Содержание:

Введение

С появлением самых ранних средств связи дипломаты и военные деятели осознали необходимость разработки механизмов защиты конфиденциальной корреспонденции и способов выявления попыток её фальсификации . Например, Юлию Цезарю приписывают изобретение около 50 года до н. э. шифра Цезаря, который был предназначен для предотвращения чтения его секретных сообщений, теми, кому они не были предназначены. Хотя, по большей части, защита обеспечивалась контролем за самой процедурой обращения с секретной корреспонденцией.

Конфиденциальные сообщения помечались с тем, чтобы их защищали и передавали только с доверенными лицами под охраной, хранили в защищённых помещениях или прочных шкатулках. С развитием почты стали возникать правительственные организации для перехвата, расшифровки, чтения и повторного запечатывания писем. Так в Англии для этих целей в 1653 году появилась Тайная канцелярия.

В России перлюстрация осуществлялась, по крайней мере, со времен Петра I — с 1690 года в Смоленске вскрывались все письма, идущие за границу, а системный характер практика тайного копирования корреспонденции всех иностранных дипломатов так, чтобы у адресата не возникло никаких подозрений, приобрела в середине XVIII века.

В середине XIX века появились более сложные системы классификации секретной информации, позволяющие правительствам управлять информацией в зависимости от степени её конфиденциальности. Например, британское правительство до некоторой степени узаконило в 1889 году такую классификацию публикацией Закона о государственной тайне. Во время Первой мировой войны многоуровневые системы классификации использовались для передачи информации на различных фронтах, что способствовало интенсивному использованию подразделений шифрования и криптоанализа в дипломатических миссиях и армейских штабах.

В межвоенный период системы шифрования всё более усложнялись, так что для зашифровывания и расшифровывания секретных сообщений стали использовать специальные машины, из которых наиболее известной является «Энигма», созданая немецкими инженерами в 1920-х годах. Уже в 1932 году шифр «Энигмы» удалось расшифровать Бюро шифров польской разведки методом обратной разработки.

Объём информации, которой обменивались страны антигитлеровской коалиции в ходе Второй мировой войны потребовал формального совмещения национальных систем классификации и процедурных контролей. Сформировался доступный лишь посвящённым набор грифов секретности, определяющих, кто может обращаться с документами (как правило, офицеры, нежели рядовые), и где их следует хранить, учитывая прогресс в разработке всё более сложных сейфов и хранилищ. В Великобритании криптоанализом сообщений противника, зашифрованных с помощью «Энигмы», успешно занималась группа под руководством Алана Тьюринга. Разработанная ими дешифровальная машина «Turing Bombe» (с англ. — «бомба Тьюринга»), оказала значительную помощь антигитлеровской коалиции, а иногда ей приписывается решающая роль в победе союзников. В США для шифрования радиопереговоров на Тихоокеанском театре военных действий набирали связистов из индейского племени Навахо, язык которого за пределами США никто не знал, японцам так и не удалось подобрать ключ к этому экзотическому методу защиты информации.

В СССР с 1930-х годов для защиты телефонных переговоров высших органов управления страной (в том числе, Ставки Верховного Главнокомандования) использовалась так называемая ВЧ-связь, на голосовой модуляции высокочастотного сигнала и последующего скремблирования. Однако отсутствие криптографической защиты позволяло, используя спектрометр, восстанавливать сообщения в перехваченном сигнале.

Развитие вычислительной техники, появление удаленных терминалов, а затем и персональных компьютеров радикально изменило ситуацию. А появление и широкое распространение локальных и глобальных компьютерных сетей с одной стороны и мобильных накопителей большого объема в сочетании с возможностью фото и видеосъемки недорогими и компактными устройствами с другой стороны потребовало полного изменения подхода к данной проблеме.

В настоящее время стремительный рост компьютеризации позволил обеспечить быстрое развитие науки, техники, культуры, а также изменение образа жизни людей. Одновременно недостаточная защищенность компьютерных сетей от технических сбоев и несанкционированного доступа, а также ошибочных действий персонала значительно повышает риск возникновения нештатных ситуаций, способных вызвать непредсказуемые последствия вплоть до техногенных катастроф.

Глава 1. Виды угроз информационной безопасности.

Угрозы информационной безопасности.

Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Угроза (действие)- это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу

проявляющегося в опасности искажения и потери информации.

Фактор (уязвимость)– это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы,

протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Последствия (атака) – это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Проявления возможного ущерба могут быть различны:

-моральный и материальный ущерб деловой репутации организации;

-моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

-материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

-материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

-материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;

-моральный и материальный ущерб от дезорганизации деятельности организации;

-материальный и моральный ущерб от нарушения международных отношений.

Ущерб может быть причинен каким-либо субъектом и в этом случае имеется на лицо правонарушение, а также явиться следствием независящим от субъекта проявлений (например, стихийных случаев или иных

воздействий, таких как проявления техногенных свойств цивилизации). В первом случае налицо вина субъекта, которая определяет причиненный вред как состав преступления, совершенное по злому умыслу (умышленно, то есть деяние, совершенное с прямым или косвенным умыслом) или по неосторожности (деяние, совершенное по легкомыслию, небрежности, в результате невиновного причинения вреда) и причиненный ущерб должен квалифицироваться как состав преступления, оговоренный уголовным правом. Приложение 1

Во втором случае ущерб носит вероятностный характер и должен быть сопоставлен, как минимум с тем риском, который оговаривается гражданским, административным или арбитражным правом, как предмет

рассмотрения.

В теории права под ущербом понимается невыгодные для собственника имущественные последствия, возникшие в результате правонарушения. Ущерб выражается в уменьшении имущества, либо в недополучении дохода, который был бы получен при отсутствии правонарушения (упущенная выгода).

Вот некоторые примеры составов преступления, определяемых Уголовным Кодексом Российской Федерации.

-Хищение – совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу

имущества.

-Копирование компьютерной информации – повторение и устойчивое запечатление информации на машинном или ином носителе.

-Уничтожение – внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению.

-Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.

-Уничтожение компьютерной информации – стирание ее в памяти ЭВМ.

-Повреждение – изменение свойств имущества, при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования.

-Модификация компьютерной информации – внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.

-Блокирование компьютерной информации – искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

-Несанкционированное уничтожение, блокирование модификация, копирование информации – любые не разрешенные законом, собственником или компетентным пользователем указанные действия с

информацией.

-Обман (отрицание подлинности, навязывание ложной информации) – умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким

образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности

Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Под угрозой интересам субъектов информационных отношений понимают потенциально возможное событие, процесс или явление которое посредством воздействия на информацию или другие компоненты информационной системы может прямо или косвенно привести к нанесению ущерба интересам данных субъектов. Приложение2.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

-По аспекту информационной безопасности, на который направлены угрозы:

-Угрозы конфиденциальности (неправомерный доступ к информации). Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой. В связи с угрозой нарушения конфиденциальности, используется термин «утечка». Подобные угрозы могут возникать вследствие «человеческого фактора» (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств. К информации ограниченного доступа относится государственная тайна и конфиденциальная информация (коммерческая тайна, персональные данные, профессиональные виды тайна: врачебная, адвокатская, банковская, служебная, нотариальная, тайна страхования, следствия и судопроизводства, переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений (тайна связи), сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации (ноу-хау) и др.).

-Угрозы целостности (неправомерное изменение данных). Угрозы нарушения целостности – это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования.

-Угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы). Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

По расположению источника угроз:

-Внутренние (источники угроз располагаются внутри системы);

-Внешние (источники угроз находятся вне системы).

По размерам наносимого ущерба:

-Общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);

-Локальные (причинение вреда отдельным частям объекта безопасности);

-Частные (причинение вреда отдельным свойствам элементов объекта безопасности).

По степени воздействия на информационную систему:

-Пассивные (структура и содержание системы не изменяются);

-Активные (структура и содержание системы подвергается изменениям).

По природе возникновения:

-Естественные (объективные) — вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;

-Искусственные (субъективные) — вызванные воздействием на информационную сферу человека. Среди искусственных угроз в свою очередь выделяют:

-Непреднамеренные (случайные) угрозы — ошибки программного обеспечения, персонала, сбои в работе систем, отказы вычислительной и коммуникационной техники;

-Преднамеренные (умышленные) угрозы — неправомерный доступ к информации, разработка специального программного обеспечения, используемого для

осуществления неправомерного доступа, разработка и распространение вирусных программ и т.д. Преднамеренные угрозы обусловлены действиями людей. Основные проблемы информационной безопасности связаны прежде всего с умышленными угрозами, так как они являются главной причиной преступлений и правонарушений.

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления, например, конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Все источники угроз информационной безопасности можно разделить на три основные группы:

-Обусловленные действиями субъекта (антропогенные источники) – субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированы как умышленные или случайные преступления. Источники, действия которых могут привести к нарушению безопасности информации могут быть как внешними так и внутренними. Данные источники можно спрогнозировать, и принять адекватные меры.

-Обусловленные техническими средствами (техногенные источники) – эти источники угроз менее прогнозируемы, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внутренними, так и внешними.

-Стихийные источники – данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить), такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Такие источники угроз совершенно не поддаются прогнозированию и, поэтому меры против них должны применяться всегда. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы.

Все источники угроз ИБ можно разделить на классы, обусловленные типом носителя угрозы (источника угрозы):

-Антропогенные источники (обусловленные действиями субъекта);

-Техногенные источники (обусловленные техническими средствами);

-Стихийные источники (обусловленные природными явлениями).

Далее классы источников угроз делят на группы по местоположению источника угроз:

-Внешние источники (находящиеся вне объекта);

-Внутренние источники (находящиеся внутри объекта).

Антропогенные источники угроз.

Антропогенные источники угроз ИБ представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта (нарушителя) всегда можно оценить, спрогнозировать и принять адекватные меры.

Методы противодействия в этом случае управляемы и напрямую зависят от воли и желания организаторов защиты информации.

К антропогенным источникам угроз относятся субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления.

Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации.

К ним относятся:

-криминальные структуры;

-потенциальные преступники и хакеры;

-недобросовестные партнеры;

-технический персонал поставщиков телематических услуг;

-представители надзорных организаций и аварийных служб;

-представители силовых структур.

Внутренние источники, как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети.

К ним относятся:

-основной персонал (пользователи, программисты, разработчики);

-представители службы защиты информации;

-вспомогательный персонал (уборщики, охрана);

-технический персонал (систем жизнеобеспечение, эксплуатация).

Техногенные источники угроз.

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.
-Технические средства, являющиеся источниками потенциальных угроз безопасности информации так же могут быть внешними

средства связи;

-сети инженерных коммуникации (водоснабжения, канализации);

транспорт.

-некачественные технические средства обработки информации;

-некачественные программные средства обработки информации;

- вспомогательные средства (охраны, сигнализации, телефонии);

-другие технические средства, применяемые в учреждении;

Стихийные источники угроз.

Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.
Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы :

-пожары;

-землетрясения;

-наводнения;

-ураганы;

-различные непредвиденные обстоятельства;

-необъяснимые явления;

-другие форс-мажорные обстоятельства

Глава 2. Угрозы и уязвимости информационной безопасности.

Компьютерные вирусы.

Компьютерные вирусы одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

Современный компьютерный вирус – это практически незаметный для обычного пользователя "враг", который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности. Приложение 3.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Вирусные эпидемии способны блокировать работу организаций и предприятий.

Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно.

В последнее время вирусные эпидемии стали настолько масштабными и угрожающими, что сообщения о них выходят на первое место в мировых новостях. При этом следует иметь в виду, что антивирусные программы и аппаратные средства не дают полной гарантии защиты от вирусов, а большинство пользователей не имеют даже основных навыков "защиты" от вирусов.

Термин "компьютерный вирус" появился в середине 80-х годов, на одной из конференций по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако, строгого определения компьютерного вируса так и нет.

Трудность, возникающая при попытках сформулировать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и др.) либо присущи другим программам, которые никакого отношения не имеют к вирусам, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

Основная особенность компьютерных вирусов заключается в возможности их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые не являются вирусами, но именно эта особенность является обязательным (необходимым) свойством компьютерного вируса. К более полной характеристике современного компьютерного вируса следует добавить способность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТе Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения".

Программный вирус– это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Исходя из этого, необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной "компьютерной гигиены".

Безопасность паролей.

Сложность (или сила, стойкость) пароля — мера оценки времени, которое необходимо затратить на угадывание пароля или его подбор каким-либо методом, например, методом полного перебора. Оценка того, как много попыток (времени) в среднем потребуется взломщику для угадывания пароля. Другое определение термина — функция от длины пароля, его запутанности и непредсказуемости.

Слабый пароль — пароль, который может быть легко угадан или подобран методом полного перебора. Сильный пароль — пароль, который трудно угадать и долго подбирать методом полного перебора.

Использование сложных паролей увеличивает время, необходимое взломщику для подбора пароля, не отменяет необходимости использования других мер

безопасности. Эффективность пароля заданной силы зависит от проектирования и реализации программного обеспечения систем аутентификации, в частности, от того, насколько быстро система аутентификации будет отвечать атакующему при его попытках подобрать пароль, и как надёжно хранится и передаётся информация о пароле. Риски также представлены некоторыми способами взлома безопасности компьютера, не относящимися к сложности пароля. Это такие методы как фишинг, кейлоггинг, телефонная прослушка, социальная инженерия, поиск полезной информации в мусоре, атака по сторонним каналам, уязвимости в программном обеспечении, бэкдоры,эксплойты.

Существуют два фактора, определяющих сложность пароля:

-лёгкость, с которой атакующий может проверить истинность угадываемого пароля;

-среднее количество попыток, которые атакующий должен предпринять, чтобы найти правильный пароль.

Первый фактор определяется тем, как пароль хранится, и тем, для чего он используется. Второй фактор определяется длиной пароля, набором используемых символов и тем, как пароль был создан.

Пароли создаются или автоматически (с использованием генераторов случайных чисел), или человеком. Стойкость пароля к атаке методом полного перебора может быть вычислена точно. В большинстве случаев пароли создаются людьми, например, во время создания аккаунтов для компьютерных систем или веб-сайтов. Люди создают пароли, руководствуясь советами или набором правил, но при этом склонны следовать шаблонам, что играют на руку атакующему. Списки часто выбираемых паролей распространены для использования в программах угадывания паролей.

Несколько десятилетий анализа паролей в многопользовательских компьютерных системах показали, что больше 40 % паролей легко отгадать, используя только компьютерные программы, и ещё больше можно отгадать, когда во время нападения учитывается информация о конкретном пользователе.

Автоматическая генерация паролей, если она выполнена должным образом, помогает избежать всякой связи между паролем и его пользователем. Например, имя домашнего питомца пользователя вряд ли сгенерируется такой системой. Для пароля, выбранного из достаточно большого пространства возможностей, полный

перебор может стать практически невозможным. Однако действительно случайные пароли может быть сложно сгенерировать и, как правило, пользователю их сложно запомнить.

Рекомендации по выбору хорошего пароля составлены для того, чтобы сделать пароль более стойким к разнообразным ухищрениям взломщиков.

Минимально рекомендуемая длина пароля — в пределах от 12 до 14 символов. Увеличение длины пароля всего на 2 символа даёт в 500 раз больше вариантов, чем увеличение алфавита на 18 символов.

Рекомендуется генерировать случайные пароли, если это возможно.

Рекомендуется избегать использования паролей, содержащих словарные слова («password»), повторяющиеся наборы букв («passpass»), буквенные или числовые последовательности («ааа», «123»), ники, имена (собственное имя, имена родственников), клички домашних животных, романтические отсылки (нынешние или прошлые), биографическую информацию.

Рекомендуется включать в пароль цифры и иные символы, если это разрешено системой.

Рекомендуется использовать как прописные, так и строчные буквы, когда это возможно. Однако может быть лучше добавить к паролю слово, чем каждый раз нажимать и отпускать в нужных местах клавишу Shift.

Рекомендуется избегать использования одного пароля для различных сайтов или целей.

Некоторые рекомендации советуют никуда не записывать пароль, в то время как другие, отмечая существование большого количества защищённых паролем систем, к которым пользователь должен иметь доступ, одобряют идею записывания паролей, если, конечно, список паролей будет находиться в надёжном месте.

Некоторые похожие пароли оказываются слабее, чем другие. Например, разница между паролем, состоящим из словарного слова, и паролем, состоящим из слова спутанного (то есть слова, буквы в котором заменены на, скажем, цифры сходного начертания, например: «о» на «0», «ч» на «4»), может стоить прибору для взлома паролей несколько лишних секунд — это добавляет к паролю немного сложности. В приведённых ниже примерах показаны разнообразные способы создания слабых

паролей. В способах используются простые шаблоны, чем и объясняется низкая энтропия получаемых паролей — лёгкость их угадывания.

Пароли по умолчанию: «password», «default», «admin», «guest» и другие. Список паролей по умолчанию широко распространён по интернету.

-Словарные слова: «chameleon», «RedSox», «sandbags», «bunnyhop!», «IntenseCrabtree» и другие, включая слова из неанглийских словарей.

-Слова с добавленными числами: «password1», «deer2000», «ivan1234» и другие. Подбор подобных паролей осуществляется очень быстро.

-Слова с заменёнными буквами: «p@ssw0rd», «l33th4x0r», «g0ldf1sh» и другие. Подобные пароли могут быть проверены автоматически с небольшими временными затратами.

-Слова, составленные из двух слов: «crabcrab», «stopstop», «treetree», «passpass» и другие.

-Распространённые последовательности на клавиатуре: «qwerty», «12345», «asdfgh», «fred» и другие.

-Широко известные наборы цифр: «911», «314159…», «271828…», «112358…» и другие.

Личные данные: «ivpetrov123», «1/1/1970», номер телефона, имя пользователя, ИНН, адрес и другие.

У пароля существует много других возможностей оказаться слабым, судя по сложности некоторых схем атак; главный принцип в том, чтобы пароль обладал высокой энтропией, а не определялся каким-либо умным шаблоном или личной информацией. Онлайн-сервисы часто предоставляют возможность восстановить пароль, которой может воспользоваться хакер и узнать таким образом пароль. Выбор сложного для угадывания ответа на вопрос поможет защитить пароль.

Людям обычно советуют никогда и нигде не записывать свои пароли и никогда не использовать один пароль для разных аккаунтов. Несмотря на это обычные пользователи могут иметь десятки аккаунтов и могут использовать один и тот же пароль для всех аккаунтов. Чтобы не запоминать множество паролей, можно использовать специальное программное обеспечение — менеджер паролей, которое позволяет хранить пароли в зашифрованной форме. Также можно

зашифровать пароль вручную и записать шифрограмму на бумаге, при этом запомнив метод расшифровки и ключ. Ещё можно слегка менять пароли для обычных аккаунтов и выбирать сложные и отличающиеся друг от друга пароли для высокоценных аккаунтов, таких как, например, интернет-банкинг.

Менеджер паролей — компьютерная программа, позволяющая пользователю использовать множество паролей и, возможно, требующая ввода одного пароля для доступа к хранимым паролям. Пароль к менеджеру паролей, естественно, должен быть как можно более сложным и не должен быть нигде записан.

Уязвимости информационной безопасности.

Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости (факторы), приводящие к нарушению безопасности информации на конкретном объекте информатизации. Приложение 4.

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации) Кроме того, возможно не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть:

-Объективными

-субъективными

-случайными.

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации. К ним можно отнести:

-сопутствующие техническим средствам излучения

-электромагнитные (побочные излучения элементов технических средств , кабельных линий технических средств , излучения на частотах работы генераторов , на частотах самовозбуждения усилителей)

-электрические (наводки электромагнитных излучений на линии и проводники , просачивание сигналов в цепи электропитания, в цепи заземления , неравномерность потребления тока электропитания [3])

-звуковые (акустические , виброакустические)

активизируемые

-аппаратные закладки (устанавливаемые в телефонные линии , в сети электропитания , в помещениях , в технических средствах)

-программные закладки (вредоносные программы , технологические выходы из программ , нелегальные копии ПО)

определяемые особенностями элементов

-элементы, обладающие электроакустическими преобразованиями (телефонные аппараты , громкоговорители и микрофоны , катушки индуктивности , дроссели, трансформаторы и пр.)

элементы, подверженные воздействию электромагнитного поля (магнитные носители , микросхемы , нелинейные элементы, поверженные ВЧ навязыванию) определяемые особенностями защищаемого объекта

местоположением объекта (отсутствие контролируемой зоны , наличие прямой видимости объектов , удаленных и мобильных элементов объекта , вибрирующих

отражающих поверхностей) организацией каналов обмена информацией (использование радиоканалов , глобальных информационных сетей , арендуемых каналов)

Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами:

-Ошибки при подготовке и использовании программного обеспечения (при разработке алгоритмов и программного обеспечения, инсталляции и загрузке программного обеспечения , эксплуатации программного обеспечения , вводе данных)

-при управлении сложными системами (при использовании возможностей самообучения систем , настройке сервисов универсальных систем, организации управления потоками обмена информации)

- при эксплуатации технических средств (при включении/выключении технических средств , использовании технических средств охраны , использовании средств обмена информацией)

нарушения

-режима охраны и защиты (доступа на объект , доступа к техническим средствам)

-режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения)

-режима использования информации (обработки и обмена информацией , хранения и уничтожения носителей информации , уничтожения производственных отходов и брака)

режима конфиденциальности (сотрудниками в нерабочее время , уволенными сотрудниками).

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности:

-сбои и отказы

-отказы и неисправности технических средств (обрабатывающих информацию , обеспечивающих работоспособность средств обработки информации , обеспечивающих охрану и контроль доступа)

старение и размагничивание носителей информации (дискет и съемных носителей , жестких дисков , элементов микросхем , кабелей и соединительных линий)

-сбои программного обеспечения (операционных систем и СУБД , прикладных программ , сервисных программ , антивирусных программ

сбои электроснабжения (оборудования, обрабатывающего информацию , обеспечивающего и вспомогательного оборудования

повреждения жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации , кондиционирования и вентиляции)

ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий , корпусов технологического оборудования)

Статистические данные информационная безопасность в России.

Специалисты компании Positive Technologies выяснили, сколько стоит информационная безопасность в России. В опросе участвовали представители 170 российских компаний — руководители IT- и ИБ-подразделений и директора.

По объему бюджета на обеспечение информационной безопасности на фоне остальных компаний существенно выделяются некоторые банки и госорганизации. Это неудивительно, учитывая, что правительство РФ взяло курс на «цифровую экономику». Так, госорганизации выделяют на информбезопасность до 800 млн рублей в год, а финансовые учреждения — до 300 млн рублей.

До 50 млн рублей в год на обеспечение кибербезопасности выделяют IT и промышленная отрасли, а также транспортный сектор. Большую сумму денег расходуют компании, занятые в промышленности.

Меньше всего тратят компании, занятые в сфере образования: в некоторых случаях их годовой бюджет, выделяемый на защиту информации, не превышает 1 млн рублей.

Аналитики Positive Technologies отмечают. Такое распределение ресурсов, прежде всего, связано с общими бюджетами компаний, которые в крупных государственных учреждениях в разы больше, чем в других организациях. Более того, подразделение, отвечающее непосредственно за информационную безопасность, имеется лишь в 44% компаний-респондентов, в остальных организациях необходимые функции выполняются специалистами IT-отдела.

Как показали недавние киберэпидемии, во многих отечественных (да и в зарубежных тоже) компаниях все еще экономят на информбезопасности. Руководство российских компаний все еще склонно считать чрезмерные затраты на обеспечение ИБ лишними, считая, что кибератаки вполне способен предотвратить IT-отдел. Но это давно уже не так.

Рынок информационной безопасности в России показывает постоянный рост: год от года увеличиваются бюджеты на ИБ, создаются новые подразделения, нацеленные на обеспечение кибербезопасности, видим, как в их арсенале появляются новейшие технологии, строятся центры мониторинга и реагирования на инциденты информационной безопасности. И при всем этом общее число инцидентов, происходящих в мире (и в России в частности), также год от года растет: они приобретают все большую массовость и все чаще оборачиваются крупномасштабными эпидемиями, ущерб от которых также становится все ощутимее — от нарушения работы отдельных сервисов до полной остановки бизнес-процессов со всеми вытекающими последствиями.

Как выяснилось, **более 92,6% компаний сталкивалась с утечкой информации**. Эта цифра наводит на грустные размышления, ведь если интерпретировать данные на весь рынок, оказывается, что только у одной компании из 10 есть мизерный шанс избежать нелегкой участи жертвы.

В 55,2% случаев причиной утечки являются целенаправленные действия сотрудников. Работники крадут данные по различным причинам: продать конкурентам, для портфолио или для развития собственного бизнеса.

Из-за небрежного поведения персонала, например отправки документов или сообщений не по тому адресу, случайному предоставлению логинов и паролей третьим лицам и так далее, происходит порядка 23,6% утечек. И в 21% случаев информация оказывается вне стен компании из-за действий хакеров или вирусов.

Благодаря действиям инсайдеров компания теряет ценные коммерческие данные и новые разработки в 61,5% ситуаций.

В 37% случаев сотрудник превращается в крота при составлении портфолио. Не отстают и желающие продать информацию конкурентам, таких также 37%. Самые хитрые развивают свой бизнес за счет ресурсов компании, их — 26%.

Лидерами, среди похитителей являются работники отдела продаж – 25,4%. Остальной «ТОП» распределился следующим образом:

Руководители среднего звена – 23,5%;ТОП-менеджеры – 21,5%; Стажеры, фрилансеры, временные подрядчики – 11,7%; Системные администраторы – 7,8%; Секретари – 3,9%; Сотрудники бухгалтерии – 1,9%. Остальной персонал – 4,3%.

По мнению 59% респондентов, на сегодняшний день самая приоритетная угроза – внутренняя, сотрудники компании могут легко получить доступ к ценной информации и легко воспользоваться ей в своих корыстных целях. 33% полагает, что наиболее опасны для сохранности данных неосторожные действия персонала, совершаемые без коварного умысла. И только 8% опасаются действий хакеров.

Как оказалось, три самые важные причины, благодаря которым сотрудник может совершить кражу:

-Отсутствие систем контроля персонала и перемещения информации – 41,6%;

-Отсутствие персональной ответственности – 34,7%;

-Большой круг лиц имеет доступ к информации – 23,7%.

-В 46% случаев инциденты ведут к безвозвратной потере данных. Причины:

-Целенаправленное вредительство – 36,3%;

-Необдуманные действия персонала – 31,9%;

-Действия третьих лиц извне – 31,3%.

По мнению участников опроса, наибольшую ценность для компании представляет:

-Информация о клиентах – 27,4%;

-Интеллектуальная собственность и новые разработки – 24,6%;

-Юридическая и финансовая документация – 23,3%;

-Логины и пароли – 18,2%;

-Личные данные сотрудников – 6,5%.

Не удивительно, что в такой ситуации полностью доверяют персоналу только 10,7% опрошенных. Однако, учитывая, что тренинги по информационной безопасности проводят 51,9%, а в 77,8% случаев работники компаний письменно уведомлены о личной ответственности за сохранность данных, можно с уверенностью сделать вывод: инсайдер – больше не мифическая угроза и это осознает большинство представителей бизнеса.

К счастью, вирусы-шифровальщики еще не настолько распространены, однако риски с каждым годом растут: более 48% респондентов уже столкнулась с этой угрозой. А вот фишинг достиг массовых масштабов – 75% опрошенных получали «письма счастья».

Ситуация с планомерной защитой информации выглядит достаточно оптимистично:

-66,7 — делают резервные копии информации несколько раз в месяц;

-14,8% — один раз в месяц;

-7,4% — раз в квартал;

-И только 11,1% — раз в год или реже.

Большинство опрошенных серьезно подходят к обновлению кодов доступа к ценным данным и корпоративным аккаунтам:

-10,7% — меняют логины и пароли несколько раз в месяц;

-28,6% — один раз в месяц;

-25% — раз в квартал;

-14,3% — раз в полугодие;

-И только 7,1% — пренебрегает этой задачей на регулярной основе.

Мониторинг и контроль действий персонала ведут 71,4% участников исследования, а вот анализ трафика и перемещения ценных данных внедрен только у 35,7%. Популярный набор средств защиты информации, выглядит не так радужно. Многие все еще пренебрегают современными высокотехнологичными решениями, предпочитая надеяться на старый, добрый антивирус.

Грубые попытки просочиться через периметр информационной безопасности постепенно отходят в прошлое. Из-за трудозатрат, стоимости операций и необходимого уровня знаний хакеров подобных угроз стоит опасаться только крупным корпорациям. «Взламывать» средний и малый бизнес экономически невыгодно.

При этом с каждым годом набирает обороты «народный» инструмент – фишинг. 75% участников исследования уже столкнулись с этой проблемой. И это не предел, риски будут расти. Подготовка многоходовой атаки с рассылкой писем или звонков по телефону, вредоносными вложениями и клонами сайтов, обходится в несколько сотен долларов. А для проведения операции хватит навыков учащихся старших классов.

2017 стал революционным, дополнив фишинг новым опасным инструментом – вирусами-шифровальщиками. Конечно, о них было известно и до 2017 года, однако жертвами, чаще всего, становились рядовые пользователи. WannaCry и PetyaA начали новую эпоху, в которой определение «информационный терроризм» перестало быть пустым звуком. Блэкаут, столь любимый хакерами и фанатами киберпанка – уже не просто сетевая страшилка, а объективная реальность. Даже пробный массовый выход на сцену вирусов-шифровальщиков умудрился поставить тысячи компаний России и Европы на колени.

Внешние угрозы никогда не потеряют актуальность. Но уже очевидно, что век простого взлома канул в Лету. Будущее за социальной инженерией, фишингом и другими комбинациями цифровых атак, которые нацелены не на бездушную машину, а на главную уязвимость любой системы защиты – человека. Методы и приёмы злоумышленников будут совершенствоваться, а финансовые потери бизнеса – расти. Практически с полной уверенностью можно предположить, что в 2018 мир услышит о новых громких и крупномасштабных акциях.

На данный момент единственный способ существенно снизить риски – эшелонированная комплексная система безопасности, анализирующая трафик, контент, абсолютно все каналы коммуникаций, предиктивно оценивающая риски и, конечно же, всесторонне изучающая действия пользователей.

По данным зарубежных исследований около 90% компаний считают приоритетной угрозой – действия инсайдеров. А 53% теряли данные из-за целенаправленных или необдуманных действий персонала.

Наше исследование продемонстрировало: порядка 78% респондентов сталкивались с различными проявлениями вредительства со стороны персонала. А в 61% случаев подобные ситуации привели к реальным убыткам для компании.

Будущее нельзя назвать безоблачным. Явление «инсайдерства» базируется на трех пороках, идущих рука об руку с человечеством: жадности, глупости, мести. Всегда найдутся сотрудники, которые захотят немного подзаработать на стороне или воспользоваться ресурсами компании в личных целях. Никуда не денутся рассеянные и невнимательные, бездумно копирующие конфиденциальную информацию туда-сюда и не глядя пересылающие файлы по почте. Обиженные работники, воспылавшие праведным гневом к «злобному» работодателю, который их не ценит, или того хуже – уволил, не испаряться в одночасье. Поменяются только инструменты, которые эволюционируют из года в год.

Если каких-нибудь 5-10 лет назад украсть информацию можно было распечатав документы, отправив на почту или скопировав на флешку. Сейчас к этим каналам добавились десятки разнообразных мессенджеров, социальных сетей и облачных хранилищ, которые поддерживают отправку практически всех типов файлов.

С «кротами» бороться можно и нужно. Для этого необходимо регулярно делать бекапы ценных данных, внедрить жесткий контроль перемещения каждого бита информации в совокупности с беспрерывным мониторингом и анализом поведения персонала. И переборщить в этом вопросе просто невозможно. Каждая поблажка – целенаправленно закрытые глаза на питательную среду, в которой может внезапно зародиться инсайдер.

Тенденции осознания бизнесом реальности информационной угрозы внушают оптимизм. Пожалуй, главное достижение как зарубежных, так и отечественных компаний – комплексный подход к защите информации.

Опросы, проведенные в различных организациях Европы и США, утверждают: 94% респондентов внедрили те или иные технологии анализа поведения пользователей, а 93% — тщательно контролируют доступ к ценной информации.

Бизнес в России несколько отстает: мониторинг пользователей ведут 71,4%, а анализ перемещения данных — 35,7%. 66% участников исследования не забывают про резервные копии и делают их раз в месяц.

Не смотря на значительную разницу в цифрах, можно смело утверждать: к концу года уровень защиты информации в российском бизнесе сократит разрыв с

зарубежными коллегами. Реальность угрозы осознана и механизм запущен.

Стоит выделить еще одну положительную тенденцию. Комплексный подход к защите данных – маркер эволюции отечественных компаний. Перестройка с хаотичной реакции при малейших изменениях рынка и экономики на планомерную работу, включающую в себя долгосрочное планирование и упорядочивание внутренних процессов, уже идет полным ходом. И, как следствие, игроки, осознавшие все плюсы систематичности и стратегического планирования, имеют все шансы увеличить продажи и выйти в лидеры отрасли. Главное – своевременно обеспечить защиту и будущее компании, внедрив современные технические решения.

Угрозы кибератак.

3,3 миллиона долларов в год в среднем теряет одна российская компания из-за кибератак, в Великобритании средние ежегодные убытки одной компании от проделок хакеров составляют около 5,9 миллиона долларов, в Германии — 8,13 миллиона, а в США — 12,6 миллиона.

Так, например, Чаще всего информационная безопасность крупных компаний страдает из-за действий самих сотрудников. Их некомпетентность приводит к 18 % потерь. Ещё 14 % объясняются сбоями в работе IT-систем, а 10 % — кражей или потерей личных мобильных устройств. У представителей малого и среднего бизнеса проблемы возникают по другим причинам: 24 % потерь приходятся на кибератаки, а ещё 23 % связаны с заражением компьютеров вирусами.

Нет ни одной сферы общественной деятельности, которая не была бы интересна хакерам. На одни компании нападают в поисках конфиденциальной информации, на другие — с целью наживы, а кто-то и вовсе становится случайной жертвой массовой атаки.

Целевые атаки на объекты критической инфраструктуры могут приводить к серьезным последствиям и даже потенциально к человеческим жертвам, но наиболее частым последствием является утечка конфиденциальной информации.

Нормативные документы в области информационной безопасности.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

-Акты федерального законодательства:

-Международные договоры РФ;

-Конституция РФ;

-Законы федерального уровня (включая федеральные конституционные законы, кодексы);

-Указы Президента РФ;

-Постановления Правительства РФ;

-Нормативные правовые акты федеральных министерств и ведомств;

-Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Подробнее списки и содержание указанных нормативных документов в области информационной безопасности обсуждаются в разделе Информационное право.

К нормативно-методическим документам можно отнести;

-Методические документы государственных органов России:

Доктрина информационной безопасности РФ;

-Руководящие документы ФСТЭК (Гостехкомиссии России);

Приказы ФСБ;

-Стандарты информационной безопасности, из которых выделяют:

-Международные стандарты;

-Государственные (национальные) стандарты РФ;

-Рекомендации по стандартизации;

-Методические указания.

Заключение

Прежде всего, проблема информационной безопасности - это проблема выбора человека - выбора воспринимаемой информации, поведения в обществе и государстве, выбора круга общения. Необходимо точное понимание и опознавание себя в мире, в обществе, осознания целей и средств для их достижения, сознательно обрабатывать информацию и транслировать только проверенную, точную и объективную информацию.

Информация, бесспорно, выступает основой всего процесса управления в организации, труд управленца и заключается в ее сборе, изучении, обработке и грамотном толковании. От уровня организации сбора, обработки и передачи информации в целом зависит эффективность управления, а так же качество принимаемых управленческих решений в частности.

Список источников

https://ru.wikipedia.org/wiki/Информационная_безопасность
https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности

https://studfiles.net/preview/4349833/page:13/

https://studfiles.net/preview/6379760/page:24/

https://ru.wikipedia.org/wiki/Сложность_пароля

https://studopedia.ru/8_186624_klassifikatsiya-uyazvimostey-bezopasnosti.html

https://ceur.ru/news/921/item317493/

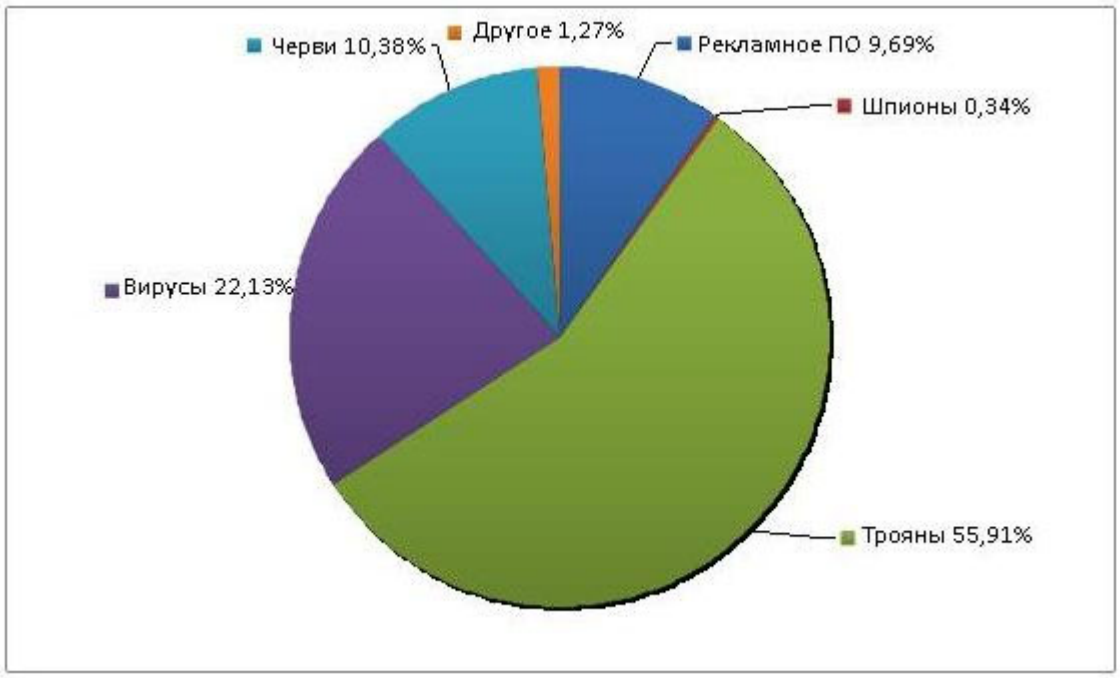
https://stakhanovets.ru/blog/issledovanie-ugrozy-informacionnoj-bezopasnosti-chast-2-trendy-i-prognozy-2018/

Приложение

Приложение 1

Приложение 2

Прилодение3



Приложение 4