Информационная безопасность

«Информационная безопасность» — это процесс обеспечения доступности, целостности и конфиденциальности информации.

Под «доступностью» понимается соответственно обеспечение доступа к информации.

«Целостность» — это обеспечение достоверности и полноты информации.

«Конфиденциальность» подразумевает под собой обеспечение доступа к информации только авторизованным пользователям.

Под «Угрозой» информационной безопасности понимается потенциальная возможность тем или иным способом нарушить информационную безопасность.

Попытка реализации угрозы называется «атакой», а тот, кто реализует данную попытку, называется «злоумышленником». Атака — ситуация, которая предполагает такую угрозу, а планирующий её человек — это злоумышленник. Потенциальными злоумышленниками являются все лица, способные нанести вред. Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем. Угроза — любое действие, потенциально способное нанести урон информационной безопасности, а именно нарушить доступность, целостность и конфиденциальность информации.

Исходя из целей и выполняемых задач, необходимы будут и различные меры, и степени защиты, применимые по каждому из этих трех пунктов.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы.

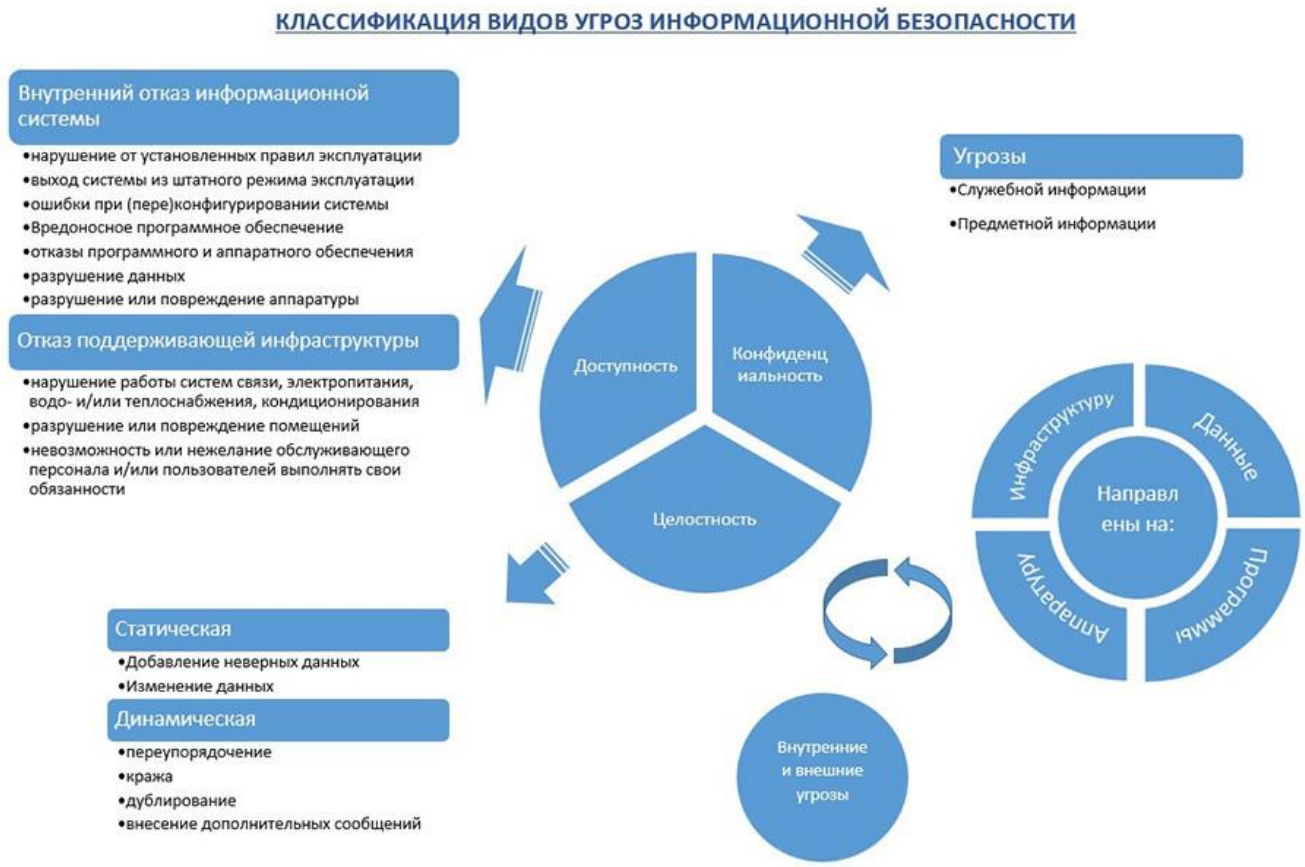

Рис. 1. Классификация видов угроз информационной безопасности

1. Виды угроз информационной безопасности:

Угрозы доступности:

Внутренний отказ информационной системы.

- Нарушение (случайное или умышленное) от установленных правил эксплуатации.
- Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.).
- Ошибки при (пере)конфигурировании системы.
- Вредоносное программное обеспечение.
- Отказы программного и аппаратного обеспечения.
- Разрушение или повреждение аппаратуры.

Отказ поддерживающей инфраструктуры.

- Нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- Разрушение или повреждение помещений;
- Невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Самая распространенный случай здесь — ошибки специалистов, которые работают с информационной системой. Это могут быть непредумышленные действия, вроде ввода некорректных данных и системного сбоя. Такие случайности являются потенциальной угрозой, из-за них в системе появляются уязвимые места, которые используют злоумышленники. В качестве технологии защиты информации в сети здесь могут выступать автоматизация (минимизация человеческого фактора) и административный контроль.

Что является источником угрозы доступности?

- Отсутствие у специалиста должной подготовки в работе с информационными системами.
- Низкая мотивация обучаться.
- Нарушение правил и алгоритмов работы (умышленное или нет).
- Отказ программного обеспечения.
- Отсутствие технической поддержки.
- Ошибки при переконфигурировании.
- Внештатная ситуация, которая приводит к выходу поддерживающей инфраструктуры из обычного режима (увеличение числа запросов или повышение температуры).
- Физическое нанесение вреда поддерживающей инфраструктуре (проводам, компьютерам и так далее).

Угрозы целостности:

Можно разделить на угрозы статической целостности и угрозы динамической целостности.

Так же стоит разделять на угрозы целостности служебной информации и содержательных данных. Под служебной информацией понимаются пароли для доступа, маршруты передачи данных в локальной сети и подобная информация. Чаще всего и практически во всех случаях злоумышленником осознано или нет, оказывается сотрудник организации, который знаком с режимом работы и мерами защиты.

С целью нарушения статической целостности злоумышленник может:

- Ввести неверные данные.
- Изменить данные.

Угрозами динамической целостности являются, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений.

Основная угроза целостности – это кража и подделка, которые также чаще всего осуществляются работниками компании.

Известная американская газета USA Today опубликовала любопытные данные по этому вопросу. Еще в 1992 году, когда компьютеры играли не такую большую роль, общий нанесенный ущерб от такой угрозы составил 882 000 000 долларов. Сейчас эти суммы значительно выше.

Что может стать источником угрозы целостности?

- Изменение данных.
- Ввод некорректных сведений.
- Подделка части информации (например, заголовка).
- Подделка всего файла.
- Внесение дополнительной информации.
- Дублирование.
- Отказ от исполненных действий.

Угрозы конфиденциальности:

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д.

Другой пример — нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Сюда относится использование паролей для несанкцинированного. Благодаря использованию этих данных они могут получить доступ к конфиденциальным сведениям.

Что служит источником угрозы конфиденциальности?

- Применение одинаковых паролей на всех системах.
- Использование многоразовых паролей и сохранение их в ненадежных источниках, к которым могут получить доступ посторонние люди.
- Размещение данных в месте, которое не гарантирует конфиденциальность.
- Презентация оборудования с конфиденциальными данными на выставках.
- Применение технических средств злоумышленниками (программы, считывающие введенный пароль, подслушивающие устройства и так далее).
- Оставление оборудования без присмотра.
- Размещение данных на резервных копиях.
- Использование информации в множестве источников, что значительно снижает её безопасность и приводит к перехвату.
- Злоупотребление полномочиями и нарушение рабочей этики сотрудниками.

Основная суть угрозы конфиденциальности — данные становятся уязвимыми и из-за этого злоумышленник получает к ним доступ.

2. Цели кибератак.

Для начала приведем любопытную статистику. Согласно мировым исследованиям, только за прошлый год 91% компаний подвергались кибератакам хотя бы раз. Если взять Россию отдельно, то статистика не лучше — 98% фирм сталкивались с внешними атаками. Еще 87% получили урон из-за внутренних угроз (утечке сведений, некорректных действий сотрудников, заражение программами и так далее).

Ущерб только от одного «нападения» злоумышленников может составить миллионы рублей. Несмотря на все это, четверть российских компаний не используют никакие технологии защиты информации в сети интернет и телекоммуникационных сетях. Даже стандартные методы, вроде антивирусных программ.

Новые вирусы создаются постоянно, автоматические системы фиксируют более 300 тысяч образцов новых вредоносных программ ежедневно. Они способны нанести значительный урон пользователям и фирмам, таких случаев в истории предостаточно. Например, в США злоумышленники взломали систему магазина Target и получили данные о 70 миллионах кредитных карт их клиентов.

С какой целью совершаются кибератаки?

Кража информации.

Компании хотят получить доступ к коммерческой тайне конкурентов, к персональным данным клиентов и сотрудников. Участились случаи атак, которые получили название MiniDuke. Они направлены на государственные и дипломатические структуры, военные учреждения, энергетические компании, операторов связи.

Доступ к ним — это доступ к огромным ресурсам. Вредоносные ПО действуют хитро, они подменяют популярные сайты и приложения. В точности копируют логотипы, описания файлов и даже их размеры. Программа крадет пароли, списки контактов, историю браузера и другие конфиденциальные данные

Ликвидация сведений и блокировка работы компании.

Существуют программы, которые полностью стирают данные на серверах без какой-либо возможности их восстановления (например, Shamoon и Wiper). Пару лет назад таким атакам подверглась нефтяная компания Saudi Arabian Oil Company. Тогда с 30 тысяч компьютеров исчезли сведения, оборудование просто перестало включаться.

Похищение денег.

Сюда относятся троянские ПО, которые крадут деньги с помощью систем дистанционного банковского обслуживания.

Нанесение финансового ущерба.

Использование DDOS-атак, которые парализуют внешние веб-ресурсы компаний на несколько дней и мешают работе.

Снижение репутации компании.

Для этих целей взламываются корпоративные сайты, куда внедряются посторонние ссылки или баннера. Если пользователь перейдет по ним, то попадет на вредоносный ресурс. Также на сайте фирмы могут быть размещены любые дискредитирующие сведения, изображения, высказывания и так далее. Таким атакам подверглись пару лет назад две известные компании, которые занимаются защитой данных.

Кража цифровых сертификатов.

Для компании это будет означать снижения доверия пользователей, поскольку документ потеряет свой статус и клиенты не будут уверены в безопасности данных. Такие потери могут привести даже к закрытию бизнеса.

3. Как подразделяются угрозы информационной безопасности.

Рассмотрим ниже классификацию видов угроз по различным критериям:

По точке приложения воздействия:

- Доступности.
- Целостности.
- Конфиденциальности.

По компонентам, на которые нацелено воздействие:

- Данные.
- Программы.
- Аппаратура.
- Поддерживающая инфраструктура.

По способу осуществления:

- Случайные или преднамеренные.
- Природного или техногенного характера.

По расположению источника угрозы:

- Внутренние.
- Внешние.

Как упоминалось в начале понятие «угроза» в разных ситуациях зачастую трактуется по-разному. И необходимые меры безопасности будут разными. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать — вся информация считается общедоступной.

Для применения наиболее оптимальных мер по защите, необходимо провести оценку не только угроз информационной безопасности, но и возможного ущерба, для этого используют характеристику приемлемости, таким образом, возможный ущерб определяется как приемлемый или неприемлемым. Для этого полезно утвердить собственные критерии допустимости ущерба в денежной или иной форме.

Каждый кто приступает к организации информационной безопасности, должен ответить на три основных вопроса:

4. Что защищать?

От кого защищать, какие виды угроз являются превалирующими: внешние или внутренние?

Как защищать, какими методами и средствами?

Принимая все выше сказанное во внимание, Вы можно наиболее оценить актуальность, возможность и критичность угроз. Оценив всю необходимую информацию и взвесив все «за» и «против» можно подобрать наиболее эффективные и оптимальные методы и средства защиты.

Основные принципы защиты информации.

Внедрение технологий защиты информации в интернете и в организациях подчиняется некоторым базовым принципам, о которых мы расскажем ниже.

Ведущая роль должна отводиться мероприятиям организационного характера, но при разработке охранных мер нужно учитывать все аспекты. Что это значит? Оптимальное соотношение программно-аппаратных средств и координации внедренных мер защиты. Изучите практику построения аналогичных систем в нашей стране и заграницей.

Минимизируйте и распределяйте полномочия сотрудников, по доступу к данным и процедурам их обработки.

Давайте минимальное количество четких полномочий экономическому отделу, тогда они смогут успешно выполнять работу на благо компании. Здесь имеется ввиду и автоматизированная обработка конфиденциальных данных, которые доступны персоналу.

Вы должны быть в курсе всех попыток сотрудников получить несанкционированный доступ к данным. У вас должна быть возможность быстро установить их идентичность и составить протокол действий при расследовании. Для этого внедряйте полный контроль и предварительную регистрацию, без этого никто не должен иметь доступ к данным.

Учитывайте любые внештатные ситуации — сбои, отказ внутренних и внешних систем снабжения, умышленные действия нарушителей, некорректное поведение сотрудников. Защита информации и технологии информационной безопасности должны быть надежными всегда.

Осуществляйте контроль за функционированием технологии и системы охраны сведений. Внедряйте средства и методики, которые позволяют отслеживать их работоспособность.

Организация и технологии защиты информации должны быть понятными и прозрачными (для сотрудников, общего и прикладного программного обеспечения).

Просчитайте все финансовые показатели, сделайте систему охраны сведений целесообразной. Затраты на её разработку и эксплуатацию должны быть ниже потенциальной угрозы, которая может быть нанесена, если вы не внедрите соответствующие меры.

Задачи специалистов информационной безопасности.

Что входит в должностные обязанности сотрудников, которые занимаются организацией системы защиты данных в компании? Они:

- определяют, что относится к конфиденциальным сведениям, оценивают их значимость, объем и степень секретности;
- определяют состав необходимого технического оборудования и в каком режиме будет происходить обработка данных (интерактив, реальное время), самостоятельно разбираются в программных комплексах;
- анализируют современные разработки, выпускаемые на рынок сертифицированные технологии и средства защиты, оценивают — какие из них можно применить в компании;
- описывают функционал персонала, всех служб, научных и вспомогательных сотрудников — каким образом они участвуют в процессе обработки данных, как взаимодействуют между друг другом и со службой безопасности;

- различными способами обеспечивают секретность в вопросах системы защиты данных, начиная с этапа её создания.

Средства защиты информации.

К наиболее популярным современным технологиям защиты информации относят антивирусные программы, которые используют более 60% предприятий. Четверть организаций не применяет никакие средства охраны данных. Прослеживается тенденция: чем меньше компания, тем ниже у нее уровень безопасности. Маленькие фирмы пренебрегают любыми мерами и не уделяют этому вопросу должного внимания.

Несмотря на это, создаются и приобретают популярность новые методы защиты:

- управление обновлением программного обеспечения;
- контроль приложений.

Какие рекомендуется внедрять в обязательном порядке?

Во-первых, ставить средства защиты не только на офисные компьютеры, но и на остальные используемые в рабочих целях устройства (телефоны, планшеты). Одна ошибка, вроде случайного подключения к незащищенной сети wi-fi, может стать причиной финансовых потерь или слива клиентской базы.

Во-вторых, не скупитесь на покупку лицензионных версий антивирусов (для этого есть выгодные корпоративные предложения). Они защитят вас от вирусов на флеш-накопителях, вредоносных ПО и ссылок, зараженных сайтов.

В-третьих, уделяйте внимание обучению сотрудников в вопросах информационной безопасности. Чтобы они не попались на действия злоумышленников, которые подделывают приложения и сайты (банков, госучреждений и так далее).

Исследования фирм, которые занимаются защитой данных показывают, что российские компании не считают охрану от киберугроз своим приоритетом. Только треть респондентов (29%) готовы уделять должное внимание этому вопросу. В мире средний показатель еще ниже — 23%. Ситуация с защитой данных не лучше (33% в России и 28% в мире).

5. Технологии защиты информации.

Существует множество технических средств и технологий защиты информации, о которых мы расскажем ниже. Использовать их лучше в совокупности.

Организационно-правовая защита.

К основным технологиям правовой защиты информации относятся международные договоры, нормативно-правовые акты, принятые в стране и различные официальные стандарты.

Еще одним инструментом являются организационные мероприятия по формированию инфраструктуры, с помощью которой данные будут храниться. Они осуществляются еще на ранних этапах проектирования зданий, помещений и систем, а также их ремонта.

Инженерно-техническая защита.

К таким средствам относятся объекты, которые обеспечивают безопасность. Их нужно предусмотреть еще на этапе строительства здания или проверить наличие, если вы арендуете помещение.

Какие преимущества дают инженерно-технические инструменты?

- Профилактические меры для снижения последствий внешнего воздействия (катаклизмов и стихийных бедствий).
- Контроль за перемещениями людей по территории фирмы.
- Контроль за действиями специалистов.
- Доступ в помещения компании только уполномоченных сотрудников.
- Невозможность перехвата данных.
- Устранение возможности установки удаленного видеонаблюдения или прослушки.
- Защита от пожаров.
- Надежная защита хранилища информации.
- Защита офиса компании от действий злоумышленников.
- Криптографическая защита

Программно-аппаратные инструменты.

Они входят в состав технических средств. Что это может быть?

- Любые инструменты идентификации для определения сведений о человеке (персональные магнитные карты, коды доступа, отпечатки пальцев и так далее).
- Инструменты по шифрованию информации.
- Оборудование, блокирующее несанкционированный доступ к системам (электронные звонки и блокираторы).
- Сигнализация, срабатывающая из-за противоправных действий.
- Инструменты для уничтожения данных на носителях.

Основная задача таких инструментов — шифрование, ограничение доступа к информации и идентификация пользователей. Для этого разрабатываются различные специализированные программы.

Для обеспечения полноценной защиты используются и программные, и аппаратные инструменты. Использование совокупности мер повышает шансы и увеличивает уровень безопасности данных. Однако стоит помнить, что 100% гарантии вам никто не может дать и все равно останутся слабые места, которые необходимо выявлять.

7 технологий защиты информации от несанкционированного доступа.

Средства защиты от несанкционированного доступа

Сюда относятся программно-аппаратные средства в совокупности, а также программные и аппаратные отдельно. Их главная задача — полное предотвращение и усложнение доступа сторонних лиц к конфиденциальным данным.

Перечислим основной функционал:

- регистрация носителей информации;
- управление информационными потоками между устройствами;
- разграничение доступа;
- регистрация запуска и завершения процессов;
- идентификация устройств и отдельных пользователей и так далее.

Модули доверенной загрузки

С их помощью осуществляется запуск операционной системы с доверенных носителей информации. Они контролируют целостность программного обеспечения и технических параметров, проводят аутентификацию, идентифицируют устройства и пользователей. Могут быть как программными, так и программно-аппаратными средствами.

DLP-системы

Программы, которые обеспечивают охрану данных от возможной утечки внутри компании. Они анализируют все исходящие и иногда входящие информационные потоки, создавая защищенный цифровой периметр. Контролируют не только веб-трафик, но и распечатанные или отправляемые по wi-fi и bluetooth документы.

Анализ защищенности информационных систем.

Это процесс проверки инфраструктуры компании на наличие проблем и слабых мест. Они могут быть связаны с ошибками конфигурации, исходным кодом или используемым ПО. На этом этапе выполняется проверка всех внешних и внутренних информационных систем.

Защита виртуальной инфраструктуры.

Существуют конкретные средства и инструменты, эффективные именно для защиты виртуальной инфраструктуры. С их помощью нейтрализуются потенциальные атаки и формируется комплексная защита виртуальной среды (в совокупности с другими инструментами). Разработкой таких программных продуктов занимаются отдельные компании, которые используют особые подходы. Они основаны на глубоком анализе потенциальных киберугроз.

Межсетевое экранирование.

Это программный или программно-аппаратный комплекс средств, локальных или функционально-распределенных. Их основная задача — контроль всей входящей и исходящей информации. Безопасность системы обеспечивается с помощью фильтрации данных, её углубленного анализа по комбинации критериев. Только после этого принимается решение о её распространении или нет на основании заданных правил.

Системы обнаружения вторжений.

Это программные и аппаратные средства, используемые для обнаружения неавторизованного входа в систему. А также неправомерных и несанкционированных попыток по управлению защищаемой сетью. Применяется для дополнительного усиления уровня информационной безопасности.

Технологии криптографической защиты информации.

Развитие технологий защиты информации не стоит на месте, и появляются все новые способы. Один из них — это криптография, в рамках которой используется шифрование данных. Она является базовым методом защиты при хранении информации в компьютере. Если данные передаются с одного устройства на другое, то используются зашифрованные каналы.

Для чего используется криптография?

• Обеспечение конфиденциальности при передаче по открытым каналам.
• Подтверждение достоверности данных из различных каналов.
• Защита конфиденциальности информации, если она содержится на открытых носителях.
• Избежание угрозы целостности сведений при их передаче и хранении.
• Подтверждение отправки данных.
• Защита программного обеспечения от копирования и с использованием сторонними лицами.

На данный момент криптография – одна из наиболее продвинутых цифровых технологий и надежная защита информации.

Как мы уже упоминали выше, криптография — это применение специальных методов шифрования, кодирования и любого преобразования информации. Такой метод защиты делает сведения недоступными без обратного преобразования или предъявления ключа криптограммы.

На данный момент существует 4 крупных раздела криптографии:

Симметричные криптосистемы. Здесь для преобразования и обратного преобразования текста применяется одинаковый ключ. В процессе преобразования открытый текст заменяется шифрованным, обратного преобразования — он снова заменяется исходным).

Криптосистемы с открытым ключом. Применяются два ключа — открытый и закрытый, которые связаны между друг другом. Шифрование происходит с помощью открытого ключа, который известен всем. Дешифрование доступно только получателю сообщения с помощью закрытого ключа.

Система электронной подписи. Когда к тексту присоединяется его криптографическое преобразование. Это позволяет другим пользователям проверить достоверность полученных данных и их авторство.

Управление ключами. Обработка информации, составление и распределение ключей между пользователями.

Где используются криптографические методы? При передаче конфиденциальных данных по различным каналам связи (к примеру, e-mail). Также при необходимости установления подлинности и авторства данных, хранения зашифрованных сведений на носителях.

Для криптографического закрытия могут использоваться как программные, так и аппаратные инструменты. Последние отличаются большими финансовыми затратами, но они также обладают особыми преимуществами – простотой в использовании, высокой производительностью и уровнем защиты.

Какие требования существуют для криптографический систем?

- прочитать зашифрованное сообщение можно только при наличии ключа;
- число операций, нужных для определения ключа шифрования по фрагменту, должно быть не меньше общего числа возможных ключей;
- число операций путем перебора всевозможных ключей должно выходить за пределы возможностей современных компьютеров и иметь строгую нижнюю оценку;
- знание алгоритма шифрования не должно снижать уровень защиты;
- даже при использовании одного и того же ключа незначительное изменение должно приводить к существенному изменению вида зашифрованного сообщения;
- структурные элементы алгоритма шифрования должны быть неизменными;

- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
- исходный и шифрованный текст должны быть одинаковыми по длине;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Развитие технологий защиты информации не стоит на месте. Скорее всего, в ближайшем будущем появятся новые более продвинутые формы борьбы с киберугрозами и злоумышленниками. Но уже сейчас компаниям и частным пользователям необходимо применять существующие инструменты для охраны конфиденциальных сведений.