Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Колесников В.А., Несговоров А.Г. Перспективы использования технических средств защиты информации в России // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2018. – №6 (июнь). – АРТ 385-эл. – 0,3 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.492

Колесников Владислав Александрович
курсант 4 курса, 1 факультет (подготовки штурманов)
Несговоров Алексей Георгиевич
курсант 4 курса, 1 факультет (подготовки штурманов)
Филиал ВУНЦ ВВС «ВВА» в г. Челябинске
e-mail: brutal1061@mail.ru

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ

Аннотация: В данной статье рассмотрены вопросы, связанные с информационной безопасностью в России, раскрывается суть проблемы и способы ее решения, а также методы и средства для обеспечения защиты информации, в частности рассматриваются программные средства защиты информации и их дальнейшее развитие.

Ключевые слова: защита информации, система безопасности, криптография, стеганография, сертификат, вирус.

Kolesnikov Vladislav Alexandrovich
cadet 4 courses, 1 faculty (training navigators)
Nesgovorov Aleksey Georgievich
cadet 4 courses, 1 faculty (training navigators)
Branch of VUNTS VVS "VVA" in Chelyabinsk

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

PROSPECTS OF USING SOFTWARE PROTECTION PROTECTION IN RUSSIA

Abstract: This article discusses issues related to information security in Russia, reveals the essence of the problem and how to solve it, as well as methods and means to ensure the protection of information, in particular, software tools for protecting information and their further development.

Key words: information security, security system, cryptography, shorthand, certificate, virus.

С развитием информационного общества человек все больше связан с его личной информационной средой, интерфейс которой обычно является его персональным компьютером. В результате такого «привязывания» человек вынужден либо носить с собой персональный компьютер, либо ограничивать свои движения. То есть, действуют в ущерб либо требованиям удобства и / или качества, либо требованию мобильности.

При этом очевидно, что наличие строго определенного персонального компьютера на самом деле в большинстве случаев необязательно. Как правило, личная информационная среда, необходимая человеку - это далеко не все те разнородные данные, которые есть в его компьютере, а сравнительно небольшая их часть. Поэтому часто в ущерб требованию защищенности информации выбирают другой путь - копирование данных на различные носители и использование их на чужих компьютерах. Это связано с риском доступа к информации третьих лиц. Поэтому данные рекомендуется шифровать, но и здесь возникают различные проблемы, связанные с хранением ключевой информации, доверием к выполнению

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

криптографических алгоритмов тем или иным техническим устройством и тому подобные.

Проблемы информационной безопасности: надежное обеспечение её сохранности и установленного статуса использования - является одной из важнейших проблем современности. Появление персональных компьютеров, локальных и глобальных компьютерных сетей, спутниковых каналов связи, эффективных средств технической разведки и получения конфиденциальной информации существенно обострило проблему защиты информации.

Особенностями современных информационных технологий, прямо или косвенно влияющими на безопасность информации, являются [3]:

1. Увеличение числа автоматизированных процедур в системах обработки данных и усиление важности принимаемых на их основе решений;

2. Территориальная распределенность компонентов компьютерных систем и передача информации между этими компонентами;

3. Усложнение используемых программных и аппаратных средств компьютерных систем;

4. Интеграция в единых базах данных информации различного назначения и различных режимов доступа;

5. Накопление и долговременное хранение больших массивов данных на электронных носителях, зачастую не имеющих твердых копий;

6. Рост стоимости ресурсов компьютерных систем;

7. Непосредственный доступ к ресурсам компьютерных систем большого количества пользователей различных категорий и с различными полномочиями в системе.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Рост количества и качества угроз безопасности информации в компьютерных системах не всегда приводит к адекватному ответу в виде создания надежных систем защиты информации и информационных технологий.

Меры по защите информации и сетей осуществляются в России нормами закона «Об информации, информационных технологиях и о защите информации» [1].

Под средствами сетевой безопасности имеются в виду меры предотвращения нарушений безопасности, которые возникают только при передаче информации по сетям, а также меры, позволяющие определять, что такие нарушения безопасности имели место.

В современной практике выделяют следующие группы средств: антивирусные; организационные; защита с помощью паролей; стенографические; криптографические.

Обеспечение защиты средств обработки информации и АРМ от несанкционированного доступа достигается системой разграничения доступа субъектов к объектам. Данная система реализуется в программно-технических комплексах в рамках ОС, прикладных программ или систем управления базами данных, в средствах реализации локальных вычислительных сетей, в использовании криптографических преобразований и методов контроля доступа.

При разработке средств защиты информации так же следует принимать во внимание и то, что вся система состоит из более мелких систем. К ним относится: подсистема управления доступом, подсистема регистрации и учета, криптографическая защита информации и подсистема обеспечения целостности.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Общие принципы организации защиты конфиденциальной информации, применяемые при разработке средств защиты информации [2]: непрерывность; комплексность; достаточность; эффективность; согласованность.

Способы антивирусной защиты составляют технические и программные средства по защите информации от вирусов.

Вирус — это программа содержащая, вредоносный код, поэтому основным средством от их защиты является антивирусное программное обеспечение — приложение, обеспечивающее отслеживание и уничтожение вирусов.

Как и вирусы, антивирусы постоянно развиваются. Также постоянно расширяются общее определение и классификация антивирусного ПО.

Существует достаточно большое количество антивирусных программ. Наиболее эффективными, на наш взгляд, являются: антивирус Касперского и Dr. Web.

Как правило, все антивирусные программы платные. Существующие бесплатные программы, такие как Calm.AV и Avast, менее эффективны. Эффективность антивирусного ПО оценивается по проценту обнаруженных и обезвреженных вирусов и скорости реакции на вновь возникающие вирусные угрозы.

После успешного лечения компьютера от вирусов в системе все равно могут остаться неисправимые изменения, делающие систему неработоспособной. Поэтому лучшей защитой от вирусных атак является профилактика, заключающаяся в использовании проективной защиты, а также защиты компьютера от сетевых атак. Еще один действенный вариант — использование операционных систем семейства Linux, вирусы для которых на сегодня практически не получили распространения.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Использование надежного пароля является одним из наиболее важных факторов защиты компьютера от злоумышленников и других нежелательных пользователей.

Пароль — это условное слово или набор знаков, предназначенный для подтверждения полномочий или личности.

Использование представленных паролей не может служить эффективной защитой информации. Пароль, несущий в себе высокую степень защиты, должен отвечать следующим требованиям: длина не менее 6—8 символов; использование цифр; использование букв разных регистров; использование букв разных алфавитов; использование специальных символов; отсутствие словарных выражений.

Криптография — это комплексная наука о защите данных. Защита осуществляется на основе математических преобразований данных.

Существуют следующие криптографические методы защиты: открытый текст — это данные, которые можно преобразовать с помощью стандартных процедур; зашифрованный текст — это данные, которые невозможно преобразовать с помощью стандартных процедур; ключ шифрования — это данные, необходимые для преобразования открытого текста в зашифрованных (и наоборот).

Виды криптографических алгоритмов: симметричные — для шифрования и дешифрования используется один и тот же ключ; асимметричные — для шифрования и дешифрования используется ключевая пара: открытый — известный всем и закрытый — который известный только владельцу.

Сертификат — бумажный или цифровой документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующий владельца ключа.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Сертификат содержит: информацию о владельце ключа; сведение об открытом ключе; название центра сертификации.

Целью стенографической защиты является скрытие самого факта существования или передачи данных.

Стенография — (от греч. «тайнопись») раздел знаний о защите данных на основе скрытия канала передачи.

Различают несколько направлений стеганографии: классическая стеганография; компьютерная стеганография — использование особенностей компьютерной платформы (стеганографические файловые системы, скрытие данных в неиспользуемых областях формата файла); цифровая стеганография — направление компьютерной стеганографии, основанное на скрытии информации в цифровых объектах, изначально имеющих аналоговую природу (изображения, видео, звуки).

Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера (атакам). Например, плагины к редактору Adobe Photoshop позволяют встроить в само изображение информацию об авторе. Метод наименее значимых битов — скрытие данных в младших битах графического изображения.

Такой подход приводит к минимальным изменениям в конечном файле.

Проведенные исследования выявили преимущества и недостатки групп методов защиты информации в сети, и каждый из них имеет границы использования. Поэтому, для полноценной защиты информации необходимо комплексное использование методов, которые должны быть регламентированы в рамках организации, то есть иметь четкую организационную структуру применения.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Для того чтобы оценить перспективы развития технических средств защиты информации, нужно для начала оценить состояние развития среды, влияющей на объект защиты. Необходимо понять, как развиваются технические средства вычислительной техники (программные и аппаратные), появились ли новые угрозы, и если да, то какие.

Очевидно, что назрела необходимость в устройстве, которое позволило бы человеку сделать свою персональную информационную среду мобильной и в то же время - защищенной. Это Персональное Средство Криптографической Защиты Информации - ПСКЗИ.

Подводя итог, можно выделить главную, на наш взгляд, тенденцию: развитие средств защиты информации будет идти по двум различным, но взаимодополняющим направлениям, а именно:

- стандартные ПЭВМ все более и более будут «впитывать» в себя лучшие достижения в области аппаратной защиты, при этом дополнительно к новому уровню «стандартности» будут необходимы лишь средства идентификации/аутентификации, которые будут активными;

- в областях, где требуется высокий уровень защищенности, будут использоваться новые специально спроектированные технические средства. Средства защиты будут все более и более приобретать черты полноценных компьютеров. Они будут содержать все стандартные для компьютеров составляющие, и при этом сохранять специализацию за счет ОС реального времени и аппаратных спецканалов. В первую очередь появятся специализированные терминалы.

Среди ближайших перспектив - средства создания персональной защищенной среды. Наиболее близко к этому подошли разработчики ПСКЗИ «ШИПКА».

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

В это же время будут активно развиваться технологии HSM [4], со временем все более приближаясь к серверным решениям. Скорее всего, наиболее активно будут развиваться аппаратные решения на базе ОС реального времени и специализированных микропроцессоров. Обнадеживающими здесь являются решения «Инфотекс» на базе спецЭВМ разработки «ОКБ САПР».

Чуть далее по времени, но все же недалеко - создание защищенных терминалов. На первом этапе наиболее эффективными обещают быть аппаратно-программные решения. В качестве примера можно привести совместную разработку специалистов «Ками» и «ОКБ САПР».

Далее на очереди - создание резидентных средств сетевой защиты. Это будут средства, в которых за счет собственных ресурсов будут исполняться процедуры антивирусной защиты, межсетевого экранирования, браузера и др.

Список использованной литературы:

1. Домарев В.В. Безопасность информационных технологий. - М.: Диасофт, 2002. - 688 с;
2. Конявский В.А. Управление защитой информации на базе СЗИ НСД "Аккорд". - М.: Радио и связь, 1999. - 328 с;
3. Мельников В.П. Защита информации в компьютерных системах. - М.: Финансы и статистика, 1997. — 368 с;
4. Титоренко Г.А. Информационные технологии управления. М.: ЮНИТИ-ДАНА, 2003. - 439 с.

Дата поступления в редакцию: 20.06.2018 г.

Опубликовано: 25.06.2018 г.