АРХАНГЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ АРХАНГЕЛЬСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное образовательное учреждение
Архангельской области «Архангельский государственный многопрофильный колледж»

ЕН.02 ИНФОРМАТИКА И ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ
ТЕМА 01. ВВЕДЕНИЕ: ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ПОНЯТИЕ ИНФОРМАЦИИ. ЗАЩИТА ИНФОРМАЦИИ.

Информатика - наука, изучающая технологию сбора, хранения и переработки информации с помощью электронно-вычислительных машин (ЭВМ).

Термин «ИНФОРМАЦИЯ» происходит от латинского informatio, что означает разъяснение, осведомление, изложение. Понятие «ИНФОРМАЦИЯ» многозначно, и поэтому строгого определения быть не может.

Информация – сведения об объектах и явлениях окружающего мира, их свойствах, параметрах и состояниях, которые уменьшают имеющуюся о них степень неопределенности.

Понятие «ИНФОРМАЦИЯ» обычно предполагает наличие *двух объектов* - ***источника*** информации и ***потребителя*** (приемник, адресат) информации. Информация от источника к приемнику может *передаваться* с помощью ***электрического, светового, звукового сигналов*** и т.д. Информация может *поступать* ***непрерывно***, а может и ***в виде последовательности отдельных сигналов.***

Чтобы информация способствовала принятию на ее основе правильных решений, она должна характеризоваться следующими ***свойствами***:

- ***Достоверность*** (определяется свойством информации отображать реально существующие объекты с необходимой точностью)
- ***Полнота*** (означает, что информация содержит минимальный, но достаточный для принятия правильного решения состав)
- ***Актуальность*** (определяется степенью хранения ценности информации для управления в момент ее использования)
- ***Полезность***
- ***Понятность***
- ***Адекватность*** (определенный уровень соответствия создаваемого с помощью полученной информации образа реальному объекту, процессу, явлению и т.п., что позволяет говорить о возможности уточнения, расширения объема информации, приближения в процессе познания к ее большей достоверности; т.е. односмысленность или однозначность)

Средства вычислительной техники обладают способностью обрабатывать информацию автоматически, без участия человека. Эти средства могут работать с искусственной, абстрактной и даже ложной информацией, не имеющей объективного отражения ни в природе, ни в обществе.

Данные – это информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.

Минимальной единицей информации в компьютере является **1 бит** – информация, определяемая одним из двух возможных значений – 0 или 1.

На практике используется более крупная единица информации – **байт** – это информация, соответствующая ***последовательности из 8 нулей и единиц,*** **1 байт = 8 бит**.

При работе с большими объёмами информации удобнее пользоваться более крупными единицами: в компьютерах IBM PC используются следующие единицы измерения информации:

1 кбайт=1024 байт$\approx 10^3$ байт
1Мбайт$\approx 10^6$ байт
1Гбайт$\approx 10^9$ байт

Примеры:
Объем оперативной памяти современных ПК от 2 Гбайт и выше
Объем CD – R (RW) – 700 - 800 Мбайт
Объем современных винчестеров 500 Гбайт – 8 Тбайт.

Информационная технология (ИТ) — совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления –информационного продукта.

Информация является одним из ценнейших ресурсов общества, следовательно, процесс ее переработки следует понимать как технологию.

Под ***технологией материального производства*** понимают совокупность средств и методов обработки, изготовления, изменения состояния, свойств, формы сырья или материала. Технология изменяет качество или первоначальное состояние материи в целях получения материального продукта.

Рисунок 1. Сравнение технологии материального производства и информационной технологии

Защита информации.

Современный этап развития общества характеризуется возрастающей ролью *информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.* Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности государства.

Правовое регулирование:

• В *статье 24* ***Конституции РФ*** предусмотрена защита некоторой части персональных данных - «1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

• *Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 07.10.2022)* регламентирует юридические вопросы, связанные с авторскими правами на программные продукты и базы данных.

• В *Уголовном кодексе Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 24.09.2022)* имеется ГЛАВА 28. «Преступления в сфере компьютерной информации». Он предусматривает наказания за:

1. Неправомерный доступ к компьютерной информации;
2. Создание, использование и распространение вредоносных компьютерных программ;
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

• В *Федеральном законе от 27.07.2006 №149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации» в ст. 16* говорится, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию прав на доступ к информации.

Также в данном законе говорится об ответственности за нарушение законодательства РФ об информации, информационных технологиях и о защите информации.

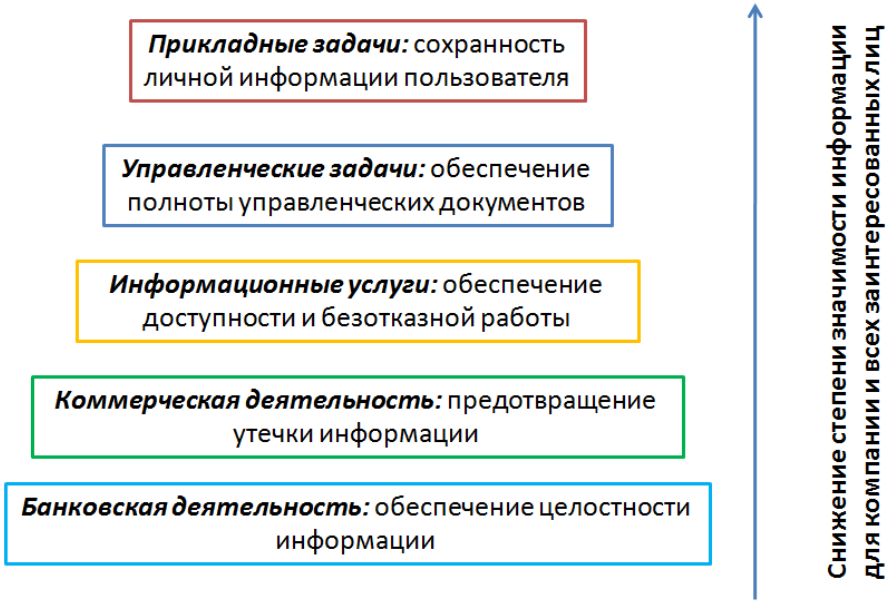

Рисунок 2. Значимость безопасности информации

Под ***информационной безопасностью*** *понимают состояние субъектов РФ в информационной сфере, отражающих совокупность сбалансированных интересов личности, общества и государства.* На уровне отдельной личности предполагается реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также на защиту информации, обеспечивающей личную безопасность. На уровне общества речь идет об обеспечении интересов личности в этой сфере, упрочении демократии, о создании правового социального государства, достижении и поддержании общественного согласия в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения конституционного строя, суверенитета и территориальной целостности России. Информационная безопасность каждого обеспечивает политическую, экономическую и социальную стабильность государства, что сказывается на развитии равноправного и взаимовыгодного международного сотрудничества.

Под ***угрозой безопасности*** *понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов компьютера, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.* Различают *два типа угроз*: случайные (или непреднамеренные) и умышленные. Источником *случайных* ***угроз,*** возникающих при работе компьютера, могут быть ошибки в программном обеспечении, выходы из строя аппаратных средств, неправильные действия пользователей, операторов или системных администраторов и т. п.

Умышленные *угрозы* преследуют определенные цели, связанные с нанесением ущерба пользователям (абонентам) сети. Они также подразделяются на *два типа*: активные и пассивные. При *пассивном* вторжении злоумышленник только наблюдает за прохождением и обработкой информации, не вторгаясь в информационные потоки. Эти вторжения, как правило, направлены на несанкционированное использование информационных ресурсов компьютера, не оказывая при этом влияния на ее функционирование. ***Пассивной угрозой*** является, например, получение информации, передаваемой по каналам связи путем их прослушивания. При этом нарушитель выполняет анализ потока сообщений (трафика), фиксирует идентификаторы, пункты назначений, длину сообщений, частоту и время обменов.

Активные вторжения нарушают нормальное функционирование компьютера, вносят несанкционированные изменения в информационные потоки, в хранимую и обрабатываемую информацию. Эти угрозы реализуются посредством целенаправленного **воздей**ствия на ее аппаратные, программные и информационные ресурсы. К активным вторжениям относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя всей системы,

подключенной к сети, или ее операционной системы, искажение информации **в** пользовательских базах данных или системных структурах данных и т. п. Информация, хранящаяся в памяти компьютера, может быть выборочно модифицирована, уничтожена, к ней могут быть добавлены недостоверные данные.

В общем случае пассивные вторжения легче **предотвратить,** но сложнее выявить, в то время как активные вторжения **легко вы**явить, но сложно предотвратить. Для создания **хорошей защиты** данных компьютера необходимо знать все возможности **активных** и пассивных вторжений и исходя из данных знаний **формировать** средства защиты. Таким образом, первый шаг по организации защиты информации состоит в определении требований к компьютеру. Этот этап включает:

- анализ уязвимых элементов компьютера **(возможные сбои** оборудования и ошибочные операции, выполняемые **пользо**вателями, кража магнитных носителей **и несанкционирован**ное копирование и передача данных**, умышленное искажение** информации или ее уничтожение **и** т. п.);
- оценку угроз (выявление проблем, которые могут возникнуть из-за наличия уязвимых элементов);
- анализ риска (прогнозирование возможных последствий, которые могут вызвать эти проблемы).

Возможные пути вмешательства в чужое информационное пространство могут быть таковы:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- применение подслушивающих устройств;
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- хищение носителей информации и производственных отходов;
- считывание данных в массивах других пользователей;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением средств их защиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- использование программных ловушек;
- использование недостатков систем программирования операционных систем;
- включение в библиотеки программ специальных блоков типа «троянский конь».

Рисунок 3. Методы защиты информации

Техническая система должна обеспечивать защиту ресурсов, прав пользователей компьютера. Линии связи, по которым передаются данные, являются уязвимым компонентом коммуникационных технологий, поэтому они тоже требуют защиты. Программное обеспечение, под управлением которого функционирует компьютер, также должно быть защищено. Поэтому все средства защиты данных компьютера могут быть отнесены к одной из следующих *групп*:

- защита аппаратных составляющих компьютера;
- защита линий связи;
- защита баз данных;
- защита подсистемы управления компьютера.

Под ***системой защиты*** *понимают совокупность средств и технических приемов, обеспечивающих защиту компонентов компьютера, способствующих минимизации риска, которому могут быть подвержены его ресурсы и пользователи.* Они представляют собой комплекс процедурных, логических и физических мер, направленных на предотвращение, выявление и устранение сбоев, отказов и ошибок, несанкционированного доступа в систему.

Существуют различные *механизмы безопасности*:

- шифрование;
- цифровая (электронная) подпись;
- контроль доступа;
- обеспечение целостности данных;
- обеспечение аутентификации;
- подстановка трафика;
- управление маршрутизацией;
- арбитраж (или освидетельствование).

Рисунок 4. Биометрические системы защиты

Защита информации необходима не только от несанкционированного доступа, но и от неумелых действий пользователя либо возможных аппаратных ошибок. При хранении важной информации с использованием одного носителя можно потерять важную информацию. Поэтому необходимо создавать копии данных на различных носителях. В этом случае в качестве минимизации электронного ресурса используют средства архивации. Есть две возможности использования средств архивирования. В одном случае можно воспользоваться служебной программой, встроенной в операционную систему, в другом - специальными программами-архиваторами, основное назначение которых - создание сжатой копии оригинала.