Виды и способы защиты информации

Дудниченко Ю.В.

БГУ- Брянский Государственный Университет имени академика И.Г Петровского. Россия, Брянск

В современном мире главную ценность представляет информация и защита - главная задача при ее передаче. Как обеспечить безопасность информации? Какие для этого существуют способы и программы? Ответы на эти вопросы представлены в данной статье.

Ключевые слова: защита информации, информационные технологии, защита, информация, безопасность личных данных.

Types and methods of information protection

Dudnichenko Yu. V.

BSU-Bryansk state University named after academician I. G. Petrovsky. Russia, Bryansk

In today's world, the main value is information and protection - the main task in its transmission. How to ensure information security? What methods and programs are available for this purpose? The answers to these questions are presented in this article.

Keywords: information security, information technology, security, information, personal data security.

С появлением интернета появилось множество новых способов передачи информации. Но также возросли риски того что ваши личные сообщения или персональные данные будут похищены посторонними людьми. Существует множество способов для этого. Злоумышленник может намерено взломать ваше устройство или запустить в него вирус через рекламу в интернете, подозрительные сайты или неосторожно скаченные приложения. Для того чтобы такого не случалось, были разработаны специальные программы для защиты информации.

Перечислить, какие именно могут возникнуть опасности, если защита информации в сети интернет не организована или организована плохо — практически невозможно. Каждый отдельный случай — это обычно совокупность, зачастую самое неприятное сочетание нескольких факторов. Их краткий список можно сформулировать так:

- получение несанкционированного доступа к информации;
- кража критически важных данных;
- подмена или намеренное изменение информации в хранилище или непосредственно при передаче;
- злонамеренное удаление важных данных;
- разглашение конфиденциальной информации после получения доступа к ней различными методами;
- намеренное шифрование данных с целью последующего шантажа, вымогательства.

Существует несколько видов защиты информации:

- Аппаратные

Аппаратные средства применяются на всех организационных уровнях. Однако особенно важно правильно организовать хранение информации.
Задача аппаратных средств при этом:

- обеспечивать нужную скорость доступа к данным;
- гарантировать надлежащую скорость систем проведения расчетов;
- обеспечивать целостность данных и гарантию их сохранения при выходе из строя отдельных средств хранения;
- организовывать резервное копирование, быстрое восстановление информации при сбоях;
- обеспечивать взаимодействие со средствами связи;
- реагировать и минимизировать ущерб при аварийных ситуациях (пожар, затопление);
- сохранять работоспособность основного оборудования во время отключения основного источника энергии (генераторы, источники бесперебойного питания).
- обрабатывать запросы подключенных пользователей.

- Программные

Область программных средств — самая обширная. Выбор конкретного списка пакетов зависит от используемых платформ и операционных систем, принятых механик доступа.
Среднестатистический список защитных мер включает:

- систему обнаружения сетевых атак и попыток несанкционированного доступа на узел в составе программно управляемого оборудования;
- комплексы шифрования (программные или аппаратные);
- средства подтверждения подлинности, электронные ключи и системы для работы с ними;
- средства управления доступом, которые могут включать и аппаратные средства.

Для безопасности личных данных при использовании сети интернет рекомендуется не впадать в крайности, а следовать простым советам:

- Антивирус. По стандарту это самая распространенная мера безопасности. Программа обнаруживает вредоносное ПО, шпионские ссылки, фишинговые сайты и подозрительный трафик. Антивирус спасает от угроз, которые атакуют компьютер, но не защищает от действий клиента на сервисах.
- VPN — сеть, скрывающая ip. Для обхождения блокировки сайта или обеспечения анонимности рекомендуется использовать данную программу. VPN оберегает от кражи информации, шифрует ее, скрывает личные данные.
- Двухфакторная аутентификация. Для авторизации на сайте придется ввести два доказательства того, что аккаунт принадлежит пользователю. Обычно это пароль и смс-код на телефон. Если мошенник получил доступ к паролю, взломать аккаунт у него не получится.
- Внимательность и осторожность с почтой. Не рекомендуется открывать письма от неизвестных источников и переходить по сомнительным ссылкам.

Существует множество систем защиты информации. Таких как Dallas Lock и Аура. Рассмотрим их возможности.
Dallas Lock – система защиты информации от несанкционированного доступа, сертифицированная и позволяющая привести автоматизированные системы в соответствие требованиям законов РФ, стандартов и руководящих документов.

Возможности Dallas Lock:

- Однофакторная или двухфакторная аутентификация пользователей
- Контроль каналов распространения конфиденциальной информации
- Позволяет выполнять очистку остаточной информации
- Позволяет разграничить права доступа администраторов и пользователей к локальным и сетевым ресурсам
- Позволяет разграничить доступ к сменным накопителям для предотвращения возможной утечки конфиденциальной информации.
- Возможность администрирования рабочих мест удаленно
- Возможность работы с помощью сервера терминального доступа
- Разграничение прав по мандатному и дискреционному принципу
- Организация доверенной информационной среды
- Способность создать замкнутую программную среду
- Имеет трехуровневую систему управления безопасностью (компьютер-домен безопасности-лес безопасности), что позволяет применять Dallas Lock в организации с большим количеством филиалов
- Контроль целостности ресурсов компьютера и программно-аппаратной конфигурации
- Отсутствие обязательной аппаратной части
- При использовании Сервера безопасности, возможность централизованно управлять политиками безопасности
- Дает возможность проводить оперативный мониторинг и аудит действий пользователей

Аура — система защиты информации от несанкционированного доступа. Разработана и выпускается Научно-исследовательским отделом проблем информационной безопасности Санкт-Петербургского института информатики и автоматизации РАН

Возможности Ауры:

- Наличие доверенной среды для аутентификации, контроля целостности и настройки СЗИ вне защищаемой операционной системы. Усиление аутентификации с помощью так называемого «пароля на загрузку». В этом случае доверенная среда СЗИ зашифрована на данном пароле и без него загрузка любого пользователя невозможна.
- Многоуровневый контроль целостности информационных объектов вычислительной системы. Контроль целостности объектов файловой системы и реестра до загрузки защищаемой ОС, в том числе на прозрачно шифрованных дисках. Возможность настройки реакции СЗИ на нарушение контроля целостности.
- Контроль доступа к устройствам, файлам и папкам;
- Управление печатью, автоматическая маркировка и учёт документов. Возможность создания своего шаблона для маркировки печатаемых документов.
- Прозрачное кодирование (шифрование) жёстких дисков, съемных носителей и виртуальных дисков. Экспорт/импорт ключей кодирования на электронный ключ или внешний носитель.
- Достоверное уничтожение информационных объектов. Возможность гибкой настройки метода затирания (выбор байта заполнения-определённое значение, случайный; количество проходов; настройка затирания с учётом особенностей файловой системы.)
- Регистрация действий пользователя и событий в системных журналах;

- Идентификация и аутентификация пользователей в доверенной среде с применением электронных устройств Rutoken.
- Блокировка консоли по таймауту, извлечению электронного ключа, при загрузке защищаемой операционной системы. Разблокировка по электронному ключу или паролю.
- Динамическая смена пароля пользователя в операционной системе для управления доступом к сетевым ресурсам.
- Сессионный мандатный доступ.

В результате проделанной работы было выяснено, какие средства можно использовать для защиты информации и какие системы для этого существуют.

В заключении хочу напомнить, что важная роль в защите вашей информации зависит от ваших действий и своевременного обновления программного обеспечения.

Список литературы:

- https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%80%D0%B0_(%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) – Аура (система защиты информации)
- https://scam.zone/stati/zaschita-informatsii-v-internete – Защита информации в интернете, технологии, средства и методы
- https://bezopasnostin.ru/informatsionnaya-bezopasnost/zashhita-informatsii-v-internete.html – особенности методов защиты информации в интернете: аппаратные, программные и смешанные
- http://xn--h1anfb.xn--p1ai/ HYPERLINK "http://спси.рф/szi-ot-nsd/Dallas-Lock/?yclid=83163328830538692"szi-ot-nsd HYPERLINK "http://спси.рф/szi-ot-nsd/Dallas-Lock/?yclid=83163328830538692"/ HYPERLINK "http://спси.рф/szi-ot-nsd/Dallas-Lock/?yclid=83163328830538692"Dallas-Lock HYPERLINK "http://спси.рф/szi-ot-nsd/Dallas-Lock/?yclid=83163328830538692"/? HYPERLINK "http://спси.рф/szi-ot-nsd/Dallas-Lock/?yclid=83163328830538692"yclid HYPERLINK "http://спси.рф/szi-ot-nsd/Dallas-Lock/?yclid=83163328830538692"=83163328830538692 – Dallas Lock – система защиты информации от несанкционированного доступа