Содержание:

ВВЕДЕНИЕ

Основная черта постиндустриального общества заключается в том, что наибольшую ценность составляют не материальные объекты, а информация. Исходя из этого, совершенно естественным видится стремление человека оградить собственную информационную среду от дестабилизирующего воздействия. Именно эту цель и ставит перед собой организация защиты информации.

В настоящее время расширяется разнообразие подлежащей защите информации. Если в 1993 г. в России существовал закон, рассматривающий только один вид тайны (а именно – государственную тайну), то уже в 2004 году принят закон о коммерческой тайне, в 2006 году – о персональных данных. На сегодняшний день защите подлежит и информация, относящаяся к служебной, профессиональной и личной тайнам, а также так называемая инсайдерская информация.

К тому же защита информации становится все более актуальной в связи с высоким уровнем технологического прогресса: постоянно появляются новые и совершенствуются уже существующие носители информации, виды, методы и средства их защиты, а это естественным образом влечет за собой усовершенствование и усложнение средств противодействия защите.

К важнейшим мероприятиям защиты информации относятся выявление и анализ угроз защищаемой информации, так как именно они определяют, какой вид должна будет иметь комплексная система защиты информации, на чем следует делать наибольший акцент и прилагать больше усилий. Нужно помнить, что защита информации должна быть финансово обоснована, т.е. затраты на ее организацию не должны превышать цену самой защищаемой информации. Анализ угроз помогает сформировать именно такую систему защиты.

Оценка угроз защищаемой информации, в большинстве случаев, является вторым этапом проектирования комплексной защиты объекта информатизации. Ей предшествует обследование объекта информатизации и оценка состава и категорий защищаемой информации. В общем случае оценка угроз защищаемой информации и системам её обработки представляет собой анализ возможных проявлений уязвимостей, ущерба, а также контрмер. Также необходимы к

рассмотрению все составляющие структуры угроз.

Целью данной работы является рассмотрение и анализ возможных угроз защищаемой информации.

Поставленная цель раскрывается через следующие задачи:

1. формулирование понятия угрозы защищаемой информации;
2. рассмотрение структуры угроз, то есть определение ее составляющих;
3. характеристика составных частей угроз защищаемой информации.

В литературе данный вопрос достаточно широко освещен. Темы характеристики угроз защищаемой информации в своих работах касались такие авторы, как: Алексенцев А.И, Герасименко В.А., Гришина Н.В., Ищейнов В.Я., Мецатунян М.В., Торокин А.А. и многие другие.

При рассмотрении данного вопроса с законодательной точки зрения весьма полезными являются следующие источники: Федеральный закон «Об информации, информационных технологиях и защите информации», «Закон о безопасности», «Доктрина информационной безопасности», а также гост «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

1. ПОНЯТИЕ УГРОЗЫ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ И СПОСОБЫ ЕЕ КЛАССИФИКАЦИ

Существует несколько подходов к определению понятия угрозы защищаемой информации. Рассмотрим некоторые из них и сформулируем оптимальное, наиболее полное по смыслу и лаконичное по объему определение.

1. Угроза защищаемой информации – совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.[1]
2. Угроза конфиденциальной информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.[2]
3. Угроза защищаемой информации – явление или событие, следствием которого может быть нежелательное воздействие на информацию.

4. Угроза защищаемой информации – это потенциально существующая ситуация нарушения статуса защищенности.

Здесь рассматривается именно термин «угроза защищаемой информации», а не «угроза безопасности информации», так как безопасность информации – это состояние защищенности информации от воздействий, нарушающих ее статус. Следовательно, безопасность информации означает, что информация уже находится в таком защищенном виде, который способен противостоять любым дестабилизирующим воздействиям, и понятие угрозы применительно именно к защищаемой информации.

В определении №2 понятие «конфиденциальная информация» используется авторами как конкретный вид общего понятия защищаемой информации.

В рассмотренных определениях можно выделить две составляющие. Во-первых, это содержательная (определяющая) часть. Угроза – это некое явление, событие, ситуация, условие, фактор или совокупность некоторых данных компонентов. Во-вторых, существует функциональная (или результативная) составляющая, которая является конечным итогом определяющей части. Функциональная составляющая непосредственно указывает на нарушение состояния защищенности, то есть на виды уязвимости информации: утрату или утечку.

В рассматриваемом понятии также должны быть различимы три компонента: объект, субъект и действие, производимое субъектом над объектом. В противном случае, если один из этих пунктов не будет учтен, не придется говорить об угрозе как таковой.

Под объектом будем понимать саму защищаемую информацию. Нужно также отметить, что о безопасности данного объекта целесообразно говорить в том случае, если с помощью него или над ним совершаются какие-либо действия. В противном случае объект бездействует и интереса не представляет. Следовательно, необходимо рассматривать объект при условии его функционирования с внешней средой.

Под субъектом в рамках рассматриваемого определения подразумеваются источники угроз, порождающие явления, условия и факторы, при которых действие над объектом (преднамеренное или случайное) будет возможным.

И, наконец, под действием над объектом будем понимать дестабилизирующее воздействие, приводящее к нарушению состояния защищенности информации.

Обобщая все вышесказанное, сформулируем собственное определение угрозы защищаемой информации:

Угроза защищаемой информации – это совокупность явлений, условий и факторов, создающих опасность случайного или преднамеренного нарушения состояния защищенности информации.

К факторам, кроме причин и обстоятельств, следует также относить и существование каналов несанкционированного доступа к защищаемой информации и методов их реализации для воздействия на информацию лиц, не имеющих к ней законного доступа.

Классификация угроз может производиться по разным признакам. Например, по признакам отношения к природе возникновения подразделяют на классы объективные и субъективные, по отношению к объекту информатизации – на внутренние и внешние.[3]

В зависимости от конкретно поставленной задачи можно провести разделение угроз по факту возникновения, по виду нарушения, по объекту воздействия, по деструктивному воздействию, по способу реализации. Перечисленные классы могут подразделяться на соответствующие подклассы, группы, подгруппы, виды и подвиды. В данной работе рассмотрим только разделение на подклассы без дальнейшей, более тщательной классификации. Это достаточно отображает разнообразие как

самих угроз, так и методов и способов их реализации.

1. По факту возникновения подразделяют угрозы:

а) природные

б) техногенные

в) антропогенные

2. По виду нарушения подразделяют угрозы:

а) непосредственно конфиденциальности

б) целостности системного программного обеспечения

в) доступности программных средств защиты информации

3. По объекту воздействия подразделяют угрозы:

а) информации в базах данных

б) информации в составе файловой системы

в) системным программным компонентам

г) аппаратным компонентам

д) персоналу

4. По деструктивному воздействию подразделяют угрозы:

а) модификации

б) блокирования

в) хищения

г) уничтожения

д) разглашения

5. По способу реализации подразделяют угрозы:

а) с использованием технических средств перехвата информации

б) без использования технических средств перехвата информации[4]

Также важно отметить, что по источникам злонамеренного воздействия рассматриваются угрозы внутренние, которые определяются социальным и моральным климатом внутри какой-либо организации, состоянием технического и программного обеспечения, и внешние, которые характеризуются дестабилизирующим воздействием конкурентов, злоумышленников, экономическими условиями, стихийными бедствиями и т.п., то есть всем тем, что находится вне зоны контроля конкретной организации или предприятия.

Защита информации главным образом направлена на предотвращение проявление уязвимости, которое выражается в различных формах, как то: хищение носителей информации или информации, в нем отображенной, потеря носителя информации, несанкционированное уничтожение носителя или информации, в нем отображенной, несанкционированная модификация информации, ее блокирование

или разглашение. Перечисленные формы проявления уязвимости выражают результаты дестабилизирующего воздействия, в то время как в конечном счете они приводят к утрате или к утечке информации.

Для проявления уязвимости необходимо наличие источника дестабилизирующего воздействия на информацию. В свою очередь, эта деятельность возможна при существовании определенных причин.

Например, основной причиной дестабилизирующего воздействия на информацию со стороны такого источника, как человек, является стремление получить материальную выгоду. Причины могут быть реализованы в определенных условиях, которые стимулируют их возникновение и проявление. В рассматриваемом нами примере одним из условий может быть недостаточность мер, предпринятых для защиты информации со стороны ее легального обладателя. Дестабилизирующее воздействие на информацию реализуется различными видами, методами и способами при помощи использования каналов несанкционированного доступа к информации, то есть тех путей, посредством которых нелегальный доступ к защищаемой информации становится возможным.

Таким образом, структура угроз является следующей:

1. Источники угроз
2. Причины
3. Условия
4. Каналы и методы несанкционированного доступа к информации
5. Виды, методы и способы дестабилизирующего воздействия на информацию

Таким образом, угрозы могут существовать как таковые именно из-за такого свойства информации, как уязвимость. Что касается самой структуры угроз, то ее главным компонентом являются источники угроз, так как они по каким-либо существующим причинам и благодаря тем или иным условиям определяют наличие в информационной среде каналов и методов несанкционированного доступа к информации, а также виды, методы и способы дестабилизирующего воздействия на информацию. Именно источники угроз определяют, каков будет конечный результат воздействия. Состав других структурных частей угрозы также играет немаловажную роль, но определяющего характера он не носит, а скорее является следствием состава источников угроз.

Следует еще раз отметить, что угроза защищаемой информации подразумевает под собой три определяющих компонента: субъект, объект и действие субъекта на

объект. Поэтому основная важность приписывается субъекту, то есть источнику угрозы, в том случае, если он осуществляет то или иное воздействие на воздействие на защищаемую информацию. Если не происходит воздействие, то и угрозы не существует как таковой.

2. ОБЩАЯ ХАРАКТЕРИСТИКА УГРОЗ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Чтобы более полно охарактеризовать угрозы защищаемой информации, в данной работе будем отправным пунктом характеристики считать непосредственно источники угроз, для каждого из которых определим причины, условия, каналы и методы несанкционированного доступа к информации, а также некоторые виды, методы и способы дестабилизирующего воздействия на информацию.

В Доктрине информационной безопасности Российской Федерации источники угроз подразделяются на две большие группы: внешние и внутренние.[1] В рамках каждой группы рассматриваются несколько пунктов применительно к информационной безопасности России. Было бы возможным рассмотреть каждый из них и сопоставить с соответствующими причинами и условиями дестабилизирующего воздействия на информацию, придавая перечисленным угрозам более общий характер, то есть относительно не только информационной безопасности государства, но также и различных предприятий или компаний.

Тем не менее, в данной работе более удобной видится классификация источников угроз защищаемой информации, представленная в работе Н.В.Гришиной.[2] Она выглядит следующим образом:

1. Люди;
2. Технические средства отображения (фиксации), хранения, обработки,

[1] Доктрина информационной безопасности Российской Федерации, (утверждена Президентом Российской Федерации В.В.Путиным и принята Советом безопасности Российской Федерации 12 сентября 2000 г.), СПС «КонсультантПлюс».

[2] Гришина Н.В. Организация комплексной системы защиты информации – М.: «Гелиос АРВ», 2007. – с. 75

воспроизведения, передачи информации, средства связи;

1. Системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации;
2. Технологические процессы отдельных категорий промышленных объектов;
3. Природные явления.

Рассмотрим более подробно каждый пункт.

Люди являются самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию. Распространенность этого источника угроз объясняется тем, что неблагоприятное воздействие может оказываться как со стороны людей, имеющих санкционированный доступ к защищаемой информации (таковыми являются непосредственно сотрудники организации или лица, не работающие на предприятии, но имеющие доступ в силу своего служебного положения), так и со стороны людей, его не имеющих (лица из криминальных структур, хакеры). Многообразность этого источника обусловлена большим количеством видов дестабилизирующего воздействия. Существует две группы этих видов: преднамеренное или непреднамеренное воздействие и непосредственное или опосредованное (подразумевающее использование других источников). Наибольшая же степень опасности приписывается этому источнику по причине большого количества возможных методов и способов дестабилизирующего воздействия.

Основной причиной преднамеренного воздействия со стороны людей является желание получить материальную выгоду. Также человек (или группа лиц) может стремиться нанести вред руководству, коллегам, государству или показать значимость своей персоны. Возможны и случаи, когда человек (либо его родные, близкие) подвергается шантажу, физическому или моральному неблаготворному воздействию и единственным способом избавления от шантажиста ему видится выполнение требований злоумышленника, которые в данном случае подразумевают какое-либо дестабилизирующее воздействие на информацию. Воздействие является преднамеренным, но опосредованным, так как непосредственным источником угроз является шантажист. Аналогичная классификация применяется и в случае, когда человек из дружеских чувств оказывает безвозмездную услугу представителю конкурирующей фирмы.

Обстоятельствами, способствующими появлению причин преднамеренного воздействия со стороны людей, являются тяжелое материальное положение, финансовые затруднения, недовольство служебным положением, политическое

или научное инакомыслие, а также такие морально-нравственные характеристики, как корыстолюбие и алчность, завистливость, тщеславие, самомнение, склонность к развлечениям и употреблению наркотических веществ. В приведенном примере шантажа обстоятельствами являются страх и трусость, а в случае безвозмездной услуги представителю конкурирующей фирмы – личные связи с данным представителем.

Для предотвращения данных воздействий руководителю предприятия или другим уполномоченным лицам кадровой службы следует особое внимание уделить морально-нравственному портрету сотрудников, который может быть выявлен в ходе собеседования при приеме на работу, посредством изучения досье или же в процессе выполнения лицом своих обязанностей. В тех же целях (в том числе) некоторыми организациями используются проверки на полиграфах. Результаты некоторых медицинских анализов помогут обнаружить наличие вредных привычек или факт употребления наркотиков.

К условиям, создающим возможность преднамеренного дестабилизирующего воздействия, относятся, прежде всего, недостаточность мер, принятых для защиты безопасности и низкий уровень контроля реализации процессов, происходящих с защищаемой информацией. Негативные последствия также будут иметь поспешные, необдуманные решения производственных вопросов без учета требований по защите информации. К тому же, плохие и недоброжелательные отношения между сотрудниками, сотрудниками и администрацией тоже являются данными условиями.

Необходимыми мерами предосторожности в данных случаях будут являться грамотно организованная система защиты информации и выполнение ее требований, а также контроль благоприятного морального климата на предприятии.

Непреднамеренное воздействие в большинстве случаев происходит по причине недостаточной квалификации работников, халатности, безответственности, небрежности или по причине физического недомогания, плохого самочувствия.

К обстоятельствам, способствующим появлению причин непреднамеренного воздействия со стороны людей, относятся низкий уровень профессиональной подготовки, физические болезни и недуги, незаинтересованность в качественном выполнении обязанностей, большой объем работы и срочность ее выполнения, легкомыслие, плохое отношение со стороны администрации.

Для предотвращения перечисленных обстоятельств руководство предприятия должно позаботиться о создании благоприятных условий работы сотрудников (правильное соотношение объема работы и сроков выполнения, соблюдение режима работы) и стимулов к профессиональному совершенствованию (выплата премий, возможность карьерного роста). Также следует регулярно производить тестирования на профессиональную пригодность, медицинские обследования и использовать методы для определения морально-нравственного облика сотрудников, указанные выше.

Условиями реализации непреднамеренного дестабилизирующего воздействия являются отсутствие или низкое качество правил работы с защищаемой информацией, незнание исполнителями данных правил, недостаточный контроль со стороны администрации за соблюдением режима конфиденциальности, недостаточное внимание к условиям работы, уровню профессиональной подготовки, повышению квалификации, профилактике заболеваний.

Как и в случае преднамеренного дестабилизирующего воздействия, эти условия можно нейтрализовать, организовав соответствующую систему защиты информации, выполнять ее требования. Зачастую на предприятиях для планирования организации контроля и совершенствования системы защиты информации создается служба безопасности. Основными ее задачами являются:

- мониторинг угроз защищаемой информации;
- организация работы по защите информации на предприятии;
- управление доступом сотрудников, автотранспорта и посетителей на территорию и в помещения организации;
- обеспечение безопасности информации при проведении всех видов деятельности внутри и вне предприятия, в том числе при чрезвычайных ситуациях;
- формирование у работников организации устойчивого понимания необходимости выполнения норм защиты информации;
- охрана территории, зданий, помещений и других мест и конструкций с защищаемой информацией.[5]

Теперь же перейдем к рассмотрению сразу нескольких источников угроз, к которым относятся: системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации; технологические процессы отдельных категорий промышленных объектов; технические средства отображения (фиксации), хранения, обработки,

воспроизведения, передачи информации, средства связи.

К системам обеспечения функционирования технических средств отображения, хранения, обработки и передачи информации относятся системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования.

Технологические процессы отдельных категорий промышленных объектов включают в себя процессы, связанные с ядерной энергетикой, химической промышленностью, радиоэлектроникой, изготовлением некоторых видов вооружений и военной техники. Все эти процессы изменяют естественную структуру среды, окружающей объект.

Технические средства отображения, хранения, обработки, воспроизведения, передачи информации и средства связи очень многообразны в силу высокого уровня технологического развития. К этим средствам можно отнести электронно-вычислительную технику, копировально-множительную технику, средства видео- и звукозаписывающей и воспроизводящей техники, средства телефонной, факсимильной, громкоговорящей передачи информации, средства радиовещания и телевидения, радио, кабельной и беспроводной связи и т.п.

Причины, обстоятельства и условия дестабилизирующего воздействия со стороны этих источников угроз не рассматриваются отдельно относительно каждого источника, так как они имеют общий характер.

Сразу отметим, что данные источники оказывают дестабилизирующее воздействие на информацию всегда непреднамеренно, так как у них отсутствуют цели по изменению, уничтожению, хищению и блокированию информации.

К причинам дестабилизирующего воздействия со стороны источников, перечисленных выше, относятся недостаток или низкое качество средств функционирования, перезагруженность этих средств, низкое качество технологии выполнения работ, а также дестабилизирующее воздействие со стороны других источников, в особенности – людей.

Обстоятельствами, вызывающими причины дестабилизирующего воздействия, являются низкий уровень финансирования ресурсов, неправильный выбор средств функционирования, износ данных средств, конструктивные недоработки или ошибки при монтаже средств, ошибки при разработке технологии выполнения работ, в том числе программного обеспечения, дефекты используемых материалов, чрезмерный объем обрабатываемой информации. Также сюда относятся причины

преднамеренного и непреднамеренного дестабилизирующего воздействия со стороны людей.

К условиям дестабилизирующего воздействия со стороны перечисленных источников относятся недостаточное внимание к составу и качеству средств со стороны администрации или других ответственных лиц, нерегулярность профилактических проверок средств функционирования, низкое качество обслуживания этих средств.

Нелишним будет заметить, что по мере совершенствования и усложнения систем обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации, технологических процессов отдельных категорий промышленных объектов, технических средств отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средств связи возрастает также и количество ошибок, неисправностей. Скрытые дефекты, медленно протекающие химические процессы в местах контакта и другие негативные факторы все чаще проявляются с ростом сложности электротехнических, электронных средств. Даже если предпринимаются достаточно серьезные меры по обеспечению их надежности, выявить все скрытые дефекты невозможно.[6]

Также проблема усложняется еще тем обстоятельством, что ошибки в электротехнических, электронных сетях зачастую не могут быть выявлены оперативно и непосредственно, а только лишь благодаря сбоям, являющимися следствием неисправности. Например, неисправность систем охлаждения компьютера обычно выявляется на довольно поздней стадии, когда становятся явно заметными различные неисправности в ходе работы: снижение скорости обработки, отображения информации, неестественные звуки, издаваемые системным блоком. Поломка средств кондиционирования в данном случае может привести к частичному или полному выходу из строя любой составляющей компьютера. В итоге, данная неисправность может повлечь за собой изменение, уничтожение и блокирование информации. То же касается и программного обеспечения. В процессе написания программы могут быть допущены ошибки, устранение которых впоследствии будет достаточно трудоемким. После того, как было начато использование программы, содержащей ошибку, исходные неисправности повлекут за собой цепь других, и задача устранения неполадок усложняется во много раз.

К тому же, зачастую исправление ошибки в уже рабочей программе может привести к еще большему увеличению ошибок во всем алгоритме. Все это приводит к проявлению уязвимости информации. Поэтому еще на стадии разработки следует крайне внимательно подойти к этому вопросу.

Теперь же обратимся к последнему из обозначенных нами источников угроз защищаемой информации – природным явлениям. Под ними подразумеваются стихийные бедствия, атмосферные явления. Очевидно, что воздействие может быть только непреднамеренным.

Причины и обстоятельства дестабилизирующего воздействия со стороны этого источника угроз являются неподконтрольными со стороны людей, следовательно, не подлежат полному предотвращению или нейтрализации.

Среди стихийных сил, которые могут в случае возникновения оказать воздействие на носитель информации, одну из наибольших угроз составляет пожар. Он происходит наиболее часто и способен полностью уничтожить носители информации без возможности восстановления данных. Также при процессе тушения пожара носители подвергаются воздействиям воды или пены, что является не менее разрушительным.

Пожар – неконтролируемое горение, причиняющее материальный ущерб, вред жизни и здоровью граждан, интересам общества и государства.[7] Для возникновения пожара необходимо наличие горючей среды (различные горюющие элементы), источника зажигания (горящие или накаленные тела, электрические разряды) и окислителя (кислород в воздухе).

Важно также отметить, что источниками угроз пожара или каких-либо механических разрушений могут быть не только природные явления, но и халатные действия со стороны людей (отсутствие своевременно ремонта зданий, технических средств хранения и обработки информации и систем обеспечения их функционирования). Например, наиболее частой причиной пожара в здании является короткое замыкание между проводами электропроводки, которое возникает из-за того, что своевременно не была заменена устаревшая изоляция проводов. Таким образом, можно еще раз убедиться в том, что человек является самым распространенным, многообразным и опасным источником угроз защищаемой информации.

ЗАКЛЮЧЕНИЕ

Угроза защищаемой информации – это совокупность явлений, условий и факторов, создающих опасность случайного или преднамеренного нарушения состояния защищенности информации.

В ходе данной работы была обозначена структура угрозы защищаемой информации, в которую входят:

1. источники угроз;
2. причины;
3. условия;
4. каналы и методы несанкционированного доступа к информации;
5. виды, методы и способы дестабилизирующего воздействия на информацию.

Реализация угроз приводит к проявлению форм уязвимости, и защита информации, в конечном счете, сводится именно к предотвращению данных проявлений или к нейтрализации угроз.

Было установлено, что главным компонентом данной структуры являются именно источники угроз, так как они определяют все остальные пункты структуры. Именно поэтому одной из важнейших задач защиты информации является анализ существующих или потенциальных источников угроз.

Чтобы более подробно рассмотреть сами источники угроз защищаемой информации, была проведена их классификация, которая выглядит следующим образом:

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.

Люди являются самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию. Причины, обстоятельства и условия этого воздействия относительно людей следует рассматривать, исходя из классификации преднамеренного и непреднамеренного

воздействия. Подводя итог, следует отметить, что для предотвращения преднамеренного воздействия особое внимание руководителю предприятия (или иному уполномоченному лицу) следует уделять морально-нравственному портрету человека и организации комплексной системы защиты информации. В случае же непреднамеренного воздействия ключевыми пунктами являются уровень квалификации сотрудников, состояние здоровья и наличие хорошо разработанных правил работы с защищаемой информацией. Это еще раз подтверждает, что в процессе защиты информации должны быть задействованы все лица, работающие с защищаемой информацией, но ответственность за саму организацию защиты несет руководитель или заведующий службой безопасности.

Также и для остальных источников угроз (кроме природных явлений) были рассмотрены причины, обстоятельства и условия дестабилизирующего воздействия на информацию. В конечном счете, основное внимание следует уделить качеству как самих средств обеспечения функционирования информационных процессов, так и к их обслуживанию, профилактическим проверкам.

Что касается такого источника угроз, как природные явления, то в данном случае возможно лишь минимизировать потери от урона (например, посредством технических средств), но никак не устранить или нейтрализовать данный источник.

В конечном счете, классификация и характеристика источников угроз защищаемой информации является неотъемлемой частью процесса защиты информации. Анализ источников угроз должен производиться на каждом предприятии. Пример такого анализа, а также некоторые меры по обеспечению информационной безопасности, и были представлены. Таким образом, цель данной работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алексенцев А.И. Защита Информации. Словарь базовых терминов и определений – М.: РГГУ, 2000.
2. Алексенцев А.И. Понятие и структура угроз защищаемой информации. – «Безопасность информационных технологий», №3, 2000.
3. Андрианов В.В. Технология защиты в принципах организация информационных систем. //Защита информации. «Конфидент». №3, 2005.
4. Галатенко В.А. Информационная безопасность. – М.: «Финансы и статистика», 2007.

5. Герасименко В.А. Защита информации в автоматизированных системах обработки данных кн. 1. – М.: «Энергоатомиздат», 1994
6. Гришина Н.В. Организация комплексной системы защиты информации – М.: «Гелиос АРВ», 2007.
7. Мельников В.П. Информационная безопасность и защита информации: учебное пособие. – М.: «Академия», 2008.
8. Мецатунян М.В., Ищейнов В.Я. Защита конфиденциальной информации. – М.: «Форум», 2009.
9. Торокин А.А. Инженерно-техническая защита информации – М.: «Гелиос АРВ», 2005.
10. Шелупанов А.А., Мещеряков Р.В., Белов Е.Б., Лось В.П. Основы информационной безопасности. Учебное пособие для вузов. – М.: «Горячая линия-Телеком», 2006.
11. Ярочкин В.И. Информационная безопасность. – М.: «Академический проект», 2008.
12. Федеральный закон от 21.12.1994 № 69-ФЗ (ред. от 30.11.2011) «О пожарной безопасности» (с изм. и доп., вступающими в силу с 01.01.2012). СПС «КонсультантПлюс».
13. Гост Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. СПС «КонсультантПлюс»
14. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2011) «Об информации, информационных технологиях и о защите информации». СПС «КонсультантПлюс».
15. Доктрина информационной безопасности Российской Федерации, (утверждена Президентом Российской Федерации В.В.Путиным и принята Советом безопасности Российской Федерации 12 сентября 2000 г.). СПС «КонсультантПлюс».
16. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности». СПС «КонсультантПлюс».
17. Федеральный закон от 21.12.1994 № 69-ФЗ (ред. от 30.11.2011) «О пожарной безопасности» (с изм. и доп., вступающими в силу с 01.01.2012). СПС «КонсультантПлюс»
18. http://inf-bez.ru/
19. http://it-ideas74.ru/

1. Алексенцев А.И. Защита Информации. Словарь базовых терминов и определений – М.: РГГУ, 2000. – с. 16 ↑

2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации – М.: Форум, 2009. – с.160 ↑

3. Гост Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. СПС «КонсультантПлюс» ↑

4. см. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации – М.: Форум, 2009. – с.163 ↑

5. см. Торокин А.А. Инженерно-техническая защита информации – М.: «Гелиос АРВ», 2005. – с. 737 ↑

6. Торокин А.А. Инженерно-техническая защита информации – М.: «Гелиос АРВ», 2005. – с. 120 ↑

7. Федеральный закон от 21.12.1994 N 69-ФЗ (ред. от 30.11.2011) "О пожарной безопасности" (с изм. и доп., вступающими в силу с 01.01.2012). СПС «КонсультантПлюс» ↑