ЛЕКЦИЯ

«БАЗОВЫЕ СВОЙСТВА ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ И ВИДЫ АТАК НА ИНФОРМАЦИЮ»

ВОПРОСЫ ЛЕКЦИИ

1. Основные определения теории защиты информации.
2. Свойства защищаемой информации.
3. Виды атак на информацию.

ЛИТЕРАТУРА

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.
3. Емельянова, Н.З. Защита информации в персональном компьютере: Уч.пос / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2017. - 352 с.
4. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: Риор, 2017. - 480 с.
5. Камский, В. Защита личной информации в интернете, смартфоне и компьютере / В. Камский. - СПб.: Наука и техника, 2017. - 272 с.
6. Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. - РнД: Феникс, 2017. - 347 с.
7. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.
8. Мельников, В.П. Защита информации: Учебник / В.П. Мельников. - М.: Академия, 2019. - 320 с.

1. Основные определения теории защиты информации

Базовыми в теории защиты информации являются термины "Информационная безопасность", "Безопасность информации", "Защита информации". Их сущность определяет в конечном итоге политику и деятельность в области защиты информации

Информационная безопасность - состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

Безопасность информации - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Из определений понятий "Информационная безопасность" и "безопасность информации" вытекает, что защита информации направлена на обеспечение безопасности информации, или другими словами, безопасность информации обеспечивается с помощью ее защиты.

Однако нарушение безопасности информации (разглашение, искажение, утрата) в конечном итоге наносит ущерб (моральный и материальный) ее собственнику. Поэтому для того, чтобы четко установить что защищать, в чьих интересах защищать, как и чем защищать, введена система понятий в этой области. В целом основные понятия в этой области систематизированы в основных правовых и нормативных документах.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

Информационные системы с точки зрения ценности хранимой и обрабатываемой информации можно условно разделить на следующие группы:

− домашние персональные компьютеры, используемые главным образом для образовательных целей и развлечения;

− коммерческие компьютеры, используемые в бизнесе, промышленных и научных исследованиях и т.п.

− банковские системы, системы электронных платежей;

− правительственные и военные информационные системы.

В соответствии с этой классификацией можно выделить группы источников атак:

− вандализм, осуществляемый хакерами-любителями практически бескорыстно, с целью самоутверждения;

− криминальные атаки с целью хищения денежных средств частных лиц или коммерческих структур;

− коммерческий шпионаж;

− шпионаж (разведка) по заданию правительственных органов.

Формально понятие информационной атаки можно определить следующим образом: при хранении, поддержании и предоставлении доступа к любому информационному ресурсу его владелец накладывает некоторый набор правил по работе с этим информационным ресурсом.

Умышленное нарушение этих правил классифицируется как атака на информацию.

2. Свойства защищаемой информации

Защита информации определяется рядом свойств информации, назовем некоторые из них:

1. Информация доступна человеку, если она содержится на материальном носителе. С помощью материальных средств можно защищать только материальный объект, таким образом, объектом защиты

информации являются материальные носители информации. Носители информации бывают:

- носители - источники информации (чертёж - это источник, а бумага, на которой он нарисован, - носитель, однако, бумага, без нанесённого на ней текста или рисунка является источником информации о её физических и химических характеристиках);

- носители - переносчики информации;

- носители - получатели информации;

Передача информации путём перемещения её носителей в пространстве связана с затратами энергии, причём величина затрат зависит от длины пути, параметров среды и типа носителя.

2. Ценность информации оценивается степенью полезности её для пользователя (собственника, владельца, получателя). Полезность информации всегда конкретна - нет ценной информации вообще - информация полезна или вредна для конкретного её пользователя, поэтому при защите информации прежде всего определяют круг субъектов (государств, фирм, групп лиц, людей), заинтересованных в защищаемой информации, так как вероятно, что среди них окажутся злоумышленники. В интересах защиты информации её владелец наносит на носитель информации условный знак полезности содержащейся на нём информации - гриф секретности или конфиденциальности. В качестве критерия для определения грифа конфиденциальности информации могут служить результаты прогноза последствий попадания информации к конкуренту или злоумышленнику:

- величина экономического и морального ущерба, наносимого организации;

- реальность создания предпосылок для катастрофических последствий в деятельности организации (банкротства и тому подобное).

3. Так как информация для получателя может быть полезной или вредной, то информацию можно рассматривать как товар. Цена

информации, как любого товара, складывается из себестоимости и прибавочной стоимости (прибыли). Себестоимость определяется расходами владельца информации на её получение путём:

- исследований в лабораториях, аналитических центрах, группах;

- покупке информации;

- добыча информации противоправными действиями.

Прибыль от информации может быть получена в результате следующих действий:

- продажи информации на рынке;

- материализации информации в продукции с новыми свойствами или в технологиях, приносящими прибыль;

- использование информации для принятия эффективных решений (экономия средств, ресурсов и тому подобное).

4. Ценность информации изменяется во времени. Распространение информации и её использование приводят к изменению её ценности и цены. Характер изменения ценности от времени зависит от вида информации.

5. Невозможно объективно (без учёта полезности её для потребителя, владельца, собственника) оценить количество информации. Иногда полезность информации связывают с её качеством, но понятие "качество", применительно к информации, не имеет самостоятельного значения, т.к. оно поглощается понятием "количество". Количество информации зависит от её качества: чем более качественная фотография, тем больше оттенков и полутонов она содержит, тем менее на ней помех. Под качеством информации подразумевают качество отображения её на носителе или её достоверность (соответствие оригиналу).

6. При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а цена снижается.

Все перечисленные свойства информации являются важными составляющими для формирования политики информационной

безопасности организации, государства, группы лиц - деятельности любых субъектов информационного пространства и информационных систем.

Информация с точки зрения информационной безопасности должна обладать следующими свойствами:

Конфиденциальность **–** это свойство означает, что доступ к информации могут получить только легальные пользователи;

Целостность **–** информация существует в исходном виде и при её передаче или хранении не было сделано несанкционированных изменений. Нарушение этого свойства называется фальсификацией сообщения.

Аутентичность **–** это свойство означает, что источником информации является именно то лицо, которое заявлено как автор. Нарушение этого свойства называется фальсификацией автора сообщения.

Аппелируемость **–** означает, что можно доказать, что автором сообщения является именно заявленный человек и никто другой. Это свойство играет важную роль, когда автор сообщения пытается от него отказаться.

Свойства информационных систем:

1. Надежность – система в нормальном и внештатном режимах ведет себя так как запланировано

2. Точность - точное и полное выполнение команд

3. Контроль доступа – различные группы людей имеют различный уровень доступа к информационным объектам и ограничения доступа выполняются.

4. Контролируемость – в любой момент может быть проведена полная проверка любой компоненты программного комплекса

5. Контроль идентификации – клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает

6. Устойчивость к умышленным сбоям – при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

3. Виды атак на информацию

Существует множество способов выполнения атак: при помощи специально разработанных средств, методов социального инжиниринга, через уязвимые места компьютерных систем. При социальном инжиниринге для получения несанкционированного доступа к системе не используются технические средства. Злоумышленник получает информацию через обычный телефонный звонок или проникает внутрь организации под видом ее служащего. Атаки такого рода наиболее разрушительны.

Атаки, нацеленные на захват информации, хранящейся в электронном виде, имеют одну интересную особенность: информация не похищается, а копируется. Она остается у исходного владельца, но при этом ее получает и злоумышленник. Таким образом, владелец информации несет убытки, а обнаружить момент, когда это произошло, очень трудно.

Наиболее распространенный вид информационной атаки – это несанкционированный доступ, который может происходить через:

− Человека: хищение носителей информации, чтение информации с экрана или клавиатуры.

− Программу: перехват паролей, дешифровка зашифрованной информации, копирование информации с носителя.

− Аппаратуру: подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации, перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Компьютерные атаки характерны тем, что они, как правило, удаленные и противник может находиться за тысячи километров.

При этом нападению могут подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

Приведем некоторые примеры информационных атак. Один из широко распространенных методов атаки – атака с подбором пароля. Если исключить подглядывание и подслушивание, то часто встречающимся является метод подбора. Конечно можно использовать полный перебор, но очевидно, что если пароль достаточно длинный , то это потребует значительного времени. Пусть A – мощность алфавита паролей, L – длина пароля, тогда мощность пространства паролей S = A^L . Вероятность подбора пароля за время его существования T можно определить как

$$P = \frac{VT}{S},$$

где V обозначает известную заранее скорость подбора пароля, измеряемую числом паролей, проверяемых в единицу времени.

Гораздо эффективнее с точки зрения вычислительной сложности так называемый подбор по словарю. Значительная часть используемых на практике паролей представляет собой осмысленные слова и выражения. Существуют словари наиболее распространенных паролей. Учитывая, что в любом языке порядка 1 000 000 слов, то их перебор занимает незначительное время. Известно, что от 40 до 80 процентов паролей может быть угадано таким образом. Особенно эффективно этот метод работает, если известна некоторая персональная информация о пользователе (дни рождения и имена родственников, имена любимых собак и кошек и.т.д.). Часто в качестве пароля, например, используют собственное имя, написанное задом наперед.

Атаки, использующие “дыры” и “баги” в ПО. Особо славится своей незащищенностью ПО от Microsoft. Обычно кто-либо находит «дыру» или «баг» в ПО для сервера и публикует эту информацию в Интернет в соответствующей конференции. Производитель ПО выпускает “заплатку”, устраняющую проблему и публикует ее на своем web-сервере. Проблема в том, что администраторы сетей нерегулярно следят за “дырами “ и

“заплатками”, а хакеры же умело используют полученную информацию. Основная цель такой атаки – получить доступ к серверу от имени пользователя, работающего с приложением, обычно с правами системного администратора и соответствующим уровнем доступа.

Атаки с помощью вирусов, почтовых червей и “троянских коней”. Можно с уверенностью сказать, что с этим видом атаки каждый пользователь компьютера сталкивался хотя бы однажды. Вирусы, почтовые черви и “троянские кони” – это разные классы “враждебного” программного кода. Вирусы внедряются в другие программы с целью выполнения заложенной в них вредоносной функции на компьютере данного пользователя. Чаще всего – это уничтожение всех или только определенных файлов на винчестере. Термин «компьютерный вирус» впервые употребил сотрудник Лехайского университета (США) Фред Коэн в 1984 году на 7-й конференции по безопасности информации, проходившей в США. Вирус может создавать свои копии, внедрять их в файлы и системные области компьютера. Копии сохраняют способность к дальнейшему распространению.

По среде обитания вирусы бывают: файловые (внедряются в выполняемые файлы), загрузочные (внедряются в загрузочный сектор диска (Boot)), сетевые – распространяются по сети, специальные – ориентированы на специальное ПО, например, документы редактора Word.

По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус оставляет свою резидентную часть в оперативной памяти. Затем она перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы остаются активными даже когда удалены зараженные файлы. Если они являются загрузочными, то даже переформатирование диска может не помочь. Нерезидентные вирусы не заражают память компьютера и обычно могут быть удалены при удалении зараженных программ. Часто вирусы запрограммированы на определенную дату, а также на рассылку копий

посредством электронной почты по всем адресам, найденным в адресной книге пользователя.

В отличие от вируса, обычно, цель внедрения “троянского коня” – получение скрытого удаленного контроля над компьютером. Такая программа, не афишируя своего присутствия, может отсылать хозяину пароль и логин для доступа в Интернет с данного компьютера или даже изменять или видоизменять те или иные данные.

Большинство вирусов проникают в ОС через определенные входящие подключения, так называемые «порты», которые являются включёнными по умолчанию. Давайте, в качестве примера, поговорим об этом более подробно.

Несколько упрощая, понятие «порт» можно определить как номер входящего подключения внешних программ (в том числе и вирусов) к вашему компьютеру через IP-сеть. Каждому порту присваивается уникальный номер для определения единственно возможного получателя данных в операционной системе.

Проникнув в компьютер, вирусы начинают заражать данные пользователя и открывают все ранее закрытые порты Windows для более быстрого распространения по системе. Чтобы этого не произошло, необходимо блокировать самые уязвимые порты, тем самым предотвратив возможность заражения.

Исследование самых крупных вирусных взломов показывает, что 80% паразитного трафика проходит через 4 порта, используемые для обмена данными между разными версиями ОС Windows. Наиболее уязвимыми открытыми портами Windows считаются: TCP порт 445 (он используется для обмена файлами); TCP порт 139 (предназначен для удаленного подключения к компьютеру); UDP порт 137 (служит для поиска информации на других компьютерах); TCP порт 135 (через него выполняются задания команд).

Закрытие портов возможно различными способами. Например, через командную строку - одновременно нажав сочетание клавиш Win+R, в появившейся командной строке вводим CMD и нажимаем на кнопку «ОК».

Появится окно командной строки Windows с чёрным фоном, в котором необходимо поочередно вводить определенные команды. После каждой введенной строчки нажимайте клавишу Enter для подтверждения действия.

1) netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=135 name=»Block1_TCP-135″ (команда для закрытия порта 135)

2) netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=137 name=»Block1_TCP-137″ (команда для закрытия порта 137)

3) netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=138 name=»Block1_TCP-138″ (команда для закрытия порта 138)

4) netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=139 name=»Block_TCP-139″ (команда для закрытия порта 139)

5) netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=445 name=»Block_TCP-445″ (команда для закрытия порта 445)

6) netsh advfirewall firewall add rule dir=in action=block protocol=tcp localport=5000 name=»Block_TCP-5000″

Как было сказано, шесть введённых команд необходимы для: закрытия 4-х уязвимых TCP-портов Windows (открытых по умолчанию), закрытия UDP-порта 138, а также закрытия порта 5000, который отвечает за выведение списка доступных сервисов.

Чтобы не использовать ручную работу с командной строкой, можно использовать стороннее программное обеспечение. Суть его работы сводится к такой же правке реестра, как в способе выше, только в визуальном отображении. Windows Doors Cleaner - это программа, которая легко может закрыть порты на компьютере (в Windows 10 – 7: старые версии ОС данная программа не поддерживает).

Утилита позволяет простым нажатием пяти кнопок отключить наиболее критические службы Windows (поддержка DCOM, RPC Locator,

NetBIOS, UPnP (Universal Plug and Play) и службы сообщений - Messenger) + закрыть порты, которые этими службами используются (135, 137, 138, 139, 445, 5000).

DCOM (Distributed COM) — расширение Component Object Model для поддержки связи между объектами на различных компьютерах по сети.

Локатор удаленного вызова процедур (RPC) (Remote Procedure Call (RPC) Locator). Системная служба локатора удаленного вызова процедур управляет базой данных службы имен RPC. Служба должна быть включена, чтобы клиенты RPC могли находить серверы RPC.

NetBIOS (Network Basic Input/Output System) — протокол для работы в локальных сетях на персональных ЭВМ типа IBM/PC, разработан в виде интерфейса, который не зависит от фирмы-производителя. Был разработан фирмой Sytek Corporation по заказу IBM в 1983 году. Он включает в себя интерфейс сеансового уровня (NetBIOS interface), в качестве транспортных протоколов использует TCP и UDP.

Использование UPnP для перенаправления порта UPnP - это расширение стандартов Plug-and-Play для упрощения управления устройствами в сети. В частности, программа на компьютере в локальной сети может обратиться к роутеру «на языке» UPnP и потребовать перенаправить на себя нужный порт.

Главный плюс приведенного способа в том, что с помощью этой программы можно не только закрыть порты, но и легко открыть. В то же время следует помнить, что рассмотренная программа Windows Doors Cleaner ни в коем случае не заменит установку Firewall. Установка программы Firewall и создание правил для закрытия портов – следующий необходимый шаг.

Несколько слов о брандмауэрах. Термин брандмауэр (нем. Brandmauer, от Brand — пожар и Mauer — стена) — глухая противопожарная стена здания или его английский эквивалент файрвол (англ. firewall; fire - огонь, wall – стена) используется также в значении «межсетевой экран».

Брандмауэр или firewall – это программный комплекс, предназначенный для защиты компьютера от сетевых атак. Следует отметить, что благодаря брандмауэрам увеличивается безопасность работы в сети, а также отражается большинство атак на компьютер путем фильтрации некоторых информационных пакетов. Поэтому настоятельно рекомендуется не отключать брандмауэр.

Если вас не устраивает стандартный брандмауэр (Пуск – ПАНЕЛЬ УПРАВЛЕНИЯ – Система и безопасность – Брандмауэр Windows) всегда можно поменять его на сторонний, но полностью отключать его и работать без брандмауэра весьма опасно. Могут использоваться универсальные решения для защиты компьютера и мобильных устройств от вирусов и других угроз.

В Kaspersky Internet Security защита порта реализуется через пункты меню: «Настройка», «Анти-Хакер». В разделе «Сетевой экран» нажимаем кнопку «Настройка», выбираем закладку «Правила для пакетов» и добавляем новое правило. В открывшемся окне заполняем «Имя правила». Вы можете назвать его как угодно. В поле «Параметры» отмечаем флажком «Локальный порт». Далее в описании нужно нажимать на подчеркнутые параметры для их изменения. Так нужно выставить параметры как видно на рис. 1. Запрещать – входящие – порт TCP – номер 1078 (информация с сайта https://2ip.ru).

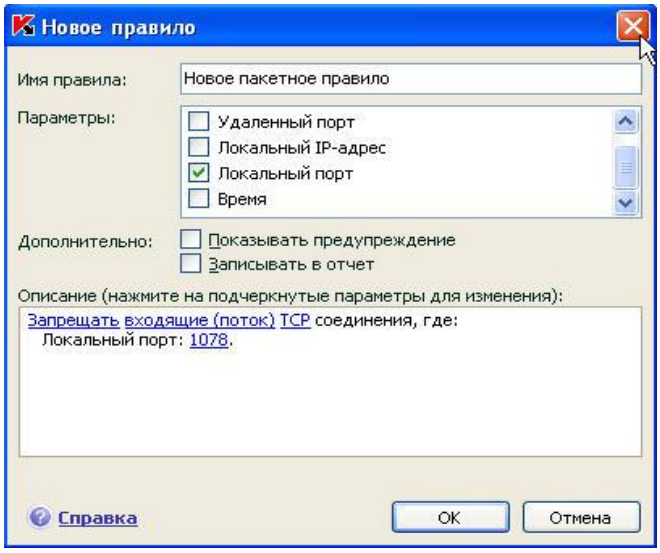

Рисунок 1 – Управление локальным портом

Kaspersky Internet Security позволяет:

- Сохранить безопасность операционной системы, файлов и персональных данных при работе в сети.
- Проверять на вирусы и другие угрозы отдельные файлы, папки, диски или выполнять полную проверку компьютера.
- Лечить зараженные файлы и удалить вирусы.
- Удалять рекламу и другие программы, которые замедляют работу компьютера.
- Искать и устанавливать обновления для программ на компьютере.
- Предотвращать установку ненужных программ на компьютер.
- Блокировать навязчивую рекламу в интернете с помощью Анти-Баннера.
- Запретить сайтам собирать информацию о ваших запросах.
- Безопасно делать покупки в интернете и оплачивать счета в онлайн-банке.
- Установить гибкие ограничения доступа к сайтам и программам для детей в зависимости от их возраста и опыта.
- Удаленно проверять на вирусы и обновлять защиту на всех ваших устройствах, подключенных к веб-порталу My Kaspersky.

Наилучшим решением в организации комплексной безопасности будет являться использование комплексных программных средств, сочетающих в себе антивирусное ПО, антиспам фильтр и межсетевой экран. Только в этом случае вы сможете получить действительно комплексную и всестороннюю защиту.

Дело в том, что firewall отслеживает все потенциально опасные подключения и блокирует их, тем самым надежно защищая личные данные пользователя. Однако не стоит путать сетевой экран (это еще одно название брандмауэра) с антивирусом.

Антивирусные приложения, как уже говорилось, предназначены для борьбы с угрозами, которые уже расположены на ПК или на съемных

носителях. В то же время антивирусы бессильны против сетевых атак. Брандмауэры же не следят за тем, что происходит на самом компьютере (если, конечно, это что-то не передает информацию в сеть). Их основной задачей является отслеживание именно сетевого трафика. Только совместное их использование может гарантировать полную безопасность компьютера.

Важно помнить, что сетевая безопасность может быть достигнута только комплексными действиями, нацеленными на закрытие всех уязвимостей вашего ПК.

Завершая изложение материала по данной теме можно сказать, что методы обеспечения информационной безопасности можно разделить на несколько групп:

1. Сервисы сетевой безопасности: криптографические методы защиты информации, идентификация и аутентификация пользователей, разграничение доступа, антивирусная защита, системы анализа сетевых атак.

2. Аппаратные методы: защита информации от утечки по техническим каналам (например, за счет перехвата электромагнитного излучения или речевой информации).

3. Организационные (действия общего характера, предпринимаемые руководством организации: создание службы охраны, организация механизма контроля над перемещениями сотрудников и посетителей).

4. Правовые методы (защита авторских прав, лицензирование и сертификация).