Содержание:

Введение

Факт наличия ценность данных был осознан людьми очень давно – недаром переписка влиятельных личностей издавна была объектом пристального внимания их недругов. Именно в то время возникла задача защиты переписки. Для решения этой задачи использовались самые разнообразные методы, одним из которых была тайнопись – умение составлять сообщения так, чтобы его смысл был доступен только посвященным в тайну. Существуют свидетельства зарождения тайнописи еще в доантичные времена. На протяжении всей своей многовековой истории данный вид искусства служил немногим, в основном верхушке общества, не выходя за пределы резиденций глав государств, посольств и разведывательных миссий. Но несколько десятилетий назад информация приобрела самостоятельную коммерческую ценность и стала широко распространенным товаром, следовательно, ее необходимо защищать. Возникновение индустрии обработки информации с железной необходимостью привело к возникновению индустрии средств защиты информации.

В данной работе рассмотрено само понятие контроля доступа и его основные задачи. Во второй части работы были рассмотрены методы защиты информации. Были рассмотрены основные виды угроз информационной безопасности, а также основные методы борьбы с ними. В качестве основных методов защиты были выделены ограничение доступа, разграничение и контроль доступа, разделение привилегий на доступ, идентификация и установление подлинности объекта, криптографические преобразования информации, а также правовые и организационные методы защиты информации.

1. Доступ к данным

1.1. Контроль доступа

Контроль доступа — функция открытой системы, обеспечивающая технологию безопасности, которая разрешает или запрещает доступ к определённым типам

данных, основанную на идентификации субъекта, которому нужен доступ, и объекта данных, являющегося целью доступа.

Контроль доступа является одним из самых важных элементов защиты ПК и информации на нём. Доступ к защищённой информации должен быть ограничен, чтобы только люди, которые имеют право доступа, могли получать эту информацию. Компьютерные программы и во многих случаях чужеродные компьютеры посредством локальной сети, Интернета, беспроводной сети могут получить секретную информацию, которая не предназначена им. Это может нанести как финансовые, так и информационные потери[1].

В связи с этим необходим механизм контроля доступа к защищённой информации. Сложность механизмов контроля доступа должна быть в паритете с ценностью информации, то есть чем более важной или ценной информация является, тем более сложными должны быть механизмы контроля доступа.

Основными механизмами контроля доступа являются идентификация и аутентификация[2] [1, 3].

1.2. Задачи, решаемые ограничением доступа

1.2.1. Блокирование доступа к настройкам операционной системы

Непродуманные действия начинающих пользователей часто приводят к тем или иным проблемам в работе отдельных приложений или операционной системы. Как показывает практика, для немалой категории пользователей лучше вообще запретить всё, что только можно запретить, иначе ни о какой стабильной работе на компьютере не может быть и речи. И это понятно, ведь достаточно всего лишь случайно удалить, например, драйвер монитора, как изображение на экране перестанет радовать глаз. Если же удалить принтер, то печать документов станет невозможной, а при изменении сетевых настроек компьютер перестанет работать в локальной сети и т.п. Для предотвращения подобных ситуаций необходимо блокировать все действия пользователя, которые могут повлечь за собой неработоспособность компьютера[3].

Кроме того, имеется немало настроек, изменение которых не имеет столь неприятных последствий, но вызывает определенные неудобства у других пользователей. К таким настройкам относятся, в частности, параметры свойств экрана, способ отображения файлов и папок, наличие определенных ярлыков на рабочем столе и в меню «Пуск», внешний вид стандартных папок и ярлыков и т.п. Наибольшее число проблем такие, казалось бы, неопасные на первый взгляд изменения вызывают в учебных заведениях, где учащиеся и студенты считают своим долгом настроить компьютер экстраординарным образом, нимало не заботясь о том, что, например, экстравагантное оформление экрана может вызывать у других пользователей утомление и головную боль, а измененный вид папок «Мой компьютер», «Корзина» и пр. потребует у них много времени на поиск и открытие. В итоге получается, что для пользы дела приходиться блокировать возможность подобных изменений настроек, ибо в противном случае о плодотворном образовательном процессе довольно быстро придется забыть[4].

Ограничив доступ разумными рамками, можно предотвратить совершение пользователями таких действий, которые так или иначе могут привести к нестабильности работы системы или к неудобству выполнения тех или иных операций[5] [2, 4, 6].

1.2.2. Защита файлов и папок операционной системы и установленных приложений

Нередко бывает, что недостаточно подготовленные пользователи умудряются в мгновение ока удалить с компьютера папки с файлами операционной системы или какого-либо приложения, или, что еще хуже, переместить их в неизвестное место, не заметив при этом даже названия удаляемой или перемещаемой папки. Часто это имеет место в учебных учреждениях, особенно при изучении тем работы с файловой системой в среде Windows или в файловых менеджерах. Результат оказывается плачевным, так как далеко не всегда юных экспериментаторов удается вычислить до момента очистки корзины, и в итоге немало времени уходит на восстановление информации. С перемещением еще хуже, ведь вначале приходится опытным путем выяснять, что же все-таки было перемещено, а затем искать соответствующие папки по всему диску и возвращать их на место[6].

Конечно, информацию в обоих случаях чаще всего удается восстановить, но это требует спокойной обстановки и немалого времени. Поэтому гораздо разумнее при помощи соответствующих утилит настроить параметры так, чтобы, например,

папки с конкретными приложениями были недоступны, но в то же время сами приложения можно было запускать[7] [4, 6].

1.2.3. Контроль за использованием приложений и ограничение времени доступа

Необходимость такого контроля и ограничений по времени, как правило, возникает в учебных учреждениях, когда необходимо ограничить студентов перечнем изучаемых по программе программных продуктов, и на домашних компьютерах при доступе к ним детей, чтобы регулировать перечень допустимых приложений и время сидения ребенка за компьютером[8].

Самое простое для решения данной проблемы — воспользоваться специализированной утилитой, которая позволит четко определить, какие программы и в какое время можно запускать, а какие — нельзя никогда и ни при каких обстоятельствах[9] [1, 3].

1.2.4. Защита персональных данных

Проблема защиты персональных файлов и папок неизбежна, если за компьютером работает несколько человек. Такая ситуация может возникнуть дома, например, при необходимости оградить ребенка от непредназначенной ему информации, а может и на работе, где даже при наличии у каждого пользователя собственного компьютера возможны моменты, когда приходится пускать за свой ПК другого сотрудника. В обоих случаях совсем не хочется демонстрировать посторонним какие-то свои рабочие материалы, и вовсе не потому, что они имеют гриф «совершенно секретно», а просто потому, что никто не любит вмешательства посторонних в свои дела[10].

Есть и более важная сторона вопроса. Всегда ли вы можете спокойно доверить свои материалы кому бы то ни было? Скорее всего, нет, ведь совсем не исключено, что ваши файлы и папки могут оказаться удаленными или измененными неподготовленным пользователем по чистой случайности. А заблокировав доступ к ним, вы можете не переживать, что с вашими документами что-либо случится по вине постороннего[11].

Кроме того, не стоит сбрасывать со счетов и то, что, если ваши материалы представляют какую-то коммерческую ценность, не исключена ситуация, что ими

захотят воспользоваться в неблаговидных целях[12].

Все эти проблемы исключаются путем создания секретных папок или даже секретных дисков с персональной информацией, которые, в зависимости от варианта ограничения доступа и от выбранного приложения, могут быть как полностью скрытыми от других пользователей, так и видимыми, но недоступными для них. В обоих случаях другие пользователи без знания вашего пароля не смогут получить доступ к данным материалам, изменить или удалить их[13] [1, 4, 6, 7].

1.2.5. Блокирование доступа к компьютеру

При работе в офисе даже при наличии собственного компьютера пользователи не в состоянии находиться рядом с компьютером постоянно, и потому нередки ситуации, когда включенный компьютер оказывается без присмотра. К сожалению, такими моментами могут воспользоваться заинтересованные в ваших материалах сотрудники[14].

Первый приходящий в голову способ обезопасить себя от таких незваных гостей — установить пароль на заставку, но это совсем не лучший вариант, так как при перезагрузке пароль с заставки можно снять без особых проблем. Гораздо надежнее — полностью заблокировать компьютер при помощи специальных программных средств, которые никого (а иногда даже администратора) не подпустят к компьютеру без знания пароля даже при перезагрузке Windows в безопасном режиме[15] [4, 7].

1.2.6. Блокирование доступа к устройствам

Встроенные механизмы распределения прав доступа и задания политик безопасности в ОС семейства Windows не позволяют контролировать доступ к потенциально опасным устройствам: дисководам и CD-ROM, а также к FireWire и инфракрасным портам, к WiFi- и Bluetooth-адаптерам и пр. В то же время использование неавторизованных устройств представляет немалую угрозу безопасности данных. С одной стороны, данные могут быть похищены, ведь при открытом доступе нет никакой сложности в том, чтобы записать информацию на внешний носитель, а с другой — данные на компьютере могут быть видоизменены. Вариантов тут много. Например, сетевые и локальные компьютеры часто страдают от вирусов, троянов и других вредоносных программ, нередко заносимых со

сменных носителей. Не менее неприятна ситуация бесконтрольной установки ПО [16].

Конечно, можно целиком отключить устройства в BIOS на каждом компьютере, но это не выход, ибо данная операция требует массу времени и в случае необходимости работы с устройством придется каждый раз обращаться в BIOS и вновь включать это устройство. И здесь гораздо важнее контролировать доступ к устройствам, введя разумные ограничения в зависимости от конкретной ситуации. Можно, например, установить доступ «Только чтение» для части сменных носителей и ограничить установку с них ненужных программ[17] [3, 8].

2. Методы защиты информации

2.1. Угрозы безопасности

С позиции обеспечения безопасности информации в компьютерных системах такие системы целесообразно рассматривать в виде единства трех компонент, которые оказывают взаимное влияние друг друга.

Схема данных компонент представлена на рисунке 1.

Рис. 1. Компоненты компьютерных систем

Целью создания любой компьютерной системы является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности[18].

Под угрозой безопасности информации понимается потенциально возможное явление, процесс или событие, имеющие возможность привести к уничтожению, утрате доступности, конфиденциальности или целостности информации.

Схематически классификация угроз безопасности информации представлена на рисунке 2.

Рис. 2. Угрозы безопасности информации в компьютерных системах

Угрозы, не связанные с преднамеренными действиями злоумышленников и реализующиеся в случайные моменты времени, называют случайными или непреднамеренными[19] [2].

2.2. Методы защиты информации

При наличии простых средств хранения и передачи информации существовали и до сих пор не потеряли значения такие методы ее защиты от преднамеренного доступа, как:

- ограничение доступа;

- разграничение доступа;
- разделение привилегий на доступ;
- криптографическое преобразование информации;
- учет и контроль доступа;
- законодательные меры[20].

С увеличением объемов и количества пользователей, а также в связи с другими причинами повышается вероятность преднамеренного несанкционированного доступа. Вследствие этого развиваются старые и возникают новые дополнительные методы защиты информации в вычислительных системах:

- методы функционального контроля, обеспечивающие диагностику и обнаружение отказов, сбоев аппаратуры и ошибок человека, а также программные ошибки;
- методы повышения достоверности информации;
- методы защиты информации от аварийных ситуаций;
- методы контроля доступа к внутреннему монтажу аппаратуры, линиям связи;
- методы контроля и разграничения доступа к информации;
- методы аутентификации и идентификации пользователей, носителей информации, технических средств и документов;
- методы защиты от наводок информации и побочного излучения[21] [1, 5].

2.2.1.Ограничение доступа

Ограничение доступа заключается в создании некоторой физически замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, которые связаны с объектом защиты по своим функциональным обязанностям. Ограничение доступа к комплексам средств автоматизации обработки информации заключается:

- в выделении специальной территории для размещения комплекса средств автоматизации;
- в сооружении по периметру зоны специальных ограждений с охранной сигнализацией;
- в выделении специальных помещений в здании;
- в создании контрольно-пропускного режима в помещениях, зданиях и на территории[22].

Задачей средств ограничения доступа является исключение случайного и преднамеренного доступа посторонних лиц на территорию размещения комплекса и непосредственно к аппаратуре. В указанных целях создается защитный контур, которые замыкается двумя видами преград: контрольно-пропускной и физической. Такие преграды часто называют системой охранной сигнализации и системой контроля доступа[23] [7, 8].

2.2.2.Разграничение и контроль доступа

Разграничение и контроль доступа к информации в вычислительной системе заключается в разделении циркулирующей в ней информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

Задачей разграничения доступа является сокращение количества должностных лиц, которые не имеют к ней отношения при выполнении своих функций, то есть защита информации от нарушителя среди допущенного к ней персонала. При этом деление информации может производиться по степени секретности, важности, по документам, по функциональному назначению и по другим подобным пунктам[24] [2].

2.2.3.Разделение привилегий на доступ

Разделение привилегий на доступ к информации заключается в выделении группы из числа допущенных к информации должностных лиц. Данной группе предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

Подобный метод несколько усложняет процедуру, но обладает высокой эффективностью защиты. На его принципах можно организовать доступ к данным с санкции вышестоящего лица по запросу или без него[25] [5].

2.2.4.Идентификация и установление подлинности объекта.

Идентификация в вычислительных системах представляет собой процедуру выявления идентификатора для субъекта идентификации, однозначно идентифицируя данного субъекта в вычислительной системе. При выполнении

процедуры идентификации в вычислительной системе субъекту предварительно назначается соответствующий идентификатор.

Идентификатором установления подлинности личности в повседневной жизни является внешний вид: форма головы, фигура, характер, черты лица, поведение, привычки и другие свойственные данному человеку признаки, создающие образ конкретной личности. Объектами идентификации и установления подлинности в вычислительной системе могут быть человек, техническое средство, документ, носитель информации или сама информация[26].

В системах защиты после процедуры идентификации чаще всего следует аутентификация, подтверждающая идентификацию субъекта. При этом достоверность идентификации полностью определяется уровнем достоверности выполненной процедуры аутентификации.

Конечной целью идентификации и установления подлинности объекта в вычислительной системе является допуск объекта к информации ограниченного пользования в случае положительного исхода проверки, или отказ в допуске в случае отрицательного исхода проверки[27].

В любой системе аутентификации обычно можно выделить такие элементы, как субъект, проходящий процедуру; отличительную черту субъекта; хозяина системы аутентификации, несущего ответственность и контролирующего ее работу; сам механизм аутентификации и механизм, который предоставляет определенные права доступа или лишает субъекта данных прав.

Существует 3 фактора аутентификации: что-то, что мы знаем; что-то, что мы имеем; что-то, что является частью нас. «Что-то, что мы знаем» является паролем, представляющим собой некоторые тайные сведения, которыми должен обладать только авторизованный субъект. Паролем обычно представляет собой текстовое слово, речевое слово, комбинацию для замка или личный идентификационный номер. «Что-то, что мы имеем» является устройством аутентификации, представляющим собой неповторимый предмет, которым обладает субъект. Неповторимый предмет обычно представляет собой ключ от замка, личную печать, файл данных для компьютера. «Что-то, что является частью нас» является биометрикой, которая представляет собой физическую особенность субъекта. Особенность обычно представляет собой отпечаток пальца или ладони, портрет, голос или особенность глаза[28].

Установление подлинности может происходить по электронной цифровой подписи, многоразовым или одноразовым паролям, с помощью SMS, на основе биометрических параметров человека или через географическое местоположение.

Использование многоразового пароля является наиболее распространенным способом защиты. Простая аутентификация имеет следующий общий алгоритм: субъект запрашивает доступ в систему и вводит личный идентификатор и пароль, введенные неповторимые данные поступают на сервер аутентификации для сравнения с эталонными, при совпадении данных с эталонными аутентификация признается успешной, при различии — субъект перемещается к первому шагу. Пароль может передаваться в сети незашифрованным способом или с использованием шифрования SSL или TLS. Для защиты пароля часто в базе может храниться только хеш-функция эталонного пароля, с которой сравнивается полученная с введенного пароля хеш-функция. При однократном получении многоразового пароля, злоумышленник получает постоянный доступ ко всем защищенным данным. Для предотвращения этого используются одноразовые пароли, каждый раз генерируемые заново. При использовании SMS пользователь получает одноразовый пароль посредством сообщения. При биометрической идентификации установление подлинности происходит при считывании биометрики, которая обычно представляет собой отпечаток пальца или ладони, портрет, голос или особенность глаза[29] [1, 3, 7].

2.2.5. Криптографические преобразования информации

Искусство и наука защиты сообщений называются криптографией, а специалисты, занимающиеся ей - криптографами. Криптографическая защита информации представляет собой преобразование исходной информации с целью ее недоступности для использования или ознакомления лицами, которые не имеют на это полномочий.

Процесс маскировки сообщения способом, который позволяет скрыть его суть, называется зашифрованием. Процедура обратного превращения называется дешифрованием. В процессе дешифровки на основе ключа шифрованный текст преобразуется в исходный, называемый открытым текстом[30].

Процесс зашифрования и расшифрования представлен на рисунке 3.

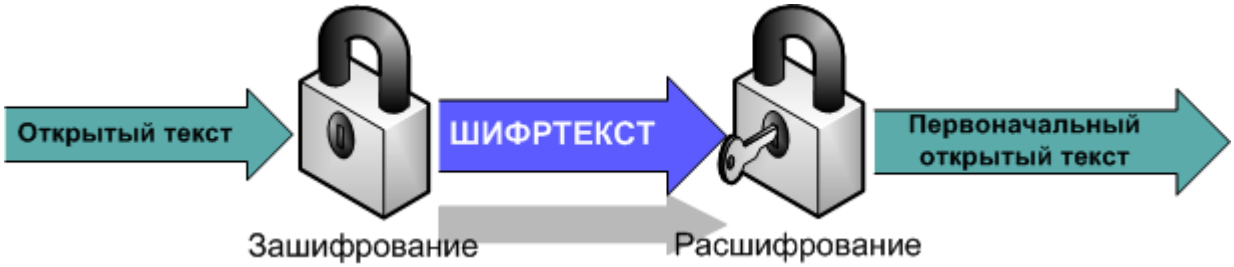

Рис. 3. Последовательность зашифрования и расшифрования

Криптосистемы разделяются на симметричные и с открытым ключом. В симметричных криптосистемах для шифрования и для расшифрования используется один и тот же ключ.

В системах с открытым ключом используются открытый и закрытый, ключи, математически связанные друг с другом. Информация шифруется с помощью открытого ключа, доступного всем желающим, а расшифровывается с помощью закрытого ключа, который известен только получателю сообщения[31].

Электронная цифровая подпись является присоединяемым к тексту его криптографическим преобразованием, позволяющим при получении текста другим пользователем проверить подлинность сообщения и авторство. Электронная цифровая подпись получается в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяет проверить отсутствие искажения информации в электронном документе с момента формирования подписи, принадлежность подписи владельцу сертификата ключа подписи, а в случае успешной проверки подтвердить факт подписания электронного документа[32].

Электронная подпись предназначена для определения лица, которое подписало электронный документ, и является аналогом собственноручной подписи в предусмотренных законом случаях. Электронная подпись применяется при оказании государственных и муниципальных услуг, совершении гражданско-правовых сделок, исполнении муниципальных и государственных функций, при совершении иных юридически значимых действий.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы[33].

Данные группы представлены на рисунке 4.

Рис. 4. Методы криптографического преобразования информации

Все традиционные криптографические системы можно подразделить на:

1. Шифры перестановки, к которым относятся:
    1. Шифр перестановки "скитала".
    2. Шифрующие таблицы.
    3. Применение магических квадратов.
2. Шифры простой замены, к которым относятся:
    1. Полибианский квадрат.
    2. Система шифрования Цезаря.
    3. Аффинная система подстановок Цезаря.
    4. Система Цезаря с ключевым словом.
    5. Шифрующие таблицы Трисемуса.
    6. Биграммный шифр Плейфейра.
    7. Криптосистема Хилла.
    8. Система омофонов.
3. Шифры сложной замены, к которым относятся:
    1. Шифр Гронсфельда.
    2. Система шифрования Вижинера.
    3. Шифр "двойной квадрат" Уитстона.
    4. Одноразовая система шифрования.
    5. Шифрование методом Вернама.
    6. Роторные машины.
4. Шифрование методом гаммирования.
5. Шифрование, основанное на аналитических преобразованиях шифруемых данных[34] [4, 8].

2.2.6. Правовые и организационные методы защиты информации в компьютерных системах

Государство должно обеспечить в стране защиту информации, как в масштабах всего государства, так и на уровне организаций и отдельных граждан. Для решения этой проблемы государство обязано:

1. выработать государственную политику безопасности в области информационных технологий;
2. законодательно определить правовой статус информации, систем защиты информации, компьютерных систем, пользователей и владельцев информации и других подобных понятий;
3. создать иерархическую структуру государственных органов, которые вырабатывают и проводят в жизнь политику безопасности информационных технологий;
4. создать систему стандартизации, лицензирования и сертификации в области защиты информации;
5. обеспечить приоритетное развитие отечественных защищенных информационных технологий;
6. повышать уровень образования граждан в области информационных технологий, воспитывать у них бдительность и патриотизм;
7. установить ответственность граждан за нарушения законодательства в области информационных технологий[35].

Стандарты в структуре информационной безопасности выступают как связующее звено между концептуальной и технической стороной вопроса. В этих стандартах косвенно затрагиваются правовые вопросы – такие, как «защита жизненно важных интересов личности».

Для обеспечения совместимости аппаратно-программных систем и их компонентов за основу российских стандартов информационной безопасности был взят стандарт США – так называемая «Оранжевая книга». Эта «оранжевая революция» в информационных технологиях и привела к тому, что правовую базу пришлось так или иначе подтягивать к стандартам. Возникают определенные трудности с пониманием вопроса, тем более что количество стандартов и спецификаций в области информационной безопасности весьма велико[36].

Чтобы разобраться в вопросах применения российских стандартов, необходимо представить себе административно-правовую структуру государственных органов, которые обеспечивают информационную безопасность, и понять занимаемое ими место. Данная структура показана на рисунке 5. Из нее видно, что стандарты относятся к специальным нормативным документам по технической защите

информации и находятся в определенном логическом соответствии с организационно-распорядительными и правовыми документами[37].

Конфиденциальной информацией называют документированную информацию, ограниченную в доступе в соответствии с законодательством РФ. Конфиденциальная информация может быть личной, коммерческой, служебной, производственной, профессиональной, судебно-следственной[38].

К конфиденциальной личной информации относится информация, которая содержит персональные данные, такие как сведения об обстоятельствах, событиях

гь его

ствах

Рис. 5.

Административно-правовая структура государственных органов, обеспечивающих информационную безопасность

Требование конфиденциальности персональных данных раскрывается в Федеральном законе «О персональных данных». Согласно п. 10 ст. 3 этого Закона конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных

данных или наличия иного законного основания.

В РФ защита персональных данных сводится к созданию режима обработки персональных данных, которые включает создание внутренней документации, создание организационной системы защиты, внедрение технических мер защиты, получение лицензий и сертификатов регулирующих органов[40] [1, 2, 9].

Заключение

Понятие контроля доступа обозначает функцию открытой системы, обеспечивающую технологию безопасности, которая разрешает или запрещает доступ к определённым типам данных, основанную на идентификации субъекта, которому нужен доступ, и объекта данных, являющегося целью доступа

В данной работе рассмотрены такие задачи контроля доступа, как блокирование доступа к настройкам информационной системы, защита файлов и папок операционной системы и установленных приложений, контроль за использованием приложений и ограничение времени доступа, защита персональных данных, блокирование доступа к компьютеру и блокирование доступа к устройствам.

Во второй части работы были рассмотрены современные методы защиты информации в вычислительных системах. Были рассмотрены угрозы информационной безопасности, разделенные на случайные и преднамеренные, а также выделены основные методы борьбы с ними. В качестве случайных угроз были выделены стихийные бедствия и аварии, сбои и отказы технических средств, ошибки при разработке компьютерных систем, алгоритмические и программные ошибки и ошибки пользователей и компьютерного персонала. В качестве преднамеренных угроз были выделены традиционный шпионаж и диверсии, несанкционированный доступ к информации, электромагнитные излучения и наводки, несанкционированная модификация структур и вредительские программы.

В качестве основных методов защиты были выделены ограничение доступа, разграничение и контроль доступа, разделение привилегий на доступ, идентификация и установление подлинности объекта, криптографические преобразования информации, а также правовые и организационные методы защиты информации.

Список используемой литературы

1. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с.
2. Зегжда Д.П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2010. – 452 с.
3. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие / А. Ю. Зубов. – М.: Гелиос АРВ, 2012. – 192 с.
4. Левин В. И. Все об информации / В. И. Левин. – М.: ООО «Издательство «РОСМЭН-ПРЕСС», 2005. – 384 с.
5. Леонтьев В. П. Новейшая энциклопедия персонального компьютера / В. П. Леонтьев. – М.: ОЛМА-ПРЕСС Образование, 2010. – 734 с.
6. Макарова Н. В. Информатика: Учебник / Н. В. Макарова. – М.: Финансы и статистика, 2007. – 768 с.
7. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика, Электронинформ, 2007. – 368 с.
8. Правовое обеспечение информационной безопасности: Учебное пособие для студентов высших учебных заведений / С. Я. Казанцев и др. – М.: Издательский центр «Академия», 2005. – 240 с.
9. Хургин В. Об определении понятия «информация» / В. Хургин // Информационные Ресурсы России. – 2007. – № 3. – С. 26-35.

1. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие / А. Ю. Зубов. – М.: Гелиос АРВ, 2012. – 192 с. ↑

2. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с. ↑

3. Макарова Н. В. Информатика: Учебник / Н. В. Макарова. – М.: Финансы и статистика, 2007. – 768 с. ↑

4. Левин В. И. Все об информации / В. И. Левин. – М.: ООО «Издательство «РОСМЭН-ПРЕСС», 2005. – 384 с. ↑

5. Зегжда Д.П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2010. – 452 с. ↑

6. Макарова Н. В. Информатика: Учебник / Н. В. Макарова. – М.: Финансы и статистика, 2007. – 768 с. ↑

7. Левин В. И. Все об информации / В. И. Левин. – М.: ООО «Издательство «РОСМЭН-ПРЕСС», 2005. – 384 с. ↑

8. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с. ↑

9. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие / А. Ю. Зубов. – М.: Гелиос АРВ, 2012. – 192 с. ↑

10. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика, Электронинформ, 2007. – 368 с. ↑

11. Левин В. И. Все об информации / В. И. Левин. – М.: ООО «Издательство «РОСМЭН-ПРЕСС», 2005. – 384 с. ↑

12. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с. ↑

13. Макарова Н. В. Информатика: Учебник / Н. В. Макарова. – М.: Финансы и статистика, 2007. – 768 с. ↑

14. Левин В. И. Все об информации / В. И. Левин. – М.: ООО «Издательство «РОСМЭН-ПРЕСС», 2005. – 384 с. ↑

15. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика, Электронинформ, 2007. – 368 с. ↑

16. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие / А. Ю. Зубов. – М.: Гелиос АРВ, 2012. – 192 с. ↑

17. Правовое обеспечение информационной безопасности: Учебное пособие для студентов высших учебных заведений / С. Я. Казанцев и др. – М.: Издательский центр «Академия», 2005. – 240 с. ↑

18. Зегжда Д.П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2010. – 452 с. ↑

19. Зегжда Д.П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2010. – 452 с. ↑

20. Леонтьев В. П. Новейшая энциклопедия персонального компьютера / В. П. Леонтьев. – М.: ОЛМА-ПРЕСС Образование, 2010. – 734 с. ↑

21. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с. ↑

22. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика, Электронинформ, 2007. – 368 с. ↑

23. Правовое обеспечение информационной безопасности: Учебное пособие для студентов высших учебных заведений / С. Я. Казанцев и др. – М.: Издательский центр «Академия», 2005. – 240 с. ↑

24. Зегжда Д.П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2010. – 452 с. ↑

25. Леонтьев В. П. Новейшая энциклопедия персонального компьютера / В. П. Леонтьев. – М.: ОЛМА-ПРЕСС Образование, 2010. – 734 с. ↑

26. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с. ↑

27. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие / А. Ю. Зубов. – М.: Гелиос АРВ, 2012. – 192 с. ↑

28. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с. ↑

29. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика, Электронинформ, 2007. – 368 с. ↑

30. Левин В. И. Все об информации / В. И. Левин. – М.: ООО «Издательство «РОСМЭН-ПРЕСС», 2005. – 384 с. ↑

31. Правовое обеспечение информационной безопасности: Учебное пособие для студентов высших учебных заведений / С. Я. Казанцев и др. – М.: Издательский центр «Академия», 2005. – 240 с. ↑

32. Левин В. И. Все об информации / В. И. Левин. – М.: ООО «Издательство «РОСМЭН-ПРЕСС», 2005. – 384 с. ↑

33. Правовое обеспечение информационной безопасности: Учебное пособие для студентов высших учебных заведений / С. Я. Казанцев и др. – М.: Издательский центр «Академия», 2005. – 240 с. ↑

34. Левин В. И. Все об информации / В. И. Левин. – М.: ООО «Издательство «РОСМЭН-ПРЕСС», 2005. – 384 с. ↑

35. Зегжда Д.П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2010. – 452 с. ↑

36. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с. ↑

37. Хургин В. Об определении понятия «информация» / В. Хургин // Информационные Ресурсы России. – 2007. – № 3. – С. 26-35. ↑

38. Хургин В. Об определении понятия «информация» / В. Хургин // Информационные Ресурсы России. – 2007. – № 3. – С. 26-35. ↑

39. Зегжда Д.П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2010. – 452 с. ↑

40. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2011. – 264 с. ↑