внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения таможенных органов;

уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии автоматизированных систем таможенных органов[2].

Анализ угроз информационной безопасности таможенных органов Республики Беларусь позволяет понять значение угроз в построении системы обеспечения информационной безопасности таможенных органов.

Реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению максимально полно и оперативно. Государство в лице этих государственных органов и организаций обеспечивает своевременное принятие мер безопасности, незамедлительно оповещает заинтересованные субъекты, минимизирует ущерб и локализует последствия, определяет причастных лиц и организации, накапливает опыт противодействия угрозам.

Литература

Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель. Информационная безопасность в таможенных органах:Учебное пособие. – Минск, 2019. – С. 108-110.

Т. П. Лепа. Информационные технологии в таможенной сфере: Учебное пособие. – Иркутск, Издательство БГУ, 2016. – С. 85-86.

Основные направления развития таможенной службы Республики Беларусь // Утверждено Приказом председателя ГТК от 08.04.2011 № 125-ОД.

Программные закладки и методы защиты от них

Жадинец Я.А.

Научный руководитель: Ковалькова И.А.

Белорусский национальный технический университет

На сегодняшний день многие традиционные ресурсы нашего человечества постепенно утрачивают своё первоначальное значение. На новом этапе развития общества появляется новый ресурс –

информация.Поэтому защита информации, хранимой в компьютерных системах от несанкционированного доступа (НСД), является весьма актуальной. Для решения этой задачи используется комплекс средств, включающий в себя технические, программные аппаратные средства и административные меры защиты информации. По мере развития средств защиты компьютерных систем развиваются и средства нападения. Одной из наиболее опасных является атака защищенной системы посредством программных закладок.

Программные закладки – это скрытные (недокументированные) возможности в программном и аппаратном обеспечении персональных компьютеров и периферийного оборудования, позволяющие осуществлять скрытый несанкционированный доступ к ресурсам системы (как правило, посредством локальной или глобальной сети). Таким образом, основное предназначение закладок – обеспечить несанкционированный доступ к конфиденциальной информации [1].

Главный вред, который может нанести программная закладка заключается в том, что она способна принимать активные меры по маскировке своего присутствия в системе, являясь частью защищённой системы. Создаётся скрытый канал информационного обмена, который, как правило, остаётся незамеченным для администраторов системы на протяжении долгого времени. Большинство программных закладок, которые применялись в разное время различными правонарушителями, были обнаружены в результате ошибок, допущенных при программировании закладки, либо случайным образом [3].

Что касается классификации программных закладок, то существует несколько их разновидностей:

Клавиатурные шпионы– самые распространённые программные закладки.Их основная цель – перехват паролей пользователей операционной системы, а также определение их легальных полномочий и прав доступа к компьютерным ресурсам. Клавиатурные шпионы также делятся на три типа: имитаторы, фильтры и заместители. Основное их отличие – это способ перехвата пользовательских паролей.

Троянская программа (*троянец* или *троянский конь*) – это особая разновидность программной закладки, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определённого ущерба.

Логическая бомба (logicbomb) – скрытый код в системе, который активизируется по возникновению определённого события (чаще всего в определённое время). Данный вид программных закладок нацелен на полное выведение системы из строя и оказывает мощное разрушительное

действие на конкретную компьютерную систему. После выполнения своей миссии логическая бомба уничтожается.

Мониторы – это программные закладки, перехватывающие те или иные потоки данных, протекающие в атакованной системе. В частности, к мониторам относятся перехватчики паролей второго рода. Основные цели: частичное или полное сохранение перехваченной информации в доступном злоумышленнику месте, искажение потоков данных, блокирование данных, мониторинг потоков данных для сбора информации об атакованной системе.

Компьютерные черви. Вирус – одна из разновидностей злоумышленного кода, который распространяется, прикрепляясь к исполняемому файлу или документу (заражая его).Червь – это злоумышленная программа, распространяющая свои копии. В отличие от вируса, червь не прикрепляется к другим файлам, а распространяется в виде копии самостоятельно [1].

Перехватчики паролей перехватывают имена и пароли, вводимые пользователями защищённой системы в процессе идентификации и аутентификации.

Программы-шутки–программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинён, либо будет причинён при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности[2].

Существует 3 основных метода защиты от программных закладок:

Защита от внедрения программных закладок.

Универсальным средством защиты от внедрения программных закладок является создание изолированного компьютера. Компьютер называется изолированным, если выполнены следующие условия:

нём установлена система BIOS, не содержащая программных закладок;

операционная система проверена на наличие в ней закладок;

на компьютере не запускалось и не запускается никаких иных программ, кроме уже прошедших проверку на присутствие в них закладок.

Выявление внедрённой программной закладки.

Выявление внедрённого кода программной закладки заключается в обнаружении признаков его присутствия в компьютерной системе. Эти признаки можно разделить наследующиедвакласса:

качественные и визуальные;

обнаруживаемые средствами тестирования и диагностики.

Удаление внедрённой программной закладки.

Конкретный способ удаления внедрённой программной закладки зависит от метода её внедрения в компьютерную систему. Это можно

сделать путём перепрограммирования ПЗУ компьютера, замены на загрузочную запись, драйвер, утилиту, прикладную или служебную программу, полученную от источника, заслуживающего доверия, можно попытаться добыть исходный текст, убрать из него имеющиеся закладки или подозрительные фрагменты, а затем заново откомпилировать [3].

Защитить информацию может только сам пользователь или владелец информационного ресурса. Для этого нужно правильно организовать работу и ограничить доступ к ценной информации. И принять все меры для предотвращения её утечки.

Литература

Анин Б. Ю. «Защита компьютерной информации». – СПб.: БХВ-Петербург, 2000. – 384 с.

Казарин О.В. «Безопасность программного обеспечения компьютерных систем». – М.: МГУЛ, 2003. - 212 с.

Романец Ю., Тимофеев П., Шаньгин В. «Защита информации в компьютерных системах и сетях». – М.: Радио и связь, 2001 – 376 с.

Криптография как наука. Типы криптосистем

Краснова А.К.
Научный руководитель:Ковалькова И.А.
Белорусский национальный технический университет

Криптография – это наука об использовании математики для зашифрования и расшифрования данных.

История криптографии насчитывает несколько тысячелетий. Первые системы шифрования появились одновременно с письменностью в четвёртом тысячелетии до н.э.. В Древней Греции и Древнем Риме криптография широко использовалась в разных областях деятельности, особенно в государственной сфере. В годы средневековья практика шифрования сохранялась в строжайшей тайне. В годы крестовых походов шифровальщики, служившие у Папы Римского, после года работы подлежали физическому уничтожению.

настоящее время, в связи с увеличением вычислительной мощности компьютеров, криптография стала значительно более сложной. Теперь она способна намного надёжнее гарантировать безопасность информации. Шифры, какие когда-то использовал Цезарь, сегодня можно расшифровать за пару секунд [1].

Практическое применение криптографии стало неотъемлемой частью жизни современного общества – её используют в таких отраслях как