Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«Воронежский государственный лесотехнический университет

имени Г.Ф. Морозова»

Кафедра Вычислительной техники и информационных систем

(название кафедры)

**Пояснительная записка**

КУРСОВОЙ РАБОТЫ

(вид работы)

Виды угроз безопасности экономических информационных систем.

Вариант № 19

(тема)

09.03.02 Информационные системы и технологии

(код и наименование направления подготовки)

По дисциплине Теория информационных процессов и систем

|  |  |  |
| --- | --- | --- |
| Студент группы ИС2-191-ОБ  (номер группы)  Руководитель, доцент  (ученая степень, ученое звание) | \_\_\_\_\_\_\_\_\_\_  (подпись)  \_\_\_\_\_\_\_\_\_\_  (подпись) | Бунеев И.А.  (инициалы и фамилия)  В.Г. Горбунов  (инициалы и фамилия) |

Воронеж 2021

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный лесотехнический университет   
имени Г.Ф. Морозова»

Кафедра Вычислительной техники и информационных систем

**З А Д А Н И Е**

на курсовую работу по дисциплине

«Теория информационных процессов и систем»

Студенту 3 курса гр. ИС2-191-ОБ Бунееву И.А.

(Фамилия И.О.)

09.03.02 Информационные системы и технологии

Срок представления к защите «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

**Тема работы:** Виды угроз безопасности экономических информационных систем

Вариант №19

**Исходные данные для проектирования:** написать краткий обзор исторических предпосылок возникновения задач теории систем данного направления, современного состояния теории и практики решения этого типа задач, перечислить характерные разновидности задач этого типа.

**Перечень вопросов, подлежащих разработке:**

Определение понятия "угроза безопасности".

Классификация возможных угроз безопасности экономических информационных систем.

Методы, средства и организация системы защиты информации в экономических информационных системах.

Руководитель, доцент \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ В.Г. Горбунов

Задание принял студент \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ Бунеев И.А.

(подпись) (число, месяц, год) (инициалы и фамилия)

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 4](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928700)

[1.Определение понятия "угроза безопасности" 6](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928701)

[2.Классификация возможных угроз безопасности экономических информационных систем 7](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928702)

[3. Методы, средства и организация системы защиты информации в экономических информационных системах 14](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928705)

[3.1 Правовые основы обеспечения информационной безопасности 14](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928703)

[3.2 Основные методы и средства защиты информации в АИТ 16](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928703)

[3.3 Механизмы криптографии 24](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928703)

[3.4 Шифрование как основной метод защиты информации 25](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928703)

[ЗАКЛЮЧЕНИЕ 29](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928709)

[СПИСОК ЛИТЕРАТУРЫ 31](file:///C:\Users\brosl\Downloads\уд.docx#_Toc72928710)

ВВЕДЕНИЕ

Данная работа посвящена исследованиям, лежащим в области информационной безопасности и касается изучения безопасности экономических информационных систем.

Актуальность проблемы защиты информации связана с ростом возможностей вычислительной техники. Развитие средств, методов и форм автоматизации процессов обработки информации, массовость применения ПЭBM резко повышают уязвимость информации.

Потребность в обеспечении безопасности связана с тем, что существует множество субъектов и структур, весьма заинтересованных в чужой информации и готовых заплатить за это высокую цену. А ведь существуют и, соответственно, приобретаются устройства для несанкционированного доступа к информации и по другим каналам.

Данная тема является актуальной, так как защита информации в автоматизированных информационных технологиях имеет очень важное значение.

Целью данной работы является обоснование необходимости защиты информации в автоматизированных информационных технологиях, подробный анализ организации системы защиты информации в экономических информационных системах и ее эффективности.  
  
Для осуществления обозначенной цели служат следующие задачи:  
  
-изучить теоретические аспекты защиты информации в экономических информационных системах;  
-исследовать определение понятия угрозы информационной безопасности в экономических информационных системах;  
-рассмотреть основные способы реализации угроз;

-привести вариант их классификации, проанализировать современные методы и средства защиты информации в экономических информационных системах и оценить их эффективность, а также рассмотреть основные принципы и этапы создания системы защиты информации экономических систем.

Объект исследования – информация, используемая в АИТ.  
  
Предмет исследования – информационная безопасность АИТ.  
  
Методологической основой для исследования послужили научные труды известных отечественных и зарубежных педагогов. В качестве теоретической базы исследования были использованы публикации, посвящённые информационной безопасности.

1. Определение понятия "угроза безопасности".

Развитие новых информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность не только становится обязательной, она еще и одна из характеристик ИС. Существует довольно обширный класс систем обработки информации, при разработке которых фактор безопасности играет первостепенную роль (например, банковские информационные системы).

Под *безопасностью ИС*понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов. Иначе говоря, это способность противодействовать различным возмущающим воздействиям на ИС.

Под *угрозой безопасности информации*понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Если исходить из классического рассмотрения кибернетической модели любой управляемой системы, возмущающие воздействия на нее могут носить случайный характер. Поэтому среди угроз безопасности информации следует выделять как один из видов угрозы *случайные,*или *непреднамеренные.*Их источником могут быть выход из строя аппаратных средств, неправильные действия работников ИС или ее пользователей, непреднамеренные ошибки в программном обеспечении и т.д. Такие угрозы тоже следует держать во внимании, так как ущерб от них может быть значительным. Однако в данной главе наибольшее внимание уделяется угрозам *умышленным,*которые, в отличие от случайных, преследуют цель нанесения ущерба управляемой системе или пользователям. Это делается нередко ради получения личной выгоды.

Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют взломщиком, а иногда «компьютерным пиратом» (хакером).

В своих противоправных действиях, направленных на овладение чужими секретами, взломщики стремятся найти такие источники конфиденциальной информации, которые бы давали им наиболее достоверную информацию в максимальных объемах с минимальными затратами на ее получение. С помощью различного рода уловок и множества приемов и средств подбираются пути и подходы к таким источникам. В данном случае под источником информации подразумевается материальный объект, обладающий определенными сведениями, представляющими конкретный интерес для злоумышленников или конкурентов.

Многочисленные публикации последних лет показывают, что злоупотребления информацией, циркулирующей в ИС или передаваемой по каналам связи, совершенствовались не менее интенсивно, чем меры защиты от них. В настоящее время для обеспечения защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода, включающего комплекс взаимосвязанных мер (использование специальных технических и программных средств, организационных мероприятий, нормативно-правовых актов, морально- этических мер противодействия и т.д.). Комплексный характер защиты проистекает из комплексных действий злоумышленников, стремящихся любыми средствами добыть важную для них информацию.

Сегодня можно утверждать, что рождается новая современная технология — *технология защиты информации*в компьютерных информационных системах и в сетях передачи данных. Реализация этой технологии требует увеличивающихся расходов и усилий. Однако все это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз ИС и ИТ.

1. Классификация возможных угроз безопасности экономических информационных систем.

Наряду с интенсивным развитием вычислительных средств и систем передачи информации все более актуальной становится проблема обеспечения ее безопасности. Меры безопасности направлены на предотвращение несанкционированного получения информации, физического уничтожения или модификации защищаемой информации.

Зарубежные публикации последних лет показывают, что возможности злоупотреблений информацией, передаваемой по каналам связи, развивались и совершенствовались не менее интенсивно, чем средства их предупреждения. В этом случае для защиты информации требуется не просто разработка частных механизмов защиты, а организация комплекса мер, т.е. использование специальных средств, методов и мероприятий с целью предотвращения потери информации. В этом смысле сегодня рождается новая современная технология - технология защиты информации в компьютерных информационных системах и в сетях передачи данных.

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным.

Под угрозой безопасности понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Угрозы принято делить на случайные, или непреднамеренные, и умышленные. Источником первых могут быть ошибки в программном обеспечении, выходы из строя аппаратных средств, неправильные действия пользователей или администрации и т.п. Умышленные угрозы преследуют цель нанесения ущерба пользователям АИТ и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

К основным угрозам безопасности информации относят:

-раскрытие конфиденциальной информации;

-компрометация информации;

-несанкционированное использование информационных ресурсов;

-ошибочное использование ресурсов;

-несанкционированный обмен информацией;

-отказ от информации;

-отказ от обслуживания.

Средствами реализации угрозы раскрытия конфиденциальной информации могут быть несанкционированный доступ к базам данных, прослушивание каналов и т.п. В любом случае получение информации, являющейся достоянием некоторого лица (группы лиц), другими лицами наносит ее владельцам существенный ущерб.

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.

Несанкционированное использование информационных ресурсов, с одной стороны, является средством раскрытия или компрометации информации, а с другой -- имеет самостоятельное значение, поскольку, даже не касаясь пользовательской или системной информации, может нанести определенный ущерб абонентам и администрации. Этот ущерб может варьировать в широких пределах -- от сокращения поступления финансовых средств до полного выхода АИТ из строя.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее может привести к разрушению, раскрытию или компрометации указанных ресурсов. Данная угроза чаще всего является следствием ошибок в программном обеспечении АИТ.

Несанкционированный обмен информацией между абонентами может привести к получению одним из них сведений, доступ к которым ему запрещен, что по своим последствиям равносильно раскрытию содержания маркетинговой информации.

Отказ от информации состоит в непризнании получателем или отправителем информации фактов ее получения или отправки. В условиях маркетинговой деятельности это, в частности, позволяет одной из сторон расторгать заключенные финансовые соглашения «техническим» путем, формально не отказываясь от них и нанося тем самым второй стороне значительный ущерб.

Отказ в обслуживании представляет собой весьма существенную и распространенную угрозу, источником которой является сама АИТ. Подобный отказ особенно опасен в ситуациях, когда задержка с предоставлением ресурсов абоненту может привести к тяжелым для него последствиям. Так, отсутствие у пользователя данных, необходимых для принятия решения, в течение периода, когда это решение еще может быть эффективно реализовано, может стать причиной его нерациональных или даже антимонопольных действий.

Основными типовыми путями несанкционированного доступа к информации, сформулированными на основе анализа зарубежной печати, являются:

-перехват электронных излучений;

-принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции;

-применение подслушивающих устройств (закладок);

-дистанционное фотографирование;

-перехват акустических излучений и восстановление текста принтера;

-хищение носителей информации и документальных отходов;

-чтение остаточной информации в памяти системы после выполнения санкционированных запросов;

-копирование носителей информации с преодолением мер защиты;

-маскировка под зарегистрированного пользователя;

-мистификация (маскировка под запросы системы);

-использование программных ловушек;

-использование недостатков языков программирования и операционных систем;

-включение в библиотеки программ специальных блоков типа «Троянский конь»;

-незаконное подключение к аппаратуре и линиям связи;

-злоумышленный вывод из строя механизмов защиты;

-внедрение и использование компьютерных вирусов.

Необходимо отметить, что особую опасность в настоящее время представляет проблема компьютерных вирусов, ибо эффективной защиты против них разработать не удалось. Остальные пути несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности.

1. Методы, средства и организация системы защиты информации в экономических информационных системах
   1. Правовые основы обеспечения информационной безопасности

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных, обеспечивающей:

конституционные права и свободы граждан, предприятий и организаций в сфере информатизации;

необходимый уровень безопасности информации, подлежащей защите;

защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи информации).

Ключевым моментом политики государства в данной области является осознание необходимости защиты любых информационных ресурсов и информационных технологий, неправомерное обращение с которыми может нанести ущерб их собственнику, владельцу, пользователю или иному лицу.

Нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации включают:

Законы Российской Федерации

Указы Президента Российской Федерации и утверждаемые этими указами нормативные документы

Постановления Правительства Российской Федерации и утверждаемые этими постановлениями нормативные документы (Положения, Перечни и т.п.)

Государственные и отраслевые стандарты

Положения, Порядки. Руководящие документы и другие нормативные и методические документы уполномоченных государственных органов (Гостехкомиссии России, ФАПСИ, ФСБ).

Федеральные законы и другие нормативные акты предусматривают:

разделение информации на категории свободного и ограниченного доступа, причем информация ограниченного доступа подразделяется на:

отнесенную к государственной тайне

отнесенную к служебной тайне (информацию для служебного пользования), персональные данные (и другие виды тайн)

и другую информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;

правовой режим защиты информации, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу, устанавливаемый:

в отношении сведений, отнесенных к государственной тайне, -уполномоченными государственными органами на основании Закона Российской Федерации "О государственной тайне" (от 21.07.93 г. N 5485-1) ФЗ РФ "О государственной тайне" (от 21.07.93 г. N 5485-1);

в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании Закона Российской Федерации "Об информации, информатизации и защите информации" (в ред. Федеральных законов от 27.07.2010 N 227-ФЗ, от 06.04.2011 N 65-ФЗ) ФЗ РФ "Об информации, информатизации и защите информации" (в ред. Федеральных законов от 27.07.2010 N 227-ФЗ, от 06.04.2011 N 65-ФЗ);

в отношении персональных данных - отдельным федеральным законом;

лицензирование деятельности предприятий, учреждений и организаций в области защиты информации;

аттестование автоматизированных информационных систем, обрабатывающих информацию с ограниченным доступом на соответствие требованиям безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности (секретности);

сертификацию средств защиты информации и средств контроля эффективности защиты, используемых в АС;

возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством Российской Федерации;

создание автоматизированных информационных систем в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;

определение прав и обязанностей субъектов в области защиты информации.

Рассмотренные выше Федеральные законы и другие нормативные акты составляют правовые основы обеспечения информационной безопасности.

3.2. Основные методы и средства защиты информации в АИТ

При разработке АИТ возникает проблема по решению вопроса безопасности информации, составляющей коммерческую тайну, а также безопасности самих компьютерных информационных систем.

Каждую систему защиты следует разрабатывать индивидуально, учитывая следующие особенности:

- организационную структуру организации;

- объем и характер информационных потоков (внутри объекта в целом, внутри отделов, между отделами, внешних);

- количество и характер выполняемых операций: аналитических и повседневных;

- количество и функциональные обязанности персонала;

- количество и характер клиентов;

- график суточной нагрузки.

Защита должна разрабатываться для каждой системы индивидуально, но в соответствии с общими правилами. Построение защиты предполагает следующие этапы:

- анализ риска, заканчивающийся разработкой проекта системы защиты и планов защиты, непрерывной работы и восстановления;

- реализация системы защиты на основе результатов анализа риска;

- постоянный контроль за работой системы защиты и АИС в целом (программный, системный и административный).

На каждом этапе реализуются определенные требования к защите; их точное соблюдение приводит к созданию безопасной системы.

Для обеспечения непрерывной защиты информации в АИС целесообразно создать из специалистов группу информационной безопасности. На эту группу возлагаются обязанности по сопровождению системы защиты, ведения реквизитов защиты, обнаружения и расследования нарушений политики безопасности и т.д.

Основные этапы построения системы защиты заключаются в следующем:

Анализ => Разработка системы защиты (планирование) => Реализация системы защиты => Сопровождение системы защиты.

Этап анализа возможных угроз АИС необходим для фиксирования на

определенный момент времени состояния АИС (конфигурации аппаратных и программных средств, технологии обработки информации) и определения возможных воздействий на каждый компонент системы. Обеспечить защиту АИС от всех воздействий на нее невозможно, хотя бы потому, что невозможно полностью установить перечень угроз и способов их реализации. Поэтому надо выбрать из всего множества возможных воздействий лишь те, которые могут реально произойти и нанести серьезный ущерб владельцам и пользователям системы.

На этапе планирования формируется система защиты как единая совокупность мер противодействия различной природы.

Сущность этапа реализации системы защиты заключается в установке и настройке средств защиты, необходимых для реализации зафиксированных в плане защиты правил обработки информации. Содержание этого этапа зависит от способа реализации механизмов защиты в средствах защиты.

Этап сопровождения заключается в контроле работы системы, регистрации происходящих в ней событий, их анализе с целью обнаружить нарушения безопасности. В том случае, когда состав системы претерпел существенные изменения (смена вычислительной техники, переезд в другое здание, добавление новых устройств или программных средств), требуется повторение описанной выше последовательности действий.

Стоит отметить тот немаловажный факт, что обеспечение защиты АИС -- это итеративный процесс, завершающийся только с завершением жизненного цикла всей системы.

Можно выделить следующие 3 направления управления защиты информации в экономических информационных системах, которые представлены на рисунке 3.1.

Рис. 3.1. Управление защитой компьютерной безопасностью. Ясенев В.Н. Информационная безопасность в экономических системах: учебное пособие. - М.: ННГУ, 2006.

К правовому обеспечению защиты информации относятся действующие в стране законы, указы и другие нормативно - правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Инженерно-техническая защита -- это совокупность специальных органов, технических средств и мероприятий, функционирующих совместно для выполнения определенной задачи по защите информации.

Инженерно-техническая защита использует следующие средства:

физические средства;

аппаратные средства;

программные средства;

криптографические средства.

В свою очередь организационные мероприятия и процедуры, используемые для решения проблемы безопасности информации, решаются на всех этапах проектирования и в процессе эксплуатации АИТ.

Среди организационных мероприятий по обеспечению безопасности информации важное место занимает охрана объекта, на котором расположена защищаемая АИТ (территория здания, помещения, хранилища информационных носителей). При этом устанавливаются соответствующие посты охраны, технические средства, предотвращающие или существенно затрудняющие хищение средств вычислительной техники, информационных носителей, а также исключающие несанкционированный доступ к АИТ и линиям связи.

Следует отметить, что без надлежащей организационной поддержки программно-технических средств защиты информации от несанкционированного доступа и точного выполнения, предусмотренных проектной документацией процедур в должной мере не решить проблему обеспечения безопасности информации, какими бы совершенными эти программно-технические средства не были.

Создание базовой системы зашиты информации в АИТ основывается на следующих принципах:

1. Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий. Он означает оптимальное сочетание программных аппаратных средств и организационных мер защиты, подтвержденное практикой создания отечественных и зарубежных систем защиты.

2. Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки. Пользователям предоставляется минимум строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автоматизированной обработки доступной им конфиденциальной информации.

3. Полнота контроля и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования.

4. Обеспечение надежности системы защиты, т.е. невозможность снижения ее уровня при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала.

5. Обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.

6. “Прозрачность” системы защиты информации для общего, прикладного программного обеспечения и пользователей АИТ.

7. Экономическая целесообразность использования системы защиты. Он выражается в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации АИТ без системы защиты (рис. 3.2.)

Рис.3.2. Управление защитой информации.

К основным методам защиты информации в ЭИС относятся: препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение. (рис 3.3.)

Рис. 3.3. Методы и средства информационной безопасности экономического объекта.

Итак, рассмотрим каждый из этих методов в отдельности.

Препятствие - метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом - метод защиты информации путем регулирования использования всех ресурсов информационной системы (элементов баз данных, программных и технических средств). Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы;

- опознание объекта или субъекта по предъявленному им идентификатору;

- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

- разрешение и создание условий работы в пределах установленного регламента;

- регистрацию обращений к защищаемым ресурсам;

- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Маскировка -- метод защиты информации путем ее криптографического закрытия. Этот метод защиты широко применяется за рубежом, как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Регламентация -- метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение - такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение -- такой метод защиты, который побуждает пользователя и персонал системы не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных). Автоматизированные информационные технологии в экономике: Учебник/ Под ред.проф. Г.А. Титоренко. - М.: Компьютер, ЮНИТИ, 1999. - 400с.

Рассмотренные методы обеспечения безопасности реализуются на практике за счет применения различных средств защиты, таких, как технические, программные, организационные, законодательные и морально-этические как это представлено на рисунке 2.3.

К основным средствам защиты, используемым для создания механизма защиты, относятся следующие:

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программные средства представляют из себя программное обеспечение, специально предназначенное для выполнения функций зашиты информации.

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование компьютерной информационной системы банковской деятельности, монтаж и наладка оборудования, испытания, эксплуатация).

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в обществе. Эти нормы большей частью не являются обязательными как законодательные меры, однако, несоблюдение их ведет обычно к потере авторитета и престижа человека. Наиболее показательным примером таких норм является Кодекс профессионального поведения членов Ассоциаций пользователей ЭВМ США.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

3.3. Механизмы криптографии

Для реализации мер безопасности используются различные механизмы шифрования (криптографии). Криптография -- это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Сущность криптографических методов заключается в том, что для предотвращения несанкционированного доступа к какому-либо сообщению оно зашифровывается. Когда санкционированный пользователь получает это сообщение, он дешифрует или раскрывает его посредством обратного преобразования криптограммы.

Криптографическая система основывается на использовании специального алгоритма, который запускается уникальным числом, называемым шифрующим ключом. Для обмена зашифрованными сообщениями, как отправителю, так и получателю необходимо знать правильную ключевую установку и хранить ее в тайне.

Наряду с шифрованием используются и другие механизмы безопасности: угроза информация шифрование криптографический

- цифровая (электронная) подпись;

- контроль доступа;

- обеспечение целостности данных;

- обеспечение аутентификации;

- управление маршрутизацией;

- арбитраж или освидетельствование.

Механизмы цифровой подписи основываются на алгоритмах ассиметричного шифрования и включают две процедуры: формирование подписи отправителем и ее опознавание (верификацию) получателем.

Механизмы контроля доступа осуществляют проверку полномочий объектов ИТ (программ и пользователей) на доступ к ресурсам сети.

Механизмы обеспечения целостности данных реализуются выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по физически ненадежным каналам.

Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами ИТ, третьей стороной (арбитром).

Для обеспечения непрерывной защиты информации в АИС целесообразно создать из специалистов группу информационной безопасности. На эту группу возлагаются обязанности по сопровождению системы защиты, ведения реквизитов защиты, обнаружения и расследования нарушений политики безопасности и т.д.

3.4. Шифрование как основной метод защиты информации

Постоянное развитие и совершенствование информационных технологий дает возможность передавать и хранить все большие объемы информации. Это благо имеет и оборотную сторону. Информация становится все более уязвимой.

Поэтому все большую важность приобретает проблема защиты информации от несанкционированного доступа (НСД) при передаче и хранении. Сущность этой проблемы - постоянная борьба специалистов по защите информации со своими "оппонентами".

Очевидная тенденция к переходу на цифровые методы передачи и хранения информации позволяет применять унифицированные методы и алгоритмы для защиты дискретной (текст, факс, телекс) и непрерывной информации.

Испытанный метод защиты информации от НСД - шифрование (криптография). Шифрованием называют процесс преобразования открытых данных в зашифрованные или зашифрованных данных в открытые по определенным правилам с применением ключей.

С помощью криптографических методов возможно:

\* шифрование информации;

\* реализация электронной подписи;

\* распределение ключей шифрования;

\* защита от случайного или умышленного изменения информации.

К алгоритмам шифрования предъявляются определенные требования:

\* высокий уровень защиты данных против дешифрования и возможной модификации;

\* защищенность информации должна основываться только на знании ключа и не зависеть от того, известен алгоритм или нет (правило Киркхоффа);

\* малое изменение исходного текста или ключа должно приводить к значительному изменению шифрованного текста (эффект "обвала");

\* область значений ключа должна исключать возможность дешифрования данных путем перебора значений ключа;

\* экономичность реализации алгоритма при достаточном быстродействии;

\* стоимость дешифрования данных без знания ключа должна превышать стоимость данных.

Существует два основных типа криптографических алгоритмов:

- симметричные, для которых ключ расшифрования совпадает с ключом зашифрования;

- асимметричные (алгоритмы с открытым ключом), использующие для зашифрования и расшифрования два разных ключа.

Симметричные алгоритмы делятся на две категории:

- потоковые шифры, в которых данные обрабатываются побитово (посимвольно),

- блочные шифры, в которых операции производятся над группами битов.

Для осуществления этих алгоритмов применяются специальные программы, которых в настоящее время на рынке информационных технологий достаточно много.

Входная информация.

Входной информацией в данном вопросе является то, что требуется защитить от несанкционированного доступа путем шифрования.

Программы, использующие для этих целей, работают с файлами (шифрование, установка защит). Таком образом, входными данными являются файлы различного типа для шифрования и EXE- и COM-файлы для установки пароля и проверки по ключевой дискете.

Постоянная информация.

В качестве постоянной информации используются таблицы перестановок и константы генератора псевдослучайных чисел при шифровании файлов.

Выходная информация.

Результатом выполнения алгоритма шифрования информации являются выходные данные. Это зашифрованные файлы и защищенные программы.

Как показывает практика, абсолютных способов защиты информации не существует. Какими бы сложными и дорогими не были предлагаемые на рынке средства защиты, их эффективность оказывается условной. С учетом сложившейся реальной обстановки востребованными оказываются несложные и недорогие средства защиты, разрабатываемые и устанавливаемые самим производителем продукта и направленные против незаконных действий квалифицированных пользователей.

ЗАКЛЮЧЕНИЕ

В данной курсовой работе были изучены информационные угрозы, их классификации и виды защиты безопасности.

Можем кратко рассмотреть изученный материал.

Создание системы защиты информации экономических систем основывается на совокупности принципов и подходов. Наиболее важными являются принципы непрерывности совершенствования и развития системы информационной безопасности и комплексного использования всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла обработки информации.

Важнейшими условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и предприятия, высокий профессионализм сотрудников, занимающихся вопросами информационной безопасности, подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.

Создание системы защиты информации экономических систем включает в себя следующие этапы: обследование организации,

проектирование системы защиты информации, внедрение системы защиты информации, сопровождение системы информационной безопасности, обучение специалистов по защите информации.

Обеспечение информационной безопасности требует комплексного подхода, в основе которого должна лежать система обеспечения информационной безопасности, включающая организационную (подготовленный персонал и нормативные документы) и техническую (средства защиты информации) составляющие.

Таким образом, система защиты информации в экономических информационных системах представляет собой сложный комплекс мер, способов и средств, гарантирующих обеспечение безопасности экономической информации. Однако из-за постоянного обновления компьютерных технологий возникают новые угрозы для информации, поэтому проблема обеспечения ее безопасности, предотвращения несанкционированного доступа к информации, ее уничтожения или модификации, становится все более актуальной, свидетельствует о необходимости более подробного изучения и решения вопросов защиты информации в экономических информационных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Автоматизированные информационные технологии в экономике: Учебник/Под ред. проф. Г.А. Титоренко. - М.: Компьютер, ЮНИТИ, 1999. - 400с.
2. Адамадзиев К.Р., Асхабова А.Н. Информационные системы в экономике: Учебное пособие. - Махачкала: 2002. - 138с.
3. Герасименко В.А. Проблемы защиты данных в системах их обработки. // Зарубежная радиоэлектроника, 1989 г., №12, с. 5-21.
4. Емельянова Н.З., Партыка Т.Л. Попов И.И. Информационные системы в экономике. Издательство "Форум", 2005, 461 с.