**Задание на 25.01.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу «Настройка удаленного доступа к сети.** Основные уязвимости удаленного доступа». Написать отчет по практической работе. *(программу с помощью которой будите настраивать доступ выбираете сами, в отчете должны быть обоснования выбора той или иной программы, скриншоты настройки).*
3. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 1**

ВВЕДЕНИЕ

**Предмет и задачи программно-аппаратной защиты информации.**

Современное развитие человеческой цивилизации, вступившей в двадцать первый век, характеризуется наиболее интенсивным Использованием компьютерных информационных технологий во всех сферах общественной жизни. В настоящее время становится трудно назвать те области жизнедеятельности, успехи в которых не были бы связаны с применением таких технологий.

На смену индустриальному этапу общественного развития приходит эволюционная фаза, названная информатизацией при которой все структуры общества преобразуются таким образом, чтобы обеспечить этим структурам и обществу в целом наиболее эффективное и динамичное развитие на основе максимально полного использования имеющихся компьютерных информационных ресурсов. Традиционные материальные ресурсы постепенно утрачивают свое первоначальное значение, а им на смену приходят информационные ресурсы, которые со временем не убывают, а неуклонно растут. Информация, как предмет труда, становится все в большей степени стратегическим ресурсом общества, его движущей производительной силой.

В условиях информатизации общества особую ценность обретают люди - носители знаний, наилучшие передатчики технологической информации и передового опыта, для их эффективного участия в информационных процессах создается мощнейшая инфраструктура средств компьютерной и телекоммуникационной техники, изменяющая не только процесс и характер трудовой деятельности, но и сам образ жизни, и систему ценностей человека. В настоящее время хорошо налаженная распределенная сеть информационно-вычислительных комплексов способна сыграть такую же роль в современном обществе, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые.

Современные информационные технологии приобретают глобальный характер, охватывая все сферы жизнедеятельности человека, формируя информационное единство всей человеческой цивилизации. С помощью глобальной вычислительной сети Интернет объединяются и перемещаются на любые расстояния гигантские объемы информации, обеспечивается доступ многочисленных пользователей, расположенных на практически неограниченной территории, к информационным ресурсам всего мирового сообщества.

Для государств современного мира становится очевидным, что отставание в области информатизации может оказаться непреодолимым препятствием для их дальнейшего развития, привести к существенным, а подчас драматическим последствиям во всех сферах жизнедеятельности, превратить их в сырьевой придаток информационно и промышленно развитых стран.

Широкое использование компьютерных информационных технологий во всех сферах жизни современного общества делает вполне закономерной и весьма актуальной проблему компьютерной защиты информации, или иначе, проблему обеспечения информационной безопасности. В условиях интенсивного развития рынка информационных продуктов и услуг информация становится полноценным товаром, обладающим своими стоимостными характеристиками и потребительскими свойствами. Подобно любым другим традиционно существующим товарам, информация также нуждается в своей сохранности и, следовательно, надежной защите.

В методологии анализа информационной безопасности обычно выделяют следующие основные понятия:

— объект информационной безопасности;

— существующие и потенциально возможные угрозы данному объекту;

— обеспечение информационной безопасности объекта от проявления таких угроз.

Если объектом информационной безопасности выступает сама информация, то для нее наиболее важным является сохранение таких свойств, как:

— целостность;

— конфиденциальность;

— доступность.

Целостность информации заключается в ее существовании в неискаженном виде по отношению некоторому фиксированному состоянию.

Конфиденциальность – это свойство, указывающее на необходимость введения Ограничений доступа к данной информации для определенного круга лиц.

доступность информации — это ее свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к необходимой информации.

Весьма распространенным и вполне естественным является также рассмотрение безопасности информации в инфраструктуре конкретной информационной системы (ИС). Такие системы представляют собой Взаимосвязанную совокупность средств, методов и персонала, обеспечивающих сбор, хранение, обработку, передачу и отображение информации в интересах достижения поставленной цели. Целью создания ИС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (в случае необходимости). Информация является при этом конечным «продуктом потребления» и выступает в качестве центральной компоненты информационной системы. Объектом информационной безопасности становится в этом случае данная информационная система.

В методологическом плане общим основанием для отнесения данного объекта к множеству объектов информационной безопасности является наличие в нем так называемого «информационного измерения» и необходимость обеспечения безопасности этого «измерения». К «информационно измеряемым» объектам относятся объекты, для которых одной из важных структурных составляющих является либо сама информация, либо деятельность, предметом которой она является.

С этой точки зрения, упомянутые ранее информационные системы, безусловно, являются объектами информационной безопасности. В инфраструктуре таких систем не только представлена различная информация, но и реализуются процессы, связанные с ее преобразованием.

Значимость «информационного измерения», а, следовательно, и необходимость обеспечения информационной безопасности хорошо прослеживаются в иерархии объектов: человек — общество — государство.

Информация, «информационное измерение» имеют для человека такое же важное значение, как пища, воздух, вода. Информация обуславливает не только возможность его адаптации как биологического существа к условиям внешней среды, но и обуславливает возникновение его социальных потребностей, возможность его социальной адаптации, развития личности, самореализации и самоутверждения. Информация является основным средством взаимодействия человека с другими людьми. Посредством информации реализуются процессы воспитания и образования, происходит овладение трудовыми навыками, осуществляется мотивация его деятельности, а также в определенной мере и сама деятельность. Таким образом, информационная безопасность человека заключается в невозможности нанесения вреда ему как личности, существование и социальная деятельность которой во многом базируется на осмыслении получаемой информации, информационных взаимодействиях с другими индивидами, и часто использующей информацию в качестве предмета своей деятельности.

Свое «информационное измерение» имеет общество, представляющее собой сложный вид организации социальной жизни. Оно позволяет поддерживать его целостность, упорядочивать отношения между отдельными общностями, интегрировать социальные новообразования и подчинять их логике поведения Основной массы населения, воспроизводить единую ткань многообразных социальных взаимодействий, осуществляемых средствами информационной коммуникации. Также трудно переоценить роль информации и информационной инфраструктуры в функционировании духовной сферы общества, в функционировании и распространении культуры, системы ценностей, норм поведения, регулирующих взаимодействие между людьми. Таким образом, информационная безопасность общества заключается в невозможности нанесения вреда его духовной сфере, культурным ценностям, социальным регуляторам поведения людей, информационной инфраструктуре и передаваемым с ее ПОМОЩЬЮ сообщениям.

«Информационное измерение» государства определяется многообразным информационным наполнением его деятельности в самых различных сферах, например, таких, как обеспечение национальной безопасности, ликвидация последствий стихийных бедствий и экономических катастроф, реализация социальных программ поддержки здравоохранения, образования, социального обеспечения нетрудноспособных, защита прав и свобод граждан. В условиях современной глобализации информационных процессов безопасность государства в информационной сфере становится важнейшей составляющей национальной безопасности. Таким образом, информационная безопасность государства заключается в невозможности нанесения вреда деятельности государства по выполнению функций управления делами общества, предметом которой выступают информация и информационная инфраструктура.

Человек, общество и государство не являются единственно возможными объектами безопасности, обладающими своим «информационным измерением». Масштабная проблематика обеспечения информационной безопасности названных объектов, безусловно, детализируется и конкретизируется на локальных уровнях сложной социально-экономической и общественно-политической иерархии любого государства. Так, в условиях конкурентно-рыночных отношений весьма распространенными объектами информационной безопасности становятся компьютерные системы, отображающие информационными средствами деятельность различных предприятий, организаций и учреждений. Очевидной является необходимость обеспечения безопасного и надежного функционирования таких систем.

С любым объектом информационной безопасности естественным образом связано существование той или иной угрозы, под которой понимается совокупность условий и факторов, возникающих в процессе взаимодействия данного объекта с другими объектами или составляющих его компонентов между собой и способных оказывать на него негативное воздействие. в широком смысле такие угрозы могут носить как случайный, таки преднамеренный характер.

Случайные угрозы могут быть вызваны авариями и стихийными бедствиями, сбоями и отказами в работе компьютерных систем, ошибками, допущенными при их разработке, а также ошибочными действиями пользователей и обслуживающего персонала. В настоящее время такие угрозы достаточно хорошо изучены статистическими методами, что позволяет вполне адекватно противодействовать им.

Более опасными с точки зрения характера и последствий проявления являются преднамеренные угрозы, вызванные злоумышленными действиями людей. Арсенал и изощренность таких угроз неуклонно расширяются, поэтому для их нейтрализации необходимо предугадать не только возможные цели злоумышленника, но и его квалификацию, и техническую оснащенность.

Для любого объекта информационной безопасности (государство, отрасль, ведомство, государственное предприятие, частная фирма и т.д.) противодействие существующим и потенциально возможным угрозам достигается проведением соответствующей политики безопасности. Для ее реализации используются различные средства, методы и мероприятия. К их числу относятся, в частности, правовые нормы, организационные мероприятия, инженерно-технические и программно-аппаратные средства, методы криптографии. Названные средства обычно рассматриваются также в качестве соответствующих видов обеспечения информационной безопасности.

Учитывая системный характер влияния на компьютерную информационную безопасность многочисленных факторов и обстоятельств, вполне очевидно, что эффективное решение этой проблемы возможно только на основе комплексного и целенаправленного использования всех имеющихся средств, обеспечивающих в целом необходимый и, главное, гарантированный уровень защищенности информационных ресурсов.

Следует отметить, что рассматриваемая проблема обеспечения информационной безопасности весьма актуальна для нашей страны. Нельзя считать, что из-за унаследованной информационной замкнутости, некоторой технической отсталости Россия мене уязвима в информационном отношении, чем другие страны. Скорее наоборот: достаточно высокая степень централизации структур государственного управления российской экономикой может привести к гибельным последствиям в результате информационной агрессии.

В 2000 году Президентом была утверждена Доктрина информационной безопасности Российской Федерации, устанавливающая официальную систему взглядов на содержание национальных интересов России в информационной сфере, методы противодействия существующим угрозам и систему обеспечения информационной безопасности. При этом были учтены проблемы развития российского общества, порожденные как советским периодом его истории, так и периодом продолжающихся социально-экономических и политических преобразований.

Реализация закрепленных в Доктрине положений должна создать необходимые условия, обеспечивающие устойчивое развитие российского общества и его институтов на базе информатизации производственной, духовной, политической и социальной сфер общественной жизни, а также поддержание соответствующего современным международным стандартам правового статуса личности.

Так, с 1992 года выявление угроз информационной безопасности и подготовка предложений по противодействию этим угрозам возложено законодательством на Совет Безопасности РФ, при котором образована Межведомственная комиссия по информационной безопасности. С 1996 года в Комитете Государственной Думы РФ существует подкомитет по информационной безопасности, а также экспертный совет по законодательству в области обеспечения информационной безопасности. Большую работу в этой области выполняют также федеральные органы исполнительной власти, а также государственные органы субъектов РФ.

Интенсифицируются исследования проблем обеспечения программно-аппаратной компьютерной информационной безопасности, выполняемые как в естественных и технических науках, так и в рамках гуманитарных наук. Комплексное научное осмысление этих проблем существенно способствует развитию индустрии средств защиты информации, используемых, в том числе, в современных компьютерных и телекоммуникационных системах.

Развивается правовое регулирование отношении в области обеспечения информационной безопасности. Приняты такие базовые законодательные акты как законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «О связи», «О государственной тайне», первая и вторая части Гражданского кодекса РФ, новые редакции Уголовного и Уголовно-процессуального кодексов РФ, ряд законов, регулирующих отношения в области средств массовой информации, и др.

Совершенствуется система подготовки кадров высшей квалификации по вопросам обеспечения информационной безопасности. Специальности, по которым осуществляется подготовка специалистов в этой области, выделены в отдельный раздел Перечня направлений подготовки и специальностей высшего профессионального образования.

**Аппаратные средства защиты информации**

Аппаратные средства – это технические средства, используемые для обработки данных.

Сюда относятся:

- персональный компьютер (комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач).

-периферийное оборудование (комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора).

-физические носители машинной информации.

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

-специальные регистры для хранения реквизитов защиты: паролей,

идентифицирующих кодов, грифов или уровней секретности;

-генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;

-устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;

-специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты;

-схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

-особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (криптографические методы).

**Программные средства обеспечения защиты информации**

Программные средства - это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения. К ним относятся:

-Программное обеспечение (совокупность управляющих и обрабатывающих программ).

Состав:

-Системные программы (операционные системы, программы технического обслуживания);

-Прикладные программы (программы, которые предназначены для решения задач определенного типа, например редакторы текстов, антивирусные программы, СУБД и т.п.);

-Инструментальные программы (системы программирования, состоящие из языков программирования: Turbo C, Microsoft Basic и т.д. и трансляторов – комплекса программ, обеспечивающих автоматический перевод с алгоритмических и символических языков в машинные коды);

-Машинная информация владельца, собственника, пользователя.

К программным средствам защиты относятся специальные программы, которые предназначены для выполнения функций защиты и включаются в состав программного обеспечения систем обработки данных. Программная защита является наиболее распространенным видом защиты, чему способствуют такие положительные свойства данного средства, как универсальность, гибкость, простота реализации, практически неограниченные возможности изменения и развития и т.п. По функциональному назначению их можно разделить на следующие группы:

-идентификация технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач и пользователей;

-определение прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей;

-контроль работы технических средств и пользователей;

-регистрация работы технических средств и пользователей при обработки

информации ограниченного использования;

-уничтожения информации в ЗУ после использования;

-сигнализации при несанкционированных действиях;

-вспомогательные программы различного назначения: контроля работы механизма защиты, проставления грифа секретности на выдаваемых документах.

**Задачи обеспечения программно-аппаратной защиты информации.**

Под программно-аппаратным обеспечением средств защиты операционной системы традиционно понимается совокупность средств и методов, используемых для решения следующих задач:

-управление оперативной и виртуальной памятью компьютера;

-распределение процессорного времени между задачами в многозадачной операционной системе;

-синхронизация выполнения параллельных задач в многозадачной

операционной системе;

-обеспечение совместного доступа задач к ресурсам операционной

системы.

Основные выводы о способах использования средств, методов и мероприятий защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.

2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.

3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.

4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.

Вопросы

1. Что такое информационное единство?
2. В чем заключается актуальность, проблемность компьютерной безопасности информации?
3. Что значит «Информационное измерение» объекта информации? Какие объекты информации являются измеряемыми?
4. Перечислите угрозы информационной безопасности.
5. В каком году Президентом была утверждена Доктрина информационной безопасности Российской Федерации, устанавливающая официальную систему взглядов на содержание национальных интересов России в информационной сфере, методы противодействия существующим угрозам и систему обеспечения информационной безопасности?
6. С какого года в Комитете Государственной Думы РФ существует подкомитет по информационной безопасности, а также экспертный совет по законодательству в области обеспечения информационной безопасности.
7. Что такое Кейлоггер, к каким средствам защиты информации он относится и для чего применяется.