МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ОБРАЗОВАНИЮ

МОГИЛЕВСКОГО ОБЛАСТНОГО ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«МОГИЛЕВСКИЙ ГОСУДАРСТВЕННЫЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

**ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

ДОМАШНЯЯ КОНТРОЛЬНАЯ РАБОТА

Выполнил Учащийся группы ПО-455

О.И. Любаль

Шифр 14

2023

# 5 Приведите классификацию средств защиты информации.

Средство защиты информации: техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Для организации защиты информации в компьютерных сетях важным вопросом является классификация методов и средств защиты, которые позволяют воспрепятствовать ее использованию. В Приложении Г показана схема наиболее часто используемых методов защиты информации в компьютерных сетях и средств, с помощью которых они могут быть реализованы.

Методами обеспечения защиты информации являются следующие: регламентация, препятствие, маскировка информации, противодействие вирусам, управление доступом, принуждение и побуждение.

Препятствие - это метод, при котором пути злоумышленнику к защищаемой информации преграждаются физически, например, к аппаратуре, носителям информации и т.п.

Регламентация заключается в реализации системы организационных мероприятий, которые определяют все стороны процесса обработки информации. Этот метод создает такие условия автоматизированной обработки, передачи и хранения информации, при которых возможность несанкционированного доступа к ней сводится к минимуму.

Управление доступом - этот метод защиты информации регулирует использование всех ресурсов автоматизированной информационной системы организации (технические, программные, временные и др.) и включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов информационной системы, то есть присваивает каждому объекту персональный идентификатор;

- аутентификацию, то есть устанавливает подлинность объекта или субъекта по предъявленному им идентификатору;

- регистрацию или, говоря другими словами, протоколирование обращений к защищаемым ресурсам;

- проверку полномочий, таких как проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур в соответствии с установленным регламентом;

- разрешение и создание условий работы в пределах установленного регламента;

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

Маскировка информации - метод защиты информации путем ее криптографического закрытия. Механизмы шифрования все шире применяются при обработке и хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности только этот метод является единственно надежным.

Противодействие вирусам (или атакам вредоносных программ) предполагает комплексное использование организационных мер и антивирусных программ. Целью принимаемых мер является уменьшение вероятности инфицирования информационно-вычислительной системы, уменьшение последствий информационных инфекций, локализация или уничтожение вирусов, восстановление информации.

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

Побуждение - такой метод защиты информации, который за счет соблюдения сложившихся моральных и этических норм побуждает пользователей системы не нарушать установленные правила.

Указанные методы обеспечения информационной безопасности реализуются на практике применением различных механизмов защиты, для создания которых используются следующие основные средства: физические, аппаратные, программные, аппаратно-программные, организационные, морально-этические и законодательные.

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и включают в себя разнообразные инженерные устройства и сооружения, которые препятствуют проникновению злоумышленников на объекты защиты. Примером физических средств могут служить замки на дверях, средства электронной охранной сигнализации, решетки на окнах и т.д.

Аппаратные средства защиты - это электронные, электромеханические и другие устройства, непосредственно встроенные в вычислительную технику или самостоятельные устройства, которые сопрягаются с ней по стандартному интерфейсу. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д. Такие средства принадлежат к наиболее защищенной части системы. Если есть выбор, то предпочтение следует отдавать аппаратным средствам защиты, так как они исключают вмешательство в их работу непосредственно из сети. Еще одно преимущество аппаратных средств - это их большая производительность по сравнению с программными средствами защиты, особенно, при использовании их в устройствах криптографической защиты.

Недостатком аппаратных средств является их высокая стоимость.

Программные средства защиты - это специальные программы и программные комплексы, предназначенные для защиты информации. Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Основной их недостаток - это доступность для хакеров, особенно это касается широко распространенных на рынке средств защиты.

Программные средства часто делят на средства, которые реализуются в стандартных операционных системах (ОС) и в специализированных информационных системах.

Криптографические программы основаны на использовании методов шифрования (кодирования) информации. Такие методы очень надежны и значительно повышают безопасность передачи информации в сетях.

Аппаратно-программные средства защиты - средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы. Они совмещают высокую производительность аппаратно реализованных систем и гибкость настройки программных. В качестве примера такого устройства можно привести маршрутизаторы фирмы Cisco, которые допускают их настройку в качестве пакетных фильтров.

Организационные средства - это действия общего характера, предпринимаемые руководством организации. Они регламентируют процессы функционирования и использование ресурсов системы обработки данных, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности, а в случае их реализации снизить размер потерь.

Организационные меры включают в себя:

- мероприятия, осуществляемые при подборе и подготовке персонала;

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании сетей;

- организацию охраны и надежного пропускного режима; разработку политики безопасности;

- распределение реквизитов разграничения доступа; организацию учета, хранения, использования и уничтожения документов и носителей с информацией;

- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

Организационные меры играют важную роль в обеспечении безопасности компьютерных систем. Когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности, организационные меры - это единственное, что остается. Но это не означает, что систему защиты необходимо строить исключительно на их основе, так как этим мерам присущи и серьезные недостатки, такие как:

- низкая надежность без соответствующей поддержки физическими, техническими и программными средствами;

- дополнительные неудобства, связанные с большим объемом формальной и рутинной деятельности.

Организационные меры нужны для того, чтобы обеспечить эффективное применение других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными техническими и физическими средствами.

Законодательные средства - действующие в стране законы, указы и другие нормативно-правовые акты, которые регламентируют правила обращения с информацией, закрепляют права и обязанности участников информационных отношений, а также устанавливают ответственность за нарушение этих правил. Правовые меры защиты носят преимущественно упреждающий, профилактический характер. Основной целью их является предупреждение и сдерживание потенциальных нарушителей.

Морально-этические средства - всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации. Морально-этические нормы могут быть как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и оформленные в некоторый свод правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей.

Законодательные и морально-этические меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение. Они являются универсальными, так как могут применяться для всех каналов проникновения и НСД к информации. В некоторых случаях они могут быть единственно применимыми, как например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

Все рассмотренные средства защиты разделяются на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяемые целенаправленной деятельностью человека либо регламентирующие эту деятельность).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Надежная и безопасная система защиты должна соответствовать следующим требованиям:

- стоимость средств защиты должна быть меньше, чем размеры возможного ущерба;

- каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы;

- защита тем более эффективна, чем проще пользователю с ней работать;

- возможность отключения в экстренных случаях;

- специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать;

- под защитой должна находиться вся система обработки информации;

- разработчики системы защиты, не должны быть в числе тех, кого эта система будет контролировать;

- система защиты должна предоставлять доказательства корректности своей работы;

- лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность;

- объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других;

- надежная система защиты должна быть полностью протестирована и согласована;

- защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора;

- система защиты должна разрабатываться, исходя из предположения, что пользователи будут совершать серьезные ошибки и, вообще, имеют наихудшие намерения;

- наиболее важные и критические решения должны приниматься человеком;

- существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

Выводы. У специалистов по защите информации имеется широкий спектр защитных мер: законодательных, морально-этических, административных (организационных), физических и технических (аппаратно-программных) средств. Все эти средства обладают своими достоинствами и недостатками, которые необходимо правильно учитывать при создании систем защиты.

Все известные каналы проникновения и утечки информации должны быть перекрыты с учетом анализа риска, вероятностей реализации угроз безопасности в конкретной прикладной системе и обоснованного рационального уровня затрат на защиту.

Наилучшие результаты достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании определенных совокупностей различных мер защиты на всех этапах жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

# 41 Дайте понятие термину «Компьютерный вирус».

Компью́терный ви́рус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами.

Вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы, особенно вирусы майнинга.

В обиходе «вирусами» называют все вредоносные программы, хотя на самом деле это лишь один из их видов.

Ныне существует разные виды компьютерных вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через локальные и глобальные сети (Интернет). Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы

• по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);

• файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.

• по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);

• по используемым технологиям (полиморфные вирусы, стелс-вирусы, руткиты);

• по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);

• по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

• Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение: вписывая себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск через реестр и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды, — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплойтом, использующим уязвимость.

• После того как вирус успешно внедрился в коды программы, файла или документа, он будет находиться в состоянии сна, пока обстоятельства не заставят компьютер или устройство выполнить его код. Чтобы вирус заразил ваш компьютер, необходимо запустить заражённую программу, которая, в свою очередь, приведёт к выполнению кода вируса. Это означает, что вирус может оставаться бездействующим на компьютере без каких-либо симптомов поражения. Однако, как только вирус начинает действовать, он может заражать другие файлы и компьютеры, находящиеся в одной сети. В зависимости от целей программиста-вирусописателя, вирусы либо причиняют незначительный вред, либо имеют разрушительный эффект, например удаление данных или кража конфиденциальной информации.

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

* Не работать под привилегированными учётными записями без крайней необходимости (учётная запись администратора в Windows).
* Не запускать незнакомые программы из сомнительных источников.
* Стараться блокировать возможность несанкционированного изменения системных файлов.
* Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
* Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
* Пользоваться только доверенными дистрибутивами.
* Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
* Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

# 78 Выполнить расшифрование, используя метод шифрующих таблиц.

При расшифровании все пробелы учитываются. Пробелы в шифртексте обозначаются символом «\_», несколько подряд идущих пробелов разделяются символом «|». Расшифровать шифртекст «\_НОНАВОГЯПЬТЕМ\_Р», полученный методом двойной перестановки(размер таблицы 4 х 4, последовательность номеров столбцов и номеров строк «2143,2143»).

Решение:

Проводить расшифровку будем методом обратным шифровке. Для начала составим таблицу шифровки, и в ней сразу запишем переставленные номера строк и столбцов.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2 | 1 | 4 | 3 |
| 2 | \_ | н | о | н |
| 1 | а | в | о | г |
| 4 | я | п | ь | т |
| 3 | е | м | \_ | р |

Сначала расставим в необходимом порядке столбцы.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |
| 2 | н | \_ | н | о |
| 1 | в | а | г | о |
| 4 | п | я | т | ь |
| 3 | м | е | р | \_ |

Теперь расставим в правильном порядке строки таблицы.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |
| 1 | в | а | г | о |
| 2 | н | \_ | н | о |
| 3 | м | е | р | \_ |
| 4 | п | я | т | ь |

Выпишем содержимое таблицы построчно, получаем результат: ВАГОН НОМЕР ПЯТЬ.

# 96 Выполнить шифрование сообщения

Выполнить шифрование сообщения «РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ», используя систему шифрования Цезаря с ключами, соответствующими варианту.

96 k= 4, ключевое слово «ЛЕТО».

Шифр Цезаря является частным случаем шифра простой за-мены (одноалфавитной подстановки).

Ключом шифрования является целое число 1 … N, где N – количество букв алфавита шифруемого слова, уменьшенное на 1.

Ключ будет обозначаться символом К. При шифровании исходного текста каждая буква заменяется на другую букву того же алфавита. Заменяющая буква определяется путем смещения по алфавиту от исходной буквы на К букв. При достижении конца алфавита выполняется циклический переход к его началу. В нашем случае К=4, составим таблицу смещений с учетом ключевого слова.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
| 0 | А |  | 9 | И |  | 18 | С |  | 27 | Ъ |  |
| 1 | Б |  | 10 | Й |  | 19 | Т |  | 28 | Ы |  |
| 2 | В |  | 11 | К |  | 20 | У |  | 29 | Ь |  |
| 3 | Г |  | 12 | Л |  | 21 | Ф |  | 30 | Э |  |
| 4 | Д |  | 13 | М |  | 22 | Х |  | 31 | Ю |  |
| 5 | Е |  | 14 | Н |  | 23 | Ц |  | 32 | Я |  |
| 6 | Ё |  | 15 | О |  | 24 | Ч |  |  |  |  |
| 7 | Ж |  | 16 | П |  | 25 | Ш |  |  |  |  |
| 8 | З |  | 17 | р |  | 26 | Щ |  |  |  |  |

Запишем наше ключевое слово с указанным в условии смещением.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
| 0 | А |  | 9 | И |  | 18 | С |  | 27 | Ъ |  |
| 1 | Б |  | 10 | Й |  | 19 | Т |  | 28 | Ы |  |
| 2 | В |  | 11 | К |  | 20 | У |  | 29 | Ь |  |
| 3 | Г |  | 12 | Л |  | 21 | Ф |  | 30 | Э |  |
| 4 | Д | л | 13 | М |  | 22 | Х |  | 31 | Ю |  |
| 5 | Е | е | 14 | Н |  | 23 | Ц |  | 32 | Я |  |
| 6 | Ё | т | 15 | О |  | 24 | Ч |  |  |  |  |
| 7 | Ж | о | 16 | П |  | 25 | Ш |  |  |  |  |
| 8 | З |  | 17 | р |  | 26 | Щ |  |  |  |  |

Оставшиеся ячейки заполним алфавитными без повторения.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
| 0 | А | ь | 9 | И | б | 18 | С | к | 27 | Ъ | ц |
| 1 | Б | э | 10 | Й | в | 19 | Т | м | 28 | Ы | ч |
| 2 | В | ю | 11 | К | г | 20 | У | н | 29 | Ь | ш |
| 3 | Г | я | 12 | Л | д | 21 | Ф | п | 30 | Э | щ |
| 4 | Д | л | 13 | М | ё | 22 | Х | р | 31 | Ю | ъ |
| 5 | Е | е | 14 | Н | ж | 23 | Ц | с | 32 | Я | ы |
| 6 | Ё | т | 15 | О | з | 24 | Ч | у |  |  |  |
| 7 | Ж | о | 16 | П | и | 25 | Ш | ф |  |  |  |
| 8 | З | а | 17 | р | й | 26 | Щ | х |  |  |  |

Осуществим шифрование заданной фразу выбирая её буквы из первого столбца и подставляя значения из второго. Фраза: РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| р | а | з | у | м | а | л | и | ш | а |
| й | ь | а | н | ё | ь | д | б | ф | ь |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| е | т | н | е | с | о | м | н | е | н |
| е | м | ж | е | к | з | ё | ж | е | ж |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| и | е | а | у | в | е | р | е | н | н |
| б | е | ь | н | ю | е | й | е | ж | ж |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| о | с | т | ь |  |  |  |  |  |  |
| з | к | м | ш |  |  |  |  |  |  |

Таким образом зашифрованная фраза выглядит так: ЙЬАНЁЬДБФЬЕМЖЕКЗЁЖЕЖБЕЬНЮЕЙЕЖЖЗКМШ.

# Список использованных источников

1. Васильева, И.Н. Криптографические методы защиты информации :учеб. и практикум / И.Н. Васильева. М. :Юрайт, 2020. 349 с.
2. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие / А.А. Малюк. М. : Горячая линия-Телеком, 2015. 280 с.
3. Безбогов, А.А. Методы и средства защиты компьютерной информации / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов, 2006.
4. Математические и компьютерные основы криптологии: учеб. пособие / Ю.С. Харин [и др.]. – Минск, 2003.
5. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты / А.А.Петров. – М., 2000.
6. Тимошенко, А.А. Защита информации в специализированнных информационно-телекоммуникационных системах / А.А.Тимошенко. –Киев, 2010.