Государственное образовательное учреждение

высшего образования Московской области

«Государственный гуманитарно-технологический университет»

Ликино-Дулёвский политехнический колледж – филиал ГГТУ

***Проект***

***На тему: «Защита информации»***

Авторы проекта:

студенты группы ИСП21.1А

Калинин Владислав Алексеевич

Руководитель проекта:

преподаватель информатики:

Кимлык Юлия Александровна

Ликино-Дулёво

2022

**Введение**

Мы живем на стыке двух тысячелетий, когда человечество вступило в эпоху новой научно-технической революции.

К концу двадцатого века люди овладели многими тайнами превращения вещества и энергии и сумели использовать эти знания для улучшения своей жизни. Но кроме вещества и энергии в жизни человека огромную роль играет еще одна составляющая - информация. Это самые разнообразные сведения, сообщения, известия, знания, умения.

В середине прошлого столетия появились специальные устройства - компьютеры, ориентированные на хранение и преобразование информации и произошла компьютерная революция.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Информацией владеют и используют её все люди без исключения. Каждый человек решает для себя, какую информацию ему необходимо получить, какая информация не должна быть доступна другим и т.д. Человеку легко, хранить информацию, которая у него в голове, а как быть, если информация занесена в «мозг машины», к которой имеют доступ многие люди.

Многие знают, что существуют различные способы защиты информации. А от чего, и от кого её надо защищать? И как это правильно сделать?

То, что эти вопросы возникают, говорит о том, что тема в настоящее время актуальна. В курсовой работе я постарался ответить на эти вопросы, поставив перед собой

**Цель**: выяснить как защищать информацию и определить источники угроз.

**Задачи**: Определить виды защиты информации, выявить основные угрозы для информации, определить способы защиты информации.

**Кому нужны ваши данные?..**

Это зависит от того, кто вы такой и какими данными располагаете. Но также существует отдельный тип рода деятельности называемый хакером (англ. cracker взломщик). Некоторые работают группами, некоторые отдельно. Их методы различны, но основной постоянный рабочий инструмент – программа-взломщик, делящаяся на два основных компонента: программа для доступа к удаленным компьютерам по телефонным сетям и словарь вероятных кодов и паролей. Задача программы-взломщика получить доступ к удаленному компьютеру с помощью подбора кодов и паролей до тех пор, пока комбинация не будет найдена; это обеспечит доступ к системе.

Фрикеры это взломщики, которые специализируются на нападениях на телефонные системы. Телефонная сеть привлекает внимание большинства взломщиков так как она является на данный момент самой большой (глобальной) сетью на планете.

## Защита информации.

Персональным компьютерам присущ ряд таких свойств, которые, с одной стороны, благоприятствуют защите, а с другой — затрудняют ее и усложняют.К основным из указанных свойств относятся:

1. малые габариты и вес, что делает их не просто транспортабельными, а легко переносимыми;

2. наличие встроенного внутреннего ЗУ большого объема, сохраняющего записанные данные после выключения питания;

3. наличие сменного ЗУ большого объема и малых габаритов;

4. наличие устройств сопряжения с каналами связи;

5. оснащенность программным обеспечением с широкими функциональными возможностями;

6. массовость производства и распространения;

7. относительно низкая стоимость.

На формирование множества возможных подходов к защите информации в ПК и выбор наиболее целесообразного из них в конкретных ситуациях определяющее влияние оказывают следующие факторы:
1) цели защиты;
2) потенциально возможные способы защиты;
3) имеющиеся средства защиты.

Основные цели защиты информации:
1)обеспечение физической целостности;
2)обеспечение логической целостности;
3)предупреждение несанкционированного получения;
4)предупреждение несанкционированной модификации;
5)предупреждение несанкционированного копирования.

**Предупреждение несанкционированной модификации.**

Весьма опасной разновидностью несанкционированной модификации информации в ПК является действие вредоносных программ (компьютерных вирусов), которые могут разрушать или уничтожать программы или массивы данных.

**Предупреждение несанкционированного получения информации, находящейся в ПК.**

Данная цель защиты приобретает особую актуальность в тех случаях, когда хранимая или обрабатываемая информация содержит тайну того или иного характера (государственную, коммерческую и т. п.).

**Предупреждение несанкционированного копирования информации.**

Актуальность данной разновидности защиты определяется следующими тремя обстоятельствами: накопленные массивы информации все больше становятся товаром; все более широкое распространение получает торговля компьютерными программами; накопители на гибких магнитных дисках и оптические дисководы с перезаписью создают весьма благоприятные условия для широкомасштабного копирования информации ПК.

**Угрозы информации в персональных ЭВМ.**

Группу угроз, в которых основным средством несанкционированного получения информации является человек, составляют:
1. хищение носителей информации (магнитных дисков, распечаток и т. д.);
2.чтение или фотографирование информации с экрана;
3.чтение или фотографирование информации с распечаток.

В группе угроз, основным средством использования которых служит аппаратура, выделяют:
1.подключение к устройствам ПК специальной аппаратуры, с помощью которой можно уничтожать или регистрировать защищаемую информацию;
2.регистрацию с помощью специальных средств электромагнитных излучений устройств ПК в процессе обработки" защищаемой информации.

Третью группу угроз (основное средство использования которых — программы) образуют:
1.программный несанкционированный доступ к информации;
2.уничтожение (искажение) или регистрация защищаемой информации с помощью программных закладок или ловушек;
3.чтение остаточной информации из ОЗУ;
4.программное копирование информации с магнитных носителей.

**Обеспечение целостности информации в ПК.**

Актуальность данного вида защиты информации в ПК носит общий характер независимо от того, какая информация обрабатывается, поэтому знания и навыки обеспечения целостности необходимы всем пользователям ПК.

Прежде всего, следует знать и помнить, что угрозы целостности информации в ПК, как и в любой другой автоматизированной системе, могут быть случайными и преднамеренными. Основными разновидностями случайных угроз являются отказы, сбои, ошибки, стихийные бедствия и побочные явления, а конкретными источниками их проявления — технические средства, программы и пользователи. С учетом современного состояния технических и программных средств ПК, а также способов и средств их использования к наиболее реальным угрозам целостности информации случайного характера следует отнести ошибки пользователей. Основными из этих ошибок являются неправильные обращения к серийным компонентам программного обеспечения.

Гораздо большую опасность целостности информации в ПК представляют преднамеренные угрозы, создаваемые людьми в злоумышленных целях. Из преднамеренных угроз наибольшее распространение получили так называемые разрушающие программные средства (РПС): электронные вирусы, черви, троянские кони и др. Они же представляют и наибольшую опасность целостности информации в ПК.

**Физические виды защиты**

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий. Для достижения указанной цели следует применять аппаратуру, проверенную на отсутствие внедренных “закладок”, эксплуатируемую аппаратуру — пломбировать, ремонт аппаратуры производить только с привлечением доверенных специалистов под контролем владельца или сотрудника службы безопасности, исключить какие-либо инициативные переделки введенной в эксплуатацию аппаратуры обслуживающим персоналом или ремонтниками. Особое внимание следует обращать на легко заменяемые элементы.

**Аппаратные виды защиты**

**Аппаратные средства**-это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они препятствуют доступу к информации, в том числе с помощью её маскировки. К аппаратным средствам относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объём и масса, высокая стоимость. К аппаратным средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.

Аппаратные средства защиты информации применяются для решения следующих задач:

* + проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;
	+ выявление каналов утечки информации на разных объектах и в помещениях;
	+ локализация каналов утечки информации;
	+ поиск и обнаружение средств промышленного шпионажа;
	+ противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия.

**Программные виды защиты**

***Программные*** средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

## Программные средства защиты информации

* Встроенные средства защиты информации
* Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.
* Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации.
* Межсетевые экраны (также называемые брандмауэрами или файрволами). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.
* Proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код Java и JavaScript).
* VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

**Организационные методы защиты информации.** Это методы, которые предпринимает тот, кто хранит информацию. Обычно сюда относится работа с сотрудниками и внутренними регламентами компании:

* Подбор надежных и ответственных сотрудников.
* Составление и подписание договоров о неразглашении информации.
* Разграничение уровней доступа для сотрудников, чтобы определенная информация была доступна только узкому кругу лиц.

Организационные средства защиты информации — это почти то же самое, что правовые, только правила работы с информацией устанавливает не страна, а отдельная компания.

Но правовых и организационных мер недостаточно — информация все еще может быть повреждена из-за системных сбоев или похищена теми, кто игнорирует закон и правила компании.

**Законодательные средства** – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений. В настоящее время отношения в сфере информационной безопасности регулируются более чем 80 законами и нормативными документами, иногда достаточно противоречивыми.

К психологическим методам относятся внутренние установки самого человека и их непосредственное изменение и использование. Меры по обеспечению информационной безопасности с позиций «человеческого фактора» можно рассматривать в качестве щита от воровства информации как специфического ресурса, имеющего значительную ценность[3].

Поведение людей как субъектов информационной системы во многом определяется не только их личностными качествами, но и внутренней средой системы, условиями деятельности и другими внешними по отношению к человеку факторами. При определенных условиях каждый человек может быть в той или иной степени «честным». «надежным», «порядочным» и он же, при других условиях, способен проявить противоположные качества.

Это связано с основными проблемами психологии человека и идеологии на уровне государства:

1. Психологически человек не готов различать свое и чужое;
2. В сознании людей закон не воспринимается как объективная реальность;
3. Возможность заработать воспринимается людьми как возможность украсть;
4. Наличие отраслей, в которых воровство традиционно негласно входит в систему оплаты труда.