменению паролей, идентификаторов и ключей шифрования.

3. Все носители информации на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в технологическом процессе обработки информации в АС, подлежат учету в том производственном, научном или функциональном подразделении, которое является владельцем АС, обрабатывающей эту информацию.

4. Учет съемных носителей информации на магнитной или оптической основе (гибкие магнитные диски, съемные накопители информации большой емкости или картриджи, съемные пакеты дисков, иные магнитные, оптические или магнито-оптические диски, магнитные ленты и т.п.), а также распечаток текстовой, графической и иной информации на бумажной или пластиковой (прозрачной) основе осуществляется по карточкам или журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники. Журнальная форма учета может использоваться в АС с небольшим объемом документооборота.

5. Съемные носители информации на магнитной или оптической основе в зависимости от характера или длительности использования допускается учитывать совместно с другими документами по установленным для этого учетным формам.

При этом перед выполнением работ сотрудником, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка "Для служебного пользования", номер экземпляра, подпись этого сотрудника, а также другие возможные реквизиты, идентифицирующие этот носитель.

6. Распечатки допускается учитывать совместно с другими традиционными печатными документами по установленным для этого учетным формам.

7. Временно не используемые носители информации должны храниться пользователем в местах, недоступных для посторонних лиц.

6.5. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ

1. Автоматизированные рабочие места на базе автономных ПЭВМ являются автоматизированными системами, обладающими всеми основными признаками АС. Информационным каналом обмена между такими АС являются носители информации на магнитной (магнитно-оптической) и бумажной основе.

В связи с этим порядок разработки и эксплуатации АРМ на базе автономных ПЭВМ по составу и содержанию проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны полностью отвечать требованиям настоящего документа.

2. АС на базе автономных ПЭВМ в соответствии с требованиями РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" должны быть классифицированы и отнесены:

- к 3 группе АС, если в ней работает только один пользователь, допущенный ко всей информации АС;
- ко 2 и 1 группе АС, если в ней последовательно работают несколько пользователей с равными или разными правами доступа (полномочиями), соответственно.

Примечание: При использовании на автономной ПЭВМ технологии обработки информации на съемных накопителях большой емкости, классификация АС производится на основании анализа режима доступа пользователей АС к информации на используемом съемном накопителе (либо одновременно используемом их комплексе).

6.6 Защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ

1. Данная информационная технология предусматривает запись на загружаемый съемный накопитель информации большой емкости одновременно общесистемного (ОС, СУБД) и прикладного программного обеспечения, а также обрабатываемой информации одного или группы пользователей.

В качестве устройств для работы по этой технологии могут быть использованы накопители на магнитном, магнито-оптическом или лазерном дисках различной конструкции, как встроенные (съемные), так и выносные. Одновременно может быть установлено несколько съемных накопителей информации большой емкости.

Несъемные накопители должны быть исключены из конфигурации ПЭВМ.

Основной особенностью применения данной информационной технологии для АРМ на базе автономных ПЭВМ с точки зрения защиты информации является исключение этапа хранения на ПЭВМ в нерабочее время информации, подлежащей защите.

Эта особенность может быть использована для обработки защищаемой информации без применения сертифицированных средств защиты информации от НСД и использования средств физической защиты помещений этих АРМ.

2. На этапе предпроектного обследования необходимо провести детальный анализ технологического процесса обработки информации, обращая внимание, прежде всего, на технологию обмена информацией (при использовании съемных накопителей информации большой емкости или гибких магнитных дисков (ГМД или дискет) с другими АРМ, как использующими, так и не использующими эту информационную технологию, на создание условий, исключающих попадание конфиденциальной информации на неучтенные носители информации, несанкционированное ознакомление с этой информацией, на организацию выдачи информации на печать.

3. Обмен конфиденциальной информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации.

4. На рабочих местах исполнителей, работающих по этой технологии, во время работы, как правило, не должно быть неучтенных накопителей информации.

В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть "закрыты на запись".

Условия и порядок применения таких процедур должны быть отражены в технологии обработки информации, использующей съемные накопители информации большой емкости.

5. При использовании в этой технологии современных средств вычислительной техники, оснащенных энергонезависимой, управляемой извне перезаписываемой памятью, так называемых Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности, как перед началом работ, с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.

6. Должна быть разработана и по согласованию с службой безопасности утверждена руководителем учреждения (предприятия) технология обработки конфиденциальной информации, использующая съемные накопители информации большой емкости и предусматривающая вышеуказанные, а также другие вопросы защиты информации, имеющие отношение к условиям размещения, эксплуатации АРМ, учету носителей информации, а также другие требования, вытекающие из особенностей функционирования АРМ.

6.7. Защита информации в локальных вычислительных сетях

1. Характерными особенностями ЛВС являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.

2. Средства защиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного сопровождения со стороны администратора безопасности информации.

3. Информация, составляющая служебную тайну, и персональные данные могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или в условиях, изложенных в пунктах 4. и 5. следующего подраздела.

4. Класс защищенности ЛВС определяется в соответствии с требованиями РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации".

5. Для управления ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, в дополнение к системным администраторам (администраторам ЛВС) могут быть назначены администраторы по безопасности информации, имеющие необходимые привилегии доступа к защищаемой информации ЛВС.

6. Состав пользователей ЛВС должен устанавливаться по письменному разрешению руководства предприятия (структурного подразделения) и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

7. Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств, используемых для защиты информации при передаче ее по каналам связи и хранения, и для систем электронной цифровой подписи.

6.8. Защита информации при межсетевом взаимодействии

1. Положения данного подраздела относятся к взаимодействию локальных сетей, ни одна из которых не имеет выхода в сети общего пользования типа Internet.

2. Взаимодействие ЛВС с другими вычислительными сетями должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах КЗ.

3. При конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.

4. Подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

5. Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:

- в АС класса 1Г - МЭ не ниже класса 4;
- в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.

Если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

6.9. Защита информации при работе с системами управления базами данных

1. При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:

- в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;
- БД могут быть физически распределены по различным устройствам и узлам сети;
- БД могут включать информацию различного уровня конфиденциальности;
- разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;
- разграничение доступа пользователей к объектам БД: таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п., может осуществляться только средствами СУБД, если таковые имеются;
- регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД, если таковые имеются;
- СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).

2. С учетом указанных особенностей при создании БД рекомендуется:

- при выборе СУБД ориентироваться на операционные системы и СУБД, включающие либо штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;
- при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;
- при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.

ТЕМА 7. СТР-К 6 РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В НЕГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСАХ, ПРИ ВЗАИМОДЕЙСТВИИ АБОНЕНТОВ С ИНФОРМАЦИОННЫМИ СЕТЯМИ ОБЩЕГО ПОЛЬЗОВАНИЯ

7.1. Общие положения

1. В настоящем разделе приведены рекомендации, определяющие условия и порядок подключения абонентов к информационным сетям общего пользования (Сетям), а также рекомендации по обеспечению безопасности конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (коммерческая тайна - в соответствии с п.2.3. СТР-К), при подключении и взаимодействии абонентов с этими сетями.

2. Данные рекомендации определены, исходя из требований РД "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации", настоящего документа, а также следующих основных угроз безопасности информации, возникающих при взаимодействии с информационными сетями общего пользования:

- несанкционированного доступа к информации, хранящейся и обрабатываемой во внутренних ЛВС (серверах, рабочих станциях) или на автономных ПЭВМ, как из Сетей, так и из внутренних ЛВС;
- несанкционированного доступа к коммуникационному оборудованию (маршрутизатору, концентратору, мосту, мультиплексору, серверу, Web/Proxy серверу), соединяющему внутренние ЛВС учреждения (предприятия) с Сетями;
- несанкционированного доступа к данным (сообщениям), передаваемым между внутренними ЛВС и Сетями, включая их модификацию, имитацию и уничтожение;
- заражения программного обеспечения компьютерными "вирусами" из Сети, как посредством приема "зараженных" файлов, так и посредством E-mail, апплетов языка JAVA и объектов ActiveX Control;
- внедрения программных закладок с целью получения НСД к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с Сетями;
- несанкционированной передачи защищаемой конфиденциальной информации ЛВС в Сеть;
- возможности перехвата информации внутренней ЛВС за счет побочных электромагнитных излучений и наводок от основных технических средств, обрабатывающих такую информацию.

7.2. Условия подключения абонентов к Сети

1. Подключение к Сети абонентского пункта (АП) осуществляется по решению руководителя учреждения (предприятия) на основании соответствующего обоснования.

2. Обоснование необходимости подключения АП к Сети должно содержать:

- наименование Сети, к которой осуществляется подключение, и реквизиты организации-владельца Сети и провайдера Сети;

- состав технических средств для оборудования АП;
- предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, Telnet, HTTP и т.п.) для АП в целом и для каждого абонента, в частности;
- режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);
- состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети - Browsers и т.п.);
- число и перечень предполагаемых абонентов (диапазон используемых IP- адресов);
- меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;
- перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из Сети.

3. Право подключения к Сети АП, не оборудованного средствами защиты информации от НСД, может быть предоставлено только в случае обработки на АП информации с открытым доступом, оформленной в установленном порядке как разрешенной к открытому опубликованию. В этом случае к АП, представляющим собой автономную ПЭВМ с модемом, специальные требования по защите информации от НСД не предъявляются.

4. Подключение к Сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, не разрешенная к открытому опубликованию, разрешается только после установки на АП средств защиты информации от НСД, отвечающих требованиям и рекомендациям, изложенным в подразделе 7.3.

7.3. Порядок подключения и взаимодействия абонентских пунктов с Сетью, требования и рекомендации по обеспечению безопасности информации

1. Подключение АП к Сети должно осуществляться в установленном порядке через провайдера Сети.

2. Подключение ЛВС предприятия (учреждения) к Сети должно осуществляться через средства разграничения доступа в виде МЭ (Firewall, Брандмауэр). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

3. Доступ к МЭ, к средствам его конфигурирования должен осуществляться только выделенным администратором с консоли. Средства удаленного управления МЭ должны быть исключены из конфигурации.

4. АП с помощью МЭ должен обеспечивать создание сеансов связи абонентов с внешними серверами Сети и получать с этих серверов только ответы на запросы абонентов. Настройка МЭ должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться на АП.

5. При использовании почтового сервера и Web-сервера предприятия, последние не должны входить в состав ЛВС АП и должны подключаться к Сети по отдельному сетевому фрагменту (через маршрутизатор).

6. На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения АП к Сети (обоснование может корректироваться в установленном на предприятии порядке).

Не допускается активизация не включенных в обоснование прикладных серверов (протоколов) и не требующих привязок протоколов к портам.

7. Установку программного обеспечения, обеспечивающего функционирование АП, должны выполнять уполномоченные специалисты под контролем администратора. Абоненты АП не имеют права производить самостоятельную установку и модификацию указанного программного обеспечения, однако могут обращаться к администратору для проведения его экспертизы на предмет улучшения характеристик, наличия "вирусов", замаскированных возможностей выполнения непредусмотренных действий. Вся ответственность за использование не прошедшего экспертизу и не рекомендованного к использованию программного обеспечения целиком ложится на абонента АП. При обнаружении фактов такого рода администратор обязан логически (а при необходимости - физически вместе с включающей подсетью) отключить рабочее место абонента от Сети и ЛВС и поставить об этом в известность руководство.

8. Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП (АС) и отвечать требованиям РД Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

9. СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС предприятия при обработке на них конфиденциальной информации, должна осуществлять:

- идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;
- контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;
- регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;
- регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны администратора, ответственного за эксплуатацию АП.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента.

СЗИ НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводится не реже одного раза в год.

10. Технические средства АП должны быть размещены либо в отдельном помещении (при автономной ПЭВМ, подключенной к Сети), либо в рабочих помещениях абонентов с принятием организационных и технических мер, исключающих несанкционированную работу в Сети. В этих помещениях должно быть исключено ведение конфиденциальных переговоров, либо технические средства должны быть защищены с точки зрения электроакустики. В нерабочее время помещение автономной ПЭВМ либо соответствующего сервера сдается под охрану в установленном порядке.

11. При создании АП рекомендуется:

11.1. По возможности размещать МЭ для связи с внешними Сетями, Web-серверы, почтовые серверы в отдельном ЗП, доступ в которое имел бы ограниченный круг лиц (ответственные специалисты, администраторы). Периодически проверять работоспособность МЭ с помощью сканеров, имитирующих внешние атаки на внутреннюю ЛВС. Не следует устанавливать на МЭ какие-либо другие прикладные сервисы (СУБД, E-mail, прикладные серверы и т.п.).

11.2. При предоставлении абонентам прикладных сервисов исходить из принципа минимальной достаточности. Тем пользователям АП, которым не требуются услуги Сети, не предоставлять их. Пользователям, которым необходима только электронная почта (E-mail), предоставлять только доступ к ней. Максимальный перечень предоставляемых прикладных сервисов ограничивать следующими: E-mail, FTP, HTTP, Telnet.

11.3. При создании АП следует использовать операционные системы со встроенными функциями защиты информации от НСД, перечисленными в п.6.3.9, или использовать сертифицированные СЗИ НСД.

11.4. Эффективно использовать имеющиеся в маршрутизаторах средства разграничения доступа (фильтрацию), включающие контроль по списку доступа, аутентификацию пользователей, взаимную аутентификацию маршрутизаторов.

11.5. В целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в том числе на наличие "вирусов". Копии исходящей электронной почты и отсылаемых в Сеть файлов следует направлять в адрес защищенного архива АП для последующего анализа со стороны администратора (службы безопасности).

11.6. Проводить постоянный контроль информации, помещаемой на Web-серверы предприятия. Для этого следует назначить ответственного (ответственных) за ведение информации на Web-сервере. Предусмотреть порядок размещения на Web-сервере информации, разрешенной к открытому опубликованию.

12. Приказом по учреждению (предприятию) назначаются лица (абоненты), допущенные к работам в Сети с соответствующими полномочиями, лица, ответственные за эксплуатацию указанного АП и контроль за выполнением мероприятий по обеспечению безопасности информации при работе абонентов в Сети (руководители подразделений и администраторы).

13. Вопросы обеспечения безопасности информации на АП должны быть отражены в инструкции, определяющей:

- порядок подключения и регистрации абонентов в Сети;

− порядок установки и конфигурирования на АП общесистемного, прикладного коммуникационного программного обеспечения (серверов, маршрутизаторов, шлюзов, мостов, межсетевых экранов, Browsers), их новых версий;

− порядок применения средств защиты информации от НСД на АП при взаимодействии абонентов с Сетью;

− порядок работы абонентов в Сети, в том числе с электронной почтой (E-mail), порядок выбора и доступа к внутренним и внешним серверам Сети (Web-серверам);

− порядок оформления разрешений на отправку данных в Сеть (при необходимости);

− обязанности и ответственность абонентов и администратора внутренней ЛВС по обеспечению безопасности информации при взаимодействии с Сетью;

− порядок контроля за выполнением мероприятий по обеспечению безопасности информации и работой абонентов Сети.

14. К работе в качестве абонентов Сети допускается круг пользователей, ознакомленных с требованиями по взаимодействию с другими абонентами Сети и обеспечению при этом безопасности информации и допускаемых к самостоятельной работе в Сети после сдачи соответствующего зачета.

15. Абоненты Сети обязаны:

− знать порядок регистрации и взаимодействия в Сети;

− знать инструкцию по обеспечению безопасности информации на АП;

− знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);

− уметь пользоваться средствами антивирусной защиты;

− после окончания работы в Сети проверить свое рабочее место на наличие "вирусов".

16. Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в Сети носители информации учитываются в журналах несекретного делопроизводства. При этом на корпусе (конверте) носителя информации наносится предупреждающая маркировка: "Допускается использование только в Сети ____".

17. Для приемки в эксплуатацию АП, подключаемого к Сети, приказом по учреждению (предприятию) назначается аттестационная комиссия, проверяющая выполнение установленных требований и рекомендаций. Аттестационная комиссия в своей работе руководствуется требованиями и рекомендациями настоящего документа.

18. По результатам работы комиссии оформляется заключение, в котором отражаются следующие сведения:

− типы и номера выделенных технических средств АП, в т.ч. каждого абонента, их состав и конфигурация;

− состав общего и сервисного прикладного коммуникационного программного обеспечения (ОС, маршрутизаторов, серверов, межсетевых экранов, Browsers и т.п.) на АП в целом и на каждой рабочей станции абонента, в частности: логические адреса (IP-адреса), используемые для доступа в Сети;

− мероприятия по обеспечению безопасности информации, проведенные при установке технических средств и программного обеспечения, в т.ч. средств защиты

информации от НСД, антивирусных средств, по защите информации от утечки по каналам ПЭМИН, наличие инструкции по обеспечению безопасности информации на АП.

19. При работе в Сети категорически запрещается:

− подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к Сети;

− изменять состав и конфигурацию программных и технических средств АП без санкции администратора и аттестационной комиссии;

− производить отправку данных без соответствующего разрешения;

− использовать носители информации с маркировкой: "Допускается использование только в Сети ____" на рабочих местах других систем (в том числе и автономных ПЭВМ) без соответствующей санкции.

20. Ведение учета абонентов, подключенных к Сети, организуется в устанавливаемом в учреждении (на предприятии) порядке.

Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на администраторов АП, руководителей соответствующих подразделений, определенных приказом по учреждению (предприятию), а также руководителя службы безопасности.

ТЕМА 8. ДЕЛОВАЯ РАЗВЕДКА

8.1. Деловая разведка как канал несанкционированного доступа для получения информации

Долгое время разведдеятельность являлась государственной монополией. А образ разведчика с «чистыми руками, холодной головой и горячим сердцем» (такой, как Штирлиц) знаком всем до боли.

Меняются времена... Меняется представление о разведке. И сегодня она уже не является прерогативой государственных служб, работавших только на свое правительство. В наше время — это настоятельная потребность любой корпорации, которая хочет жить и развиваться. Управляющие предприятий не могут позволить себе использовать неточную информацию о том, куда планируют двигаться их конкуренты, или о том, как те, кто еще не являются конкурентами, быстро и скрытно завоевывают свою долю рынка. Они понимают, что победа сегодня всего лишь дает возможность быть конкурентоспособным завтра. Такая деятельность получила благозвучное название – **деловая разведка,** она подразумевает этически выдержанные и законодательно не ограниченные сбор, систематизацию и анализ открытой информации.

Основная задача деловой (коммерческой) разведки — обеспечение стратегического менеджмента фирмы, ее генеральной, в том числе маркетинговой стратегии (или стратегий). Обеспечение, прежде всего, информацией упреждающего характера, информацией, предоставляющей конкурентные преимущества (стратегического или тактического характера), информацией, позволяющей принимать грамотные решения адекватные складывающейся оперативной обстановке и условиям окружающей конкурентной, агрессивной среды.

Какими методами осуществляется данная деятельность?

1. **Пассивными методами**, т.е. работой со вторичными источниками (что в большинстве случаев подразумевает методы конкурентной разведки) и активными методами, т. е. работой с первоисточниками (агентурные возможности), наблюдением, проведением активных мероприятий и иными методами добывания достоверной разведывательной информации.

2. **Активные методы** разведывательной деятельности очень часто, и небезосновательно, относят к методам промышленного шпионажа, однако именно они могут предоставить конкурентные преимущества фирме (ее разведоргану), осуществляющей разведку. Совершенно необязательно, что указанные методы являются преступными (противозаконными), другое дело, что в большинстве случаев они осуществляются негласно, т. е. тайно. Здесь стоит вспомнить, что практически все разведсведения добываются не глубоко законспирированными резидентами, а методом анализа открытых источников информации: пресса, телевидение, компьютерные сети...

В учебниках по контрразведке в свое время фигурировали цифры 70-80% по отношению к спецслужбам вероятного противника, работающим против СССР. Сохраняется этот принцип и в работе деловой разведки.

Контрразведка (контрразведывательная деятельность) предназначена для защиты и обеспечения безопасности субъекта предпринимательской деятельности. В качестве объектов контрразведки выступают различные факторы группы риска, оказывающие, в той или иной степени, негативное воздействие на субъект защиты, основными из которых являются

противоправная деятельность конкурентов, криминальных структур, проявления фактов промышленного (коммерческого) шпионажа, мошенничества и иных действующих рисков. Как уже говорилось, основная задача контрразведки обеспечение безопасности, защита субъекта предпринимательской деятельности, другими словами, контрразведка — это, прежде всего, оборона. Поэтому этот аспект мы рассматривать не будем.

Под деловой разведкой подразумеваются **четыре различных направления сбора информации:**

1) Сбор данных о партнерах и клиентах для предотвращения мошенничеств с их стороны;

2) Определение потенциальных партнеров и сотрудников. Речь, в первую очередь, идет о реальном финансовом положении и наличии и/или характере связей (криминальные структуры, милиция, спецслужбы и пр.);

3) Выполнение услуг предусмотренных «Законом о частной детективной и охранной деятельности» (поиск имущества должника и т. п.);

4) Сбор информации маркетингового характера.

Несмотря на то, что деловая разведка является развивающейся сферой деятельности, ее цели и задачи определены достаточно четко. Это службы, отвечающие за сбор, накопление и анализ информации о конкурентах и потенциальных партнерах, за проведение маркетинговых исследований и прогноз возможных рисков. Деловая разведка подразумевает использование опыта различных отраслей: экономики, юриспруденции, деятельности спецслужб. И первый вопрос, который задается, — степень легитимности деловой разведки. Четкую границу между промышленным шпионажем и деловой разведкой провести трудно. И все же главное отличие деловой разведки состоит в том, что вся информация добывается законными способами.

Если в промышленном шпионаже используют методы, которые подразумевают прямое нарушение закона: шантаж, подкуп, воровство, насилие, физическое устранение, — то в деловой разведке невозможно обращение к таким приемам. Другой аспект — соблюдение норм морали. Ведь в данном случае при их нарушении не последует никаких карательных акций. Некоторые компании декларируют кодекс поведения, несмотря на то, что это может ограничить возможности работников. Чем можно объяснить подобное стремление? Во-первых, заботой об имени и репутации фирмы. Во-вторых, таким образом можно застраховать себя от множества негативных последствий (например, судебных разбирательств).

Каковы же общие этические принципы ведения деловой разведки? Можно выделить следующие правила: отказ от получения информации путем обмана, шантажа; отказ от противоправных действий,

В принципе, все выделенные аспекты лишний раз напоминают о том, что при проведении деловой разведки необходимо использовать законные методы, несоблюдение этих норм влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность.

В России вопросы права на информацию полны парадоксов. С одной стороны, в нашей стране существует около 20 видов тайны, поэтому теоретически можно ограничить доступ к сведениям почти по любой тематике. При этом отсутствует законодательство, которое регулирует открытость различных категорий данных (тех же кредитных историй юридических и физических лиц). С другой стороны, коррупция чиновников всех уровней позволяет без особого труда добыть нужные сведения. На рынках, торгующих электроникой, и в Интернете можно сегодня купить CD-ROM со служебными базами данных практически всех государственных ведомств: начиная с таможни и ГИБДД, заканчивая списками владельцев

элитного жилья и базами данных телефонных сетей. Причем в последних есть даже «закрытые» телефоны и адреса сотрудников МВД, ФСБ, судей, политиков, эстрадных звезд.

Большую часть всей информации разведка получает из открытых источников. Основную роль в этой категории сегодня играет Интернет, открывающий доступ к СМИ, сайтам компаний, профессиональным базам данных и т. п. Интернет-сеть дает возможность получить сведения о любом человеке, товаре, предприятии. Посетить сайт компании — все равно что побывать в самой фирме. Здесь можно найти информацию об услугах, продукции, контактах, сотрудниках, планах, новинках и т.п.; ярмарки, выставки, конференции, семинары. Главная проблема такого поиска в том, что данные не структурированы и зачастую их невозможно найти с помощью поисковых систем.

Вторая группа источников — всевозможные бумажные документы: подшивки газет и журналов, реклама, пресс-релизы; еще в 1930-е годы аналитики советской и германской разведок могли похвастаться многочисленными достижениями в этой сфере.

Кроме того, очень популярны имеющиеся в продаже, но в отличие от упоминавшихся выше вполне легальные базы данных госучреждений. Особенно часто используются базы данных Московской регистрационной палаты, регистрационных органов других городов и регионов России, Госкомстата, Торгово-промышленной палаты, Госкомимущества. Отдельные доступные базы данных есть в некоторых министерствах и комитетах. Существует негосударственная база данных «Лабиринт», составленная на основе публикаций ведущих изданий, с помощью которой можно получить обширную информацию о конкретных персоналиях и компаниях.

Для облегчения работы аналитиков созданы специальные компьютерные программы, позволяющие в кратчайшие сроки отбирать и сортировать информацию из СМИ и баз данных. На сегодняшний день их разработано более двухсот.

Хорошую информацию о конкурентах приносит визуальный мониторинг. Его использование может подкорректировать представление о стратегии компании конкурента. Как правило, к проведению таких акций, как выставки или конференции, очень тщательно готовятся, фирмы хотят продемонстрировать свою новую продукцию или хотя бы рассказать о ней. Посещение подобных мероприятий дает возможность получить наглядное впечатление, определить степень интереса к новинке как со стороны потенциальных партнеров, так и со стороны потребителя, увидеть результаты всевозможных тестов или сравнительных испытаний. Небезынтересным в этом смысле будет изучение книги отзывов. К визуальному мониторингу можно отнести и обход торговых точек конкурирующих компаний. Наблюдения такого рода дают материал о товарном ассортименте, работе персонала, услугах, ценовой политике, портрете покупателя и т.п.; неформальное общение с коллегами и партнерами. Не должна ускользать от внимания и информация, не подтвержденная официальными источниками или СМИ. Кулуарные беседы с коллегами по бизнесу зачастую способны добавить более достоверные сведения.

Важно уделять внимание не только специальной литературе или профильным изданиям. Часто крупицы информации можно обнаружить в неосторожном интервью или необдуманном комментарии. Даже рекламные объявления или список опубликованных вакансий способны навести на размышления о планируемых мероприятиях.

Хотя методы деловой разведки еще только формируются, очевидно, что без применения современных компьютерных технологий и умения работать с информацией положительных результатов не будет. При этом речь идет о работе не столько со средствами

массовой информации, сколько со специальными, сложными информационными системами, обеспечивающими доступ ко всем открытым источникам.

Практическое использование программных продуктов сетевой разведки дает, в частности, возможность:

а) постоянно отслеживать и анализировать информацию, имеющую отношение к деловой деятельности клиента;

б) выбирать специфическую информацию, которую обычно не предоставляют информационно-поисковые системы общего пользования;

в) наладить постоянный поток информации о действиях конкурента (таких как ценовая политика, слияния и поглощения, рекламные объявления и анонсы);

г) раскрывать планы конкурента еще до их реализации;

д) проводить изучение потенциального спроса на продукцию и услуги.

Деловая разведка — это постоянный процесс сбора, обработки, оценки и накопления данных, их анализа с целью принятия оптимальных решений. В самом процессе ее проведения можно выделить следующие этапы:

1. сбор данных, которые, по сути, еще не являются информацией;
2. структурирование информации;
3. хранение и анализ структурированных данных;
4. синтез знаний, которые и станут первым продуктом деловой разведки;
5. фаза принятия управленческого решения (стратегического или тактического);
6. принятие решения приводит к действию и, соответственно, к конкретному результату.

Разведывательная деятельность является одной из разновидностей информационной работы, основополагающий принцип которой — четкое разделение понятий: данные (сведения), информация и знания.

Когда говорят, что для принятия решения необходимо осмыслить огромное количество информации, то совершают огромную понятийную ошибку, смешивая термины «данные» и «информация». Часто бывает много данных, а информации как раз недостаточно.

Понимание этой разницы помогает сделать процесс принятия решений более эффективным. В чем же различие? Данные основаны на фактах. Это может быть статистика, отрывки информации о персоналиях, хозяйствующих субъектах, т. е. обо все том, что представляет оперативный интерес. Дилетантам часто кажется, что данные могут о чем-то рассказать, но на самом деле этого не происходит. Никто не может принять правильное решение, исходя только из данных, независимо от того, насколько они точны или обширны.

Информация, напротив, представляет собой некую совокупность данных, которые были отобраны, обработаны и проанализированы, после чего их можно использовать для дальнейших действий.

Синтезированные решения и рекомендации представляют собой конечный информационный продукт — знания. Лицу, принимающему решение, нужны именно информация и знания, а не просто данные.

8.2. Информационный продукт как следствие реализации несанкционированных действий

Остановимся на принципах информационной работы.

1) **Определение цели**. Подход к решению любой информационной задачи должен зависеть то того, в каких целях будут использованы полученные результаты. Цель задания не только определяет сроки его выполнения, но и размах работы, форму изложения и подход к работе. И хотя непосредственная цель информационного документа5 как правило, состоит в решении «задачи», может существовать и более широкая цель: использовать полученное решение задачи для выработки дальнейшего курса, или руководства к действию.

2) **Определение понятий.** Вопрос терминологии всегда считался самым сложным в любой сфере деятельности. Четкие определения особенно необходимы и в информационной работе деловой разведки. Четкие определения заставляют четко мыслить и сосредоточиться на достижении действительно желаемой цели и ограждают от ошибок. Для примера достаточно вспомнить широко употребляемые термины, такие, как уязвимые места, возможности и т. д.

3) **Использование имеющихся источников.** Для реализации этого принципа требуется тщательно использовать все источники, из которых можно почерпнуть сведения по изучаемому вопросу. При этом необходимо определить пределы использования каждого источника, а также в какой степени содержащиеся в них данные подтверждают или опровергают друг друга. Чем больше источников, тем легче произвести перепроверку. При использовании многих источников разведывательная информация получает более широкую основу, рассматриваемые вопросы освещаются глубже и уменьшается возможность допустить серьезную ошибку.

4) **Раскрытие значения фактов.** Этот принцип требует выяснять смысл сырых фактов. Добиться этого можно, например, путем сравнения имеющихся данных с аналогичными, полученными ранее (например, год назад). Показывая значения факта, мы тем самым в большой степени увеличиваем его полезность. Факты редко говорят сами за себя.

5) **Установление причины и следствия.** При решении любой информационной задачи исследователь должен установить причинно-следственные связи межу различными явлениями. Это поможет выявить решающий фактор.

6) **Определение тенденций развития**. Необходимо установить, развивается ли изучаемое явление по восходящей или нисходящей линии и с какой динамикой. Является ли тенденция развития событий устойчивой, циклической, или неизменной. Учет тенденций тесно связан с предвидением.

7) **Степень достоверности**. Этот принцип подразумевает учет достоверности полученных данных, точность цифрового материала и степень правильности оценок и выводов. Эти три аспекта являются элементами понятия степени достоверности. В каждом конкретном случае степень достоверности полученных данных, точности цифрового материала и правильности оценок и выводов может быть высокой, малой и средней.

8) **Выводы.** Собственно, в выводах и состоит цель всей работы. Именно правильно сделанные выводы могут стать достижением поставленной цели. Выводы должны быть сделаны кратко и четко, но так, чтобы краткость не порождала неправильные представления.

Информационная работа представляет собой замкнутый цикл в результате прохождения которого из «сырой» информации получаются разведывательные сведения.

На рис 8.1. представлены **этапы (цикл) информационной работы.**

Этап 1. Общее знакомство с проблемой. Ознакомление с проблемой в целом, а также со смежными вопросами, изучение которых может оказаться полезным; составление общего плана работы с указанием срока выполнения, исполнителей и основных источников, которые предположительно могут быть использованы.

Этап 2. Определение используемых терминов и понятий. Необходимо определить и объяснить тот или иной термин или понятие так, чтобы это было ясно нам самим, тем, кто контролирует нашу работу, и тем, кто пользуется нашей информацией. Следует определить, что мы имеем и чего не имеем в виду, когда употребляем тот или иной термин или понятие.

Этап 3. Сбор фактов.

Этап 4. Истолкование фактов. Так кратко можно назвать процесс изучения и обработки фактов с целью выжать из них все, что они значат. Этот этап включает оценку, классификацию, анализ и уяснение фактов. Иногда полезно на основе имеющихся фактов построить диаграммы, графики, подвергнуть их статистическому анализу.

Обратная последовательность этапов информационной работы. Прямая последовательность этапов информационной работы.

Этап 5. Построение гипотезы. Рабочие гипотезы, выдвигаемые на этом этапе, обычно связаны с какими-либо конкретными вопросами, отвечая на которые можно проверить сами гипотезы. Построение гипотезы, взятое в широком смысле, всегда присуще любой исследовательской работе. В самом начале исследования, когда вырабатывается общий план, мы исходим из определенных предположений (или гипотез) о том, какие факторы, вероятно, играют важную роль и какие почти определенно не имеют отношения к делу. Аналогичными гипотезами мы руководствуемся при сборе и истолковании фактов, формулировании выводов и предложений.

Этап 6. Выводы. На этом этапе производятся исследования, необходимые для доказательства или опровержения рабочих гипотез, выдвинутых на этапе 5, и формулируются окончательные выводы.

Этап 7. Изложение. Составление документа, завершающее работу. Составитель информационного документа должен не только ясно представлять себе то, о чем он пишет, но и уметь выразить свои мысли в ясной форме. Причем необходимо не только сформулировать полученные результаты, но и указать степень достоверности каждого утверждения.

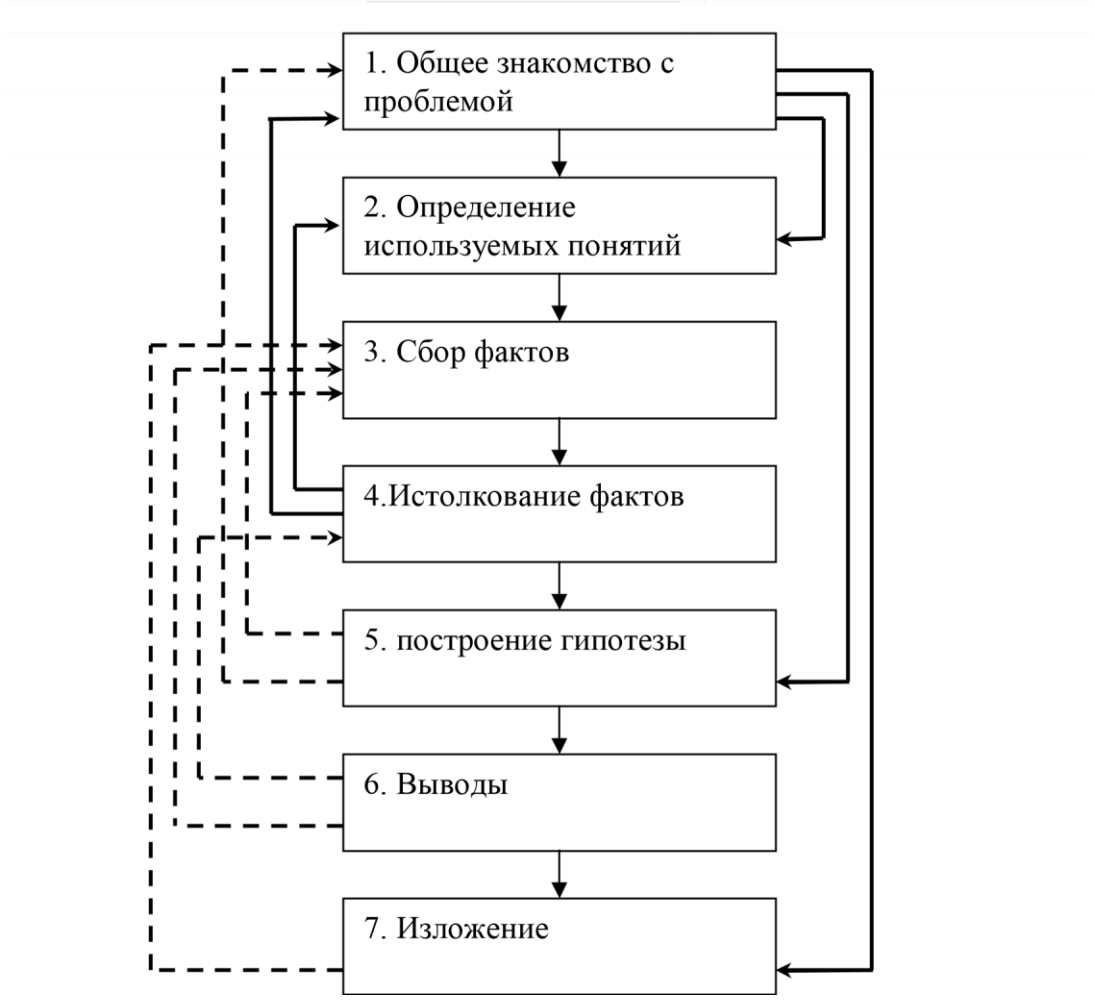

Рисунок 8.1. Последовательность этапов информационной работы

Работа, проделанная на каждом этапе, считается предварительной, и могут быть внесены изменения в зависимости от новых данных, полученных по мере продолжения исследования на последующих этапах. Например, сбор фактов нельзя провести сразу и закончить в один прием.

После того как собрана часть фактов, их истолкование, несомненно, покажет, по каким вопросам требуется собрать дополнительные факты, и тем самым даст направление последующей исследовательской работе.

Точно так же дело обстоит и на других этапах. Например, общий план работы является в момент его разработки предварительным. Мы должны быть готовы принять его и в равной мере должны быть готовы возвращаться назад и вносить изменения в наш предварительный план каждый раз, когда в свете новых данных в этом возникнет необходимость.

Применяя метод обратной последовательности этапов, мы расширяем свои знания по изучаемому вопросу.

Необходимо отметить место, занимаемое этапом «построения гипотезы» во всем процессе (или цикле) информационной работы.

Мы видели, что все предварительное планирование работы по выполнению поставленного перед нами задания подсознательно основывается на предположениях и догадках, которые имеют отношение к изучаемой проблеме.

Фактически без гипотез мы не можем даже думать об исследовании какого-либо вопроса. Иногда, составляя перечень этих гипотез и критически оценивая правильность каждой из них, мы обнаруживаем некоторые старые ошибки и находим более успешный метод решения стоящих перед нами задач. Большое количество предположений, выдвигаемых в процессе исследовательской работы, редко подтверждается или выясняется, что некоторые из них содержат серьезные ошибки.

Из всех этапов информационной работы построение гипотезы больше всех связано с процессом чистого мышления. Построение гипотезы практически можно рассматривать как важнейший этап исследовательского цикла, а все остальные основные этапы — как вспомогательные.

Информационная работа — это процесс творческого мышления. Условно его можно разделить **на четыре стадии:**

1. Накопление знаний и сведений;
2. Анализ материала;
3. Выводы;
4. Проверка выводов.

Можно связать стадии творческого мышления с основными этапами информационной работы (рис 8.2.).

На стадии накопления знаний и сведений мы сталкиваемся с огромной массой фактов, которые в большей или меньшей степени относятся к делу. С ошибками, предрассудками, идеями, представлениями, накопившимися в нашем сознании в результате образования и всего жизненного опыта. Некоторые идеи и представления, имеющие прямое отношение к поставленной задаче, могут быть выражением общепринятых взглядов и накладывать отпечаток на определение подхода к проблеме на сознательный и подсознательный процесс мышления.

То есть в информационной работе разведки часто бывает очень важно по-новому взглянуть на существующие обстоятельства, критически их переоценить.

Рисунок 8.2. Четыре стадии процесса творческого мышления
во взаимосвязи с этапами информационной работы

8.3. Модель потенциального нарушителя

Проведя анализ статистических данных, можно сделать вывод, что около 70% всех нарушений, связанных с безопасностью информации, совершаются именно сотрудниками предприятия. Человек, кроме всего прочего, является первым по значимости носителем информации. Он обеспечивает функционирование системы, ее охрану и защиту. В то же время он, при определенных обстоятельствах, может стать главным источником угрозы защищаемой информации.

Поэтому целесообразно рассмотреть модель нарушителя, которая отражает его практические и теоретические возможности, априорные знания, время и место действия и т. п.

Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно, если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений. В каждом конкретном случае,

исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной системы.

При разработке модели нарушителя определяются:

1. Нарушитель

а) предположения о категориях лиц, к которым может принадлежать нарушитель;

б) предположения о мотивах действий нарушителя (преследуемых нарушителем целях);

в) предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);

г) ограничения и предположения о характере возможных действий нарушителей.

2. По отношению к исследуемой системе нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Внутренним нарушителем может быть лицо из следующих категорий персонала:

а) пользователи системы;

б) персонал, обслуживающий технические средства (инженеры, техники);

в) сотрудники отделов;

г) технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения);

д) сотрудники службы безопасности;

е) руководители различных уровней должностной иерархии.

3. К посторонним лицам, которые могут быть нарушителями, относятся:

а) клиенты (представители организаций, граждане);

б) посетители (приглашенные по какому-либо поводу);

в) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т. п.);

г) представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;

д) лица, случайно или умышленно нарушившие пропускной режим;

е) любые лица за пределами контролируемой территории.

4. Действия злоумышленника могут быть вызваны следующими причинами:

а) при нарушениях, вызванных безответственностью, сотрудник целенаправленно или случайно производит какие-либо действия по компрометации информации, не связанные со злым умыслом;

б) бывает, что сотрудник предприятия ради самоутверждения (для себя или коллег) затевает своего рода игру «пользователь — против системы». И хотя намерения могут быть безвредными, будет нарушена сама политика безопасности. Такой вид нарушений называется зондированием системы:

в) нарушение безопасности может быть вызвано и корыстным интересом. В этом случае сотрудник будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой на предприятии информации;

г) желание найти более перспективную работу. Известна практика переманивания специалистов, так как это позволяет ослабить конкурента и дополнительно получить информацию о предприятии. Таким образом, не обеспечив закрепление лиц, осведомленных в секретах, талантливых специалистов, невозможно в полной мере сохранить секреты предприятия. Вопросам предупреждения текучести кадров необходимо уделять особое внимание. Если рассматривать компанию как совокупность различных ресурсов, то люди

должны стоять на первом месте, т. к. именно они воплощают технологию и в них в первую очередь заключается конкурентоспособная сила фирмы;

д) специалист, работающий с конфиденциальной информацией, испытывает отрицательное психологическое воздействие, обусловленное спецификой этой деятельности. Поскольку сохранение чего-либо в тайне противоречит потребности человека в общении путем обмена информацией, сотрудник постоянно боится возможной угрозы утраты документов, содержащих секреты. Выполняя требования режима секретности, сотрудник вынужден действовать в рамках ограничения своей свободы, что может привести его к стрессам, психологическим срывам и, как следствие, к нарушению статуса информации.

Всех нарушителей можно классифицировать следующим образом.

1. По уровню знаний о системе;

а) узнает функциональные особенности, основные закономерности формирования в ней массивов данных, умеет пользоваться штатными средствами;

б) обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

в) обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;

г) знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

2. По уровню возможностей (используемым методам и средствам):

а) **«Эксперт»** — индивид, чьи профессиональные знания и контакты (как работа, так и хобби) обеспечивают первоклассную ориентацию в разрабатываемом вопросе. Он может помочь по-новому взглянуть на существующую проблему, выдать базовые материалы, вывести на неизвестные источники информации. Общая надежность получаемых при этом данных чаще всего высшая.

б) **«Внутренний информатор (осведомитель**)» — человек из группировки противника (конкурента), завербованный и поставляющий информацию по материальным, моральным и другим причинам. Ценность представляемых им данных существенно зависит от его возможностей и мотивов выдавать нужные сведения, достоверность которых при соответствующем контроле может быть довольно высокой.

в) **«Горячий информатор» —** любой знающий человек из сторонников противника или его контактеров, проговаривающий информацию под влиянием активных методов воздействия в стиле жесткого форсированного допроса, пытки, гипноза, шантажа и т. д. Так как истинность сообщения в данном случае не гарантирована, такая импровизация приемлема лишь в период острой необходимости, когда нет времени, желания или возможностей «нянчиться» с другими источниками. В отличие от завербованного информатора личностный контакт здесь главным образом одномоментен.

г) **«Внедренный источник»** — свой человек, тем или иным манером просочившийся в окружение объекта (человека, группы, организации). Ценность поставляемых им данных зависит от его индивидуальных качеств и достигнутого уровня внедрения.

д) **«Легкомысленный информатор (болтун)»** — человек противника, контактер или любое информированное лицо, проговаривающее интересные факты в деловой, дружеской, компанейской либо интимной беседе. Промелькнувшее случайно сообщение может быть необычайно ценным, хотя не исключены как беспечная ложь, так и намеренная дезинформация.

е) **«Контактеры»** — люди, когда-либо контактировавшие с изучаемым человеком (группой, организацией). Это могут быть стабильные или случайные деловые партнеры, родственники и приятели, служащие сервиса и т.д. Наряду с сообщением определенных фактов, они могут содействовать в подходе к изучаемому человеку или же участвовать в прямом изъятии у него интересующей злоумышленника информации.

ж**) «Союзник»** — человек либо общественная, государственная или криминальная структура, выступающая как противник или «надзиратель» объекта. Уровень и надежность отдаваемых материалов зависят от насущных интересов, личных взаимоотношений и познаний источника. Кроме совершенно новой, он способен передать и подтверждающую информацию.

з) **«Случайный источник»** — человек, совершенно не рассматриваемый как потенциальный информатор, вдруг оказывающийся носителем уникальной информации. Ввиду явной непредсказуемости на такого человека не особенно рассчитывают, но, случайно обнаружив, разрабатывают до конца.

По времени действия:

а) в процессе функционирования системы (во время работы компонентов системы);

б) в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерыве для обслуживания и ремонта и т. п.);

в) как в процессе функционирования, так и в период неактивности компонентов системы.

3. По месту действия:

а) без доступа на контролируемую территорию организации;

б) с контролируемой территории без доступа в здания и сооружения;

в) внутри помещений, но без доступа к техническим средствам;

г) с рабочих мест конечных пользователей (операторов);

д) с доступом в зону данных (баз данных, архивов и т.п.);

е) с доступом в зону управления средствами обеспечения безопасности.

Таким образом, рассмотрев модель потенциального нарушителя, можно сделать вывод, что человек является важным звеном системы и главным источником информации.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Защита и обработка конфиденциальных документов
2. Перечислить перечень сведений конфиденциального характера.
3. Понятие конфиденциальности. Сведения, относящиеся к конфиденциальному делопроизводству
4. Какие документы относятся к коммерческой тайне
5. Коммерческая тайна
6. Грифами ограничения доступа конфиденциального делопроизводства являются: грифы?
7. Деловая информация включает в себя?
8. Перечислить сведения, которые не могут являться коммерческой тайной
9. Защита документов содержащих коммерческую тайну
10. Уязвимость документированной информации
11. Утечка информации
12. Основная цель защиты конфиденциальной информации
13. Утрата и утечка защищаемой документированной информации
14. Уязвимость документированной информации
15. Методы оценки защищенности предприятия
16. Источники, способы и результаты дестабилизирующего воздействия на информацию
17. Оценка угроз безопасности информации
18. Явления, факторы и условия дестабилизирующего воздействия на защищаемую информацию
19. Источники дестабилизирующего воздействия на информацию
20. Виды и способы дестабилизирующего воздействия на информацию со стороны людей
21. Виды и способы дестабилизирующего воздействия на информацию со стороны технических средств, технологических процессов и природных явлений
22. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию со стороны людей
23. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию со стороны технических средств, технологических процессов и природных явлений
24. В результате чего реализовывается уязвимость документированной информации?
25. Что включает в себя обеспечение защиты конфиденциальной информации Что необходимо для обеспечения защиты документированной информации
26. Организация работы с документами, содержащими конфиденциальные сведения
27. Разрешительная система доступа к конфиденциальным документам
28. Что представляет собой разрешительная система доступа к конфиденциальным документам
29. Что предусматривает разрешительная система
30. Документооборот конфиденциальных документов
31. Что запрещается делать с документами с грифом «КТ»
32. К конфиденциальным документам относятся?

33. Назовите документы долговременного периода конфиденциальности
34. Назовите документы кратковременного периода конфиденциальности
35. Обеспечение сохранности конфиденциальной информации организации требует соблюдения следующих условий
36. Что включает в себя научно - техническая информация
37. Что включает в себя деловая информация
38. Назовите сведения, которые не являются кт
39. Как происходит защита документов, содержащих коммерческую тайну
40. Организация работы с документами, содержащими конфиденциальные сведения
41. В чем заключается система грифования?
42. Информация и документы, отнесенные к коммерческой тайне, имеют несколько уровней грифа ограничения доступа, соответствующих различным степеням конфиденциальности информации, назовите их.
43. Какие группы конфиденциальных документов образуются в различных типах организационных структур?
44. В чем состоит особенность конфиденциального документа?
45. Как классифицируются конфиденциальные документы по сроку ограничения к ним доступа персонала?
46. Что понимается под разрешительной системой доступа к конфиденциальной информации?
47. Какие этапы входят в процесс документирования конфиденциальной информации?
48. С какой целью на документе ставится гриф конфиденциальности и какие виды этих грифов используются? Чем руководствуются при определении уровня грифа конфиденциальности?
49. Какие существуют требования к организации и технологии работы с конфиденциальными документами?
50. На основе каких принципов строится защищенный документооборот? За счет чего достигается защищенность документопотоков?
51. Какие стадии включаются в состав входного документопотока?
52. Какие стадии включаются в состав выходного и внутреннего документопотоков?
53. Что понимается под технологической системой обработки и хранения конфиденциальных документов? Какие существуют типы систем?
54. Что понимается под входным потоком конфиденциальных документов?
55. Какие документы несут входной поток?
56. Какие опасности угрожают документам входного потока?
57. Какие технологические стадии обработки проходят конфиденциальные документы входного потока? Каково назначение каждой стадии?
58. В чем состоят особенности процедуры выдачи закрытых дел сотрудникам для работы?
59. Какой состав операций включает в себя процедура снятия грифа конфиденциальности с документа? Цель процедуры?
60. Постановление Правительства РФ от 6 февраля 2010 г. № 63 “Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне”.
61. Сущность и задачи комплексной системы защиты информации.
62. Понятие комплексной системы защиты информации.

63. В чем состоит сущность комплексной системы защиты информации и ее основное назначение?
64. Принципы построения комплексной системы защиты информации.
65. Цели системного подхода к защите информации.
66. Стратегии защиты информации.
67. Назвать основные три стратегии защиты.
68. Комплекс мероприятий, связанных с проведением анализа рисков.
69. Основные требования, предъявляемые к комплексной системе защиты информации.
70. Методологические основы комплексной системы защиты информации.
71. Методология защиты информации как теоретический базис комплексной системы защиты информации.
72. Что понимают под научно-методологическими основами комплексной защиты информации?
73. Основные понятия теории систем.
74. Модель структуры системы.
75. Системный анализ и системный подход.
76. Основные системные представления.
77. Определение состава защищаемой информации.
78. Методика определения состава защищаемой информации.
79. Классификация информации по видам тайны и степеням конфиденциальности.
80. Определение объектов защиты.
81. Хранилища носителей информации как объект защиты.
82. Каналы и методы несанкционированного доступа к информации.
83. Методика выявления каналов несанкционированного доступа к информации.
84. Определение возможных методов несанкционированного доступа к защищаемой информации.
85. Комплексная защита информации и персонал.
86. Кадровое обеспечение комплексной системы защиты информации.
87. Кадровая политика предприятия при создании КСЗИ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бисюков, Виктор Михайлович. Защита и обработка конфиденциальных документов [Текст] : учебное пособие : Направление подготовки 10.03.01 — Информационная безопасность : Бакалавриат / В. М. Бисюков ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования "Северо-Кавказский федеральный университет". - Ставрополь : Изд-во СКФУ, 2016. - 152 с. Текст : электронный // www.twirpx.com

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст : электронный // ЭБС Юрайт

3. Воронцовский, А. В. Управление рисками : учебник и практикум для бакалавриата и магистратуры / А. В. Воронцовский. — Москва : Издательство Юрайт, 2019. — 414 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-00945-3. — Текст : электронный // ЭБС Юрайт

4. Жуковский, В. И. Оценка рисков и гарантии в конфликтах : учеб. пособие для вузов / В. И. Жуковский, М. Е. Салуквадзе. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 364 с. — (Серия : Авторский учебник). — ISBN 978-5-534-08606-5.

5. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6 -Текст: электронный //znanium.com[сайт]

6. Конфиденциальное делопроизводство : учеб. пособие / Т.А. Гугуева. — 2-е изд., перераб. и доп. — М. : ИНФРА-М, 2017. — 199 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/23514. - Режим доступа: http://znanium.com/catalog/product/766722

7. Конфиденциальное делопроизводство: Учебное пособие / Т.А. Гугуева. - М.: Альфа-М: НИЦ Инфра-М, 2012. - 192 с.: 60x90 1/16. - (Технологический сервис). (переплет) ISBN 978-5-98281-293-3 - Режим доступа: http://znanium.com/catalog/product/265483

8. Кузнецов, И. Н. Документационное обеспечение управления. Документооборот и делопроизводство : учебник и практикум для среднего профессионального образования / И. Н. Кузнецов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 462 с. — (Профессиональное образование). — ISBN 978-5-534-04604-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433861 (дата обращения: 06.07.2019).

9. Лось В.П. Основы информационной безопасности: учебное пособие для вузов/Е.Б. Белов и др. –М.: Гор. Линия-Телеком,2014-558 с.:60x88 1/16.- (Специальность;Учебное пособие для выших учебных заведений).(0) ISBN 5-93517-292-5, 100 экз. Текст : электронный // Электронная библиотечная система «Лань»

10. Методические указания к теоретическим, практическим и лабораторным занятиям по дисциплине «Защита и обработка конфиденциальных документов» для студентов специальности 10.03.01 «Информационная безопасность» очной формы обучения». / Сост. Маслова М.А. – СГУ. – Севастополь.

11. Методические указания к теоретическим, практическим и лабораторным занятиям по дисциплине «Основы управления информационной безопасностью» для студентов специальности 10.03.01 «Информационная безопасность» очной формы обучения». / Сост. Маслова М.А. – СГУ. – Севастополь.

12. Мещеряков Р.В. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - М.: Гор. линия-Телеком, 2012. - 442с.; 60х90 1/16 - (Уч. для вузов). (о) ISBN 978-5-9912-0233-6. Текст: электронный //znanium.com[сайт]

13. Нестеров С.А. Основы информационной безопасности[учебное пособие]: С.А. Нестеров; М-во образования и науки Российской Федерации ,Санкт-Петербург: Изд-во Политехнического ун-та,2017.-324 с.: ил., табл.,табл.;20см.;ISBN 978-5-8114-2290-6. Текст : электронный // Электронная библиотечная система «Лань»

14. Основы информационной безопасности : учебник/ Е.К. Баранова, А.В. Бабаш. - М. : РИОР : ИНФРА-М, 2019. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4 - Текст: электронный //znanium.com[сайт]

15. Петров А.А. Компьютерная безопасность. Криптографические методы защиты: учебное пособие. Бакалавриат. - Москва : Издательство "ДМК Пресс", 2014. - 448 с.; см Текст : электронный // Электронная библиотечная система «Лань»

16. Попова Л. Г. Концепция системного математического моделирования информационной безопасности [Интернет-журнал "Науковедение", Вып. 2 (21), 2014, Текст: электронный //znanium.com[сайт]

17. Северцев, Н. А. Введение в безопасность : учебное пособие для академического бакалавриата / Н. А. Северцев, А. В. Бецков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 177 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-05710-2. — Текст : электронный // ЭБС Юрайт

18. Северцев, Н. А. Введение в безопасность : учебное пособие для академического бакалавриата / Н. А. Северцев, А. В. Бецков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 177 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-05710-2. — Текст : электронный // ЭБС Юрайт

19. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учеб. пособие / Ю.Н. Сычев. — М. : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - Режим доступа: http://znanium.com/catalog/product/979415

20. Теплов Э.П., Гатчин Ю.А., Нырков А.П., Коробейников А.Г. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции [учебное пособие]: Теплов Э.П.; Автономная некоммерческая орг. высш. проф. Образования "Белгородский ун-т кооп., экономики и права". - Санкт-Петербург : Изд-во Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2016. - 122 с. : ил., табл.; 21 см. Текст : электронный // Электронная библиотечная система «Лань»

21. Тимошенков, С. П. Надежность технических систем и техногенный риск : учебник и практикум для бакалавриата и магистратуры / С. П. Тимошенков, Б. М. Симонов, В. Н. Горошко. — Москва : Издательство Юрайт, 2019. — 502 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-9916-8582-5. — Текст : электронный // ЭБС Юрайт [сайт].

22. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях : [Электронный ресурс] : учебное пособие для студентов высших учебных заведений; под ред. И. Г. Акперова. - 3-е изд., стер. - Москва : Издательство "ДМК Пресс", 2014. – 592 с.; ISBN 978-5-94074-637-9. Текст : электронный // Электронная библиотечная система «Лань».

У ч е б н о е и з д а н и е

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие

Составители: **Маслова** Мария Александровна,
Ожиганова Марина Ивановна

В авторской редакции

Изд. № 131/2020. Объем 6,25 п.л.
РИИЦМ ФГАОУ ВО «Севастопольский государственный университет»