МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Исследование алгоритмов защиты персональных данных в мобильных клиентах при доступе к удаленным ИС»

Студент М.Х. Темуршоев
(И.О. Фамилия) (личная подпись)

Научный руководитель д.т.н, доцент, С.В. Мкртычев
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение

В связи с появлением Интернета конфиденциальность информации стала социальной и политической проблемой первого уровня, которая приобрела глобальное значение. Глобализация проблемы конфиденциальности была вызвана с развитием процессов информатизации общества, созданием новых и интеграцией существующих информационных систем, ориентированных на обслуживание населения. Поскольку компьютерные сети упрощают поиск, хранение и обработку информации, людям становится все труднее сохранять конфиденциальность своих данных.

Почему мы должны защищать конфиденциальность персональных данных? С учетом последних интернет-событий, таких как кражи личных данных, интернет-преследование, навязчивый бизнес-маркетинг, все это стало намного проще благодаря персональным данным, которые составляют важную часть информационного пространства, содержащую сведения о физических лицах.

Также хотелось бы отметить, что на сегодняшний день на территории Российской Федерации существует более 7 миллионов операторов персональных данных - государственных и частных организаций, обрабатывающих персональные данные своих сотрудников и клиентов [6].

В связи с этим представляют интерес исследования, направленные на исследования методов и алгоритмов обработки персональных данных, позволяющих снизить затраты на обеспечение безопасности персональных данных.

Объектом исследования диссертационной работы являются методы защиты персональных данных.

П**редмет исследования** - алгоритмы защиты персональных данных, комплекс методов, которые определяют категории персональных данных, оценки защищенности и риска безопасности информационных систем персональных данных, выбор средств защиты персональных данных, обрабатываемых в ИС персональных данных.

Целью работы является исследование алгоритмов защиты персональных данных в мобильных клиентах при доступе к удаленным ИС.

Для достижения поставленной цели нужно решить следующие задачи:

- проанализировать современное состояние проблемы исследования;
- проанализировать методы обеспечения безопасности персональных данных;
- проанализировать алгоритмы защиты персональных данных;
- оценить эффективность алгоритмов защиты персональных данных.

Гипотеза исследования: применение эффективных методов и алгоритмов защиты информации позволит существенно уменьшить риск потери персональных данных мобильных клиентов при доступе к удаленным ИС.

Методы исследования: системный анализ, методы и алгоритмы защиты данных.

Научная новизна результатов диссертации связана с исследованием алгоритмов защиты персональных данных, позволившей выявить наиболее эффективные методы и алгоритмы, определить достаточные условия защищенности персональных данных.

Теоретической основой диссертационного исследования являются научные труды российских и зарубежных ученых, занимающихся проблемами защиты информации.

Основные этапы исследования: исследование проводилось с 2019 по 2021 год в несколько этапов:

На первом этапе (констатирующем этапе) – формулировалась тема исследования, выполнялся сбор информации по теме исследования из различных источников, проводилась формулировка гипотезы, определялись постановка цели, задач, предмета исследования, объекта исследования и выполнялось определение проблематики данного исследования.

Второй этап (поисковый этап) – в ходе проведения данного этапа осуществлялся анализ методов и алгоритмов защиты данных.

Третий этап (реализация) – на данном этапе выполнялась оценка эффективности алгоритмов защиты информации персональных данных в мобильных клиентах при доступе к удаленным ИС.

На защиту выносятся:

- результаты анализа алгоритмов защиты персональных данных в мобильных клиентах при доступе к удаленным ИС;
- результаты оценки эффективности алгоритмов защиты персональных данных.

По теме исследования опубликована 1 статья:

Темуршоев М.Х. Сравнение методов защиты персональных данных // Вестник научных конференций, 2021 (принята к публикации).

Диссертация состоит из введения, четырех глав, заключения и списка литературы.

Работа изложена на 70 страницах и включает 20 рисунков, 1 таблицу, 31 источник.

Глава 1 Современное состояние проблемы защиты персональных данных

1.1 Назначение персональных данных в современном интернете

Интернет стал важной частью инфраструктуры крупных городов, где качество жизни улучшается в таких областях как здравоохранения и транспорт. Интернет перешел от простых компьютерных экранов к другим объектам и невидимым датчикам, образуя систему, которая соединяет так называемые «умные вещи» с Интернетом. Эта система называется «Интернет вещей», и она ликвидирует разрыв между физическим и онлайн-миром. Интернет вещей несет с собой огромный потенциал как для частных лиц, так и для предприятий. Это может, например, помочь нам сэкономить энергию и значительно улучшить качество жизни людей в таких областях, как здравоохранение и транспорт. Данная система также присутствует в домах, где технология используется для домашней автоматизации, такой как автоматическое отопление, освещение или электроприборы. Люди также используют смарт приборы для контроля за своим здоровьем и повседневной деятельностью.

Наряду с увеличением использования смарт технологии, личные данные часто собираются и регистрируются, и они могут, например, использоваться для определения местоположения дома или рабочего места человека, для мониторинга привычек и образа жизни, или нацелить рекламу на основе интересов субъекта данных. В то же время данная система создает значительные проблемы с конфиденциальностью, безопасностью и защитой данных, и он требует более тщательного изучения. Некоторые ученые считают, что технологии толкают нас в эру «нулевой информационной конфиденциальности». Умные устройства создают мир так называемого «многопрофильного наблюдения». Это означает, что за нами могут наблюдать государство, компании, маркетологи и все те, кто находится в наших

социальных сетях.

Персональные данные — это любая информация, относящаяся к физическому лицу [5]. Данные в ИС можно разделить на два типа: они либо личные (персональные), либо нет. Устройства всех видов вокруг нас постоянно собирают информацию для предоставления услуг, но не все собранные данные попадают в категорию персональных данных. Однако такое количество неличной информации может быстро привести к идентификации физического лица и выявить очень личные аспекты. Все это подчеркивает сложности, с которыми в настоящее время сталкиваются эксперты по защите данных при работе с такими технологиями и методами, как большие данные, облачные вычисления, интеллектуальный анализ данных и сбор информации через Интернет [16, 17].

Поскольку традиционный Интернет превратился сложную структуру, закон о защите личных данных также превратился в правовую область, которая применима практически во всех секторах, услугах и технологиях [19]. Основным законом защиты персональных данных в РФ является Федеральный закон РФ от 27 июля 2006 года № 152 «О персональных данных» [9, 23].

1.2 Идентификаторы и теневые профили

Некоторые вопросы, связанные с идентификаторами, можно было бы понять, проанализировав скандал с Cambridge Analytica (частная английская компания), который поставил под сомнение то, как Facebook собирает и делится личными данными. После того как скандал стал достоянием общественности, Facebook был вызван в Конгресс США и Европейский парламент для ответа на вопрос о том, как и когда Facebook собирает и распространяет данные. Марк Цукерберг (генеральный директор Facebook) был вызван в Конгресс США и Европейский парламент для ответа на вопрос о том, как и куда Facebook собирает и распространяет данные. Они использовали теневые профили.

Теневые профили основаны на одной из основных функций Интернета: большинство веб-сайтов собирают информацию о посетителях, чтобы адаптировать такие услуги, как реклама, или хранить предпочтения пользователей, чтобы обеспечить удобство работы в Интернете.

Особенность Facebook заключается в том, что всякий раз, когда одна из его функций (например, кнопка "Нравится" и "поделиться") начинает работать, она отправляет данные о его активности использовании в Facebook, даже если активность пользователя на веб-странице была ограничена только просмотром. Эти данные полны идентификаторов, таких как файлы cookie, адреса интернет-протокола (IP) и многие другие. Facebook насчитывает около 2,2 миллиарда пользователей ежемесячно, и нетрудно понять, почему большинство веб-сайтов сегодня внедряют в него функции, что позволяет собирать большие коллекции идентификаторов. Достаточное количество идентификаторов может быть использовано для вывода информации о практически неизвестном человеке (технически, еще не идентифицированном субъекте данных).

Какая польза от этих агрегированных данных? В случае Facebook, когда человек регистрируется на нем, платформа связывает теневой профиль с этим человеком. Без теневых профилей база данных, содержащая персональные данные нового пользователя, должна быть пустой. Любой сбор персональных данных должен начинаться только в момент регистрации и, в любом случае после того, как пользователь дал на это явное согласие. Однако при использовании теневых профилей Facebook автоматически выполняет корреляцию, и уже выполненный сбор и анализ данных ассоциируется с этим субъектом данных. В свою очередь, платформа может немедленно предложить расширенные услуги, такие как предложение списка друзей или показ рекламы, представляющей интерес для этого пользователя.

Идентификаторы как таковые не обязательно должны пониматься как персональные данные: они поддерживают привилегированные отношения с субъектом данных, потому что они могут описывать некоторые из его

характеристик. Тем не менее, они могут стать персональными данными на более поздних этапах. Тем более, что идентификатор, не предназначенный для сбора персональных данных, может быть преобразован в идентификатор, обладающий высокой степенью личной идентификации [7, 8].

1.3 Обзор методов защиты данных

Защита и безопасность данных — это одно из самых важных дел, которое вы можете сделать для своей компании, если регулярно обрабатываете личные данные [11,12].

Если вам это удается, то вам гораздо меньше нужно беспокоиться, а все остальные возникающие вопросы решать намного проще.

Есть очень много методов и алгоритмов защиты персональных данных [2].

Вот некоторые из наиболее часто используемых методов и технологий [13]:

- предотвращение потери данных (DLP) — набор стратегий и инструментов, которые можно использовать для предотвращения кражи, потери или случайного удаления данных. Решения по предотвращению потери данных часто включают в себя несколько инструментов для защиты от потери данных и восстановления после нее;
- хранилище со встроенной защитой данных – современное оборудование для хранения данных обеспечивает встроенную кластеризацию и резервирование дисков. Например, гипермаркет Cloudian обеспечивает долговечность до 14 девяток, низкую стоимость, позволяющую хранить большие объемы данных;
- брандмауэры — утилиты, позволяющие отслеживать и фильтровать сетевой трафик. Вы можете использовать брандмауэры, чтобы гарантировать, что только авторизованным пользователям разрешен

доступ к данным или их передача;

- аутентификация и авторизация — элементы управления, которые помогают проверить учетные данные и убедиться, что права пользователя применяются правильно. Эти меры обычно используются как часть решения по управлению идентификацией и доступом (УИД) и в сочетании с ролевыми средствами управления доступом;
- шифрование — изменяет содержимое данных в соответствии с алгоритмом, который может быть отменен только с помощью правильного ключа шифрования. Шифрование защищает ваши данные от несанкционированного доступа, даже если данные украдены, делая их нечитаемыми;
- защита конечных точек — защищает шлюзы в вашей сети, включая порты, маршрутизаторы и подключенные устройства. Программное обеспечение для защиты конечных точек обычно позволяет контролировать периметр сети и фильтровать трафик по мере необходимости;
- удаление данных — ограничивает ответственность, удаляя данные, которые больше не нужны. Это может быть сделано после обработки и анализа данных или периодически, когда данные больше не актуальны. Удаление ненужных данных является требованием многих нормативных актов, таких как общим правилам защиты данных.

Мы будем исследовать и анализировать наиболее часто используемых методов и алгоритмов защиты персональных данных. Во втором главе более подробно будем исследовать следующих методов защиты данных.

1.3.1 Оценки рисков

Чем рискованнее данные, тем больше защитой они должны быть обеспечены. Конфиденциальные данные должны тщательно охраняться, в то время как данные с низким уровнем риска могут быть защищены в меньшей степени. Основная причина таких оценок заключается в выгоде с точки зрения затрат, поскольку более высокий уровень безопасности данных равнозначен более высоким расходам. Однако хорошей проверкой является определение того, какие данные нуждаются в более тщательной защите, и это делает всю систему обработки данных более эффективной [24].

Основные шаги выявления рисков:

- выявление опасностей. Осмотрите рабочее место и посмотрите, что можно разумно ожидать, чтобы причинить вред. Определите общие опасности на рабочем месте. Проверьте инструкции производителей или поставщиков или технические паспорта на наличие любых очевидных опасностей. Просмотрите предыдущие отчеты об авариях и почти промахах. Эффективно выявлять опасности с помощью контрольных списков. Это гарантирует, что все будет охвачено во время оценки риска и идентификации опасности, что предотвращает эскалацию рисков. Опасности и риски иногда используются взаимозаменяемо; однако на самом деле они относятся к двум различным элементам потенциального инцидента. Опасность-это то, что потенциально может причинить вред людям, имуществу или окружающей среде, в то время как риск-это вероятность того, что опасность действительно причинит вред или ущерб при определенных обстоятельствах;
- оценка рисков. Чтобы оценить риск опасности, вы должны рассмотреть, как, где, сколько и как долго люди обычно подвергаются потенциальной опасности. Назначьте оценку риска вашим опасностям с помощью матрицы рисков. Использование

матрицы рисков может помочь измерить уровень риска для каждой опасности;

- Принять решение о мерах контроля для осуществления. После присвоения рейтинга риска выявленной опасности пришло время разработать эффективные меры контроля для защиты работников, имущества, гражданских лиц и/или окружающей среды. Следуйте иерархии элементов управления при определении приоритетов реализации элементов управления;
- оформление выводов. Важно вести официальный учет оценок рисков. Это может помочь вашей организации отслеживать опасности, риски и меры контроля. Документация может включать подробное описание процесса оценки риска, схему оценок и подробные объяснения того, как были сделаны выводы;
- проверка оценки и ее обновление при необходимости. Проследите за своими оценками и посмотрите, были ли приняты рекомендуемые меры контроля. Если условия, в которых была основана ваша оценка риска, существенно изменились, используйте свое лучшее суждение, чтобы определить, необходима ли новая оценка риска [27].

Существуют два направления, на которых должна основываться оценка риска: потенциальная серьезность в случае нарушения данных и вероятность нарушения. Чем выше риск по каждому из этих направлений, тем более конфиденциальными являются данные. Неправильно охарактеризованные данные, если они будут утеряны, могут оказаться катастрофическими.

1.3.2 Резервные копии

Резервное копирование — это метод предотвращения потери данных, которая часто может произойти как из-за ошибки пользователя, так и из-за технической неисправности. Резервные копии должны регулярно создаваться и обновляться. Регулярное резервное копирование приведет к

дополнительным затратам, но потенциальные сбои в нормальной работе могут стоить еще дороже.

Резервное копирование данных включает в себя несколько важных концепций:

- решения и инструменты резервного копирования;
- администратор резервного копирования;
- объем и расписание резервного копирования;
- точка восстановления;
- время восстановления.

Решения и инструменты резервного копирования. Хотя резервное копирование данных возможно вручную, для обеспечения регулярного и последовательного резервного копирования систем большинство организаций используют технологическое решение для резервного копирования своих данных.

Администратор резервного копирования. Каждая организация должна назначить сотрудника, ответственного за резервное копирование. Этот сотрудник должен убедиться, что системы резервного копирования настроены правильно, периодически тестировать их и обеспечивать фактическое резервное копирование критически важных данных;

Объем и расписание резервного копирования. Организация должна принять решение о политике резервного копирования, указав, какие файлы и системы достаточно важны для резервного копирования и как часто следует создавать резервные копии данных;

Точка восстановления. Это объем данных, который организация готова потерять в случае аварии, и определяется частотой резервного копирования. Если резервное копирование систем выполняется один раз в день, то rpo составляет 24 часа. Чем ниже rpo, тем больше ресурсов для хранения данных, вычислительных и сетевых ресурсов требуется для обеспечения частого резервного копирования;

Время восстановления. Это время, необходимое организации для

восстановления данных или систем из резервной копии и возобновления нормальной работы. Для больших объемов данных и/или резервных копий, хранящихся вне помещений, копирование данных и восстановление систем может занять много времени, и для обеспечения низкого уровня необходимы надежные технические решения.

Резервное копирование должно производиться по принципу, описанному выше - данные с низкой импортностью не должны копироваться так часто, как это происходит с конфиденциальными данными. Такие резервные копии должны храниться в безопасном месте и, возможно, в зашифрованном виде. Конфиденциальные данные не стоит хранить в облаке. Периодически стоит проверять носители информации на предмет их порчи в соответствии с рекомендациями производителя и хранить их в соответствии с официальными рекомендациями.

Методы хранения на кассетах все равно дешевле по сравнению с жесткими дисками. Однако жесткие диски более универсальны и лучше подходят для работы в небольших масштабах. Доступ к данным также намного быстрее при использовании дисковых методов хранения.

1.3.3 Шифрование данных

Данные с высокой степенью риска являются основным кандидатом на шифрование на каждом этапе пути. Это включает в себя во время сбора (онлайн криптографические протоколы), обработки (полное шифрование памяти) и последующего хранения (RSA или AES). Хорошо зашифрованные данные по своей природе являются безопасными; даже в случае их нарушения данные будут бесполезны и невосстановимы для злоумышленников.

Помимо очевидных преимуществ усиленной защиты конфиденциальности, шифрование помогает обеспечить целостность данных, защищая их содержимое от недокументированных изменений, и может использоваться для проверки происхождения данных, сводя к минимуму риск

доступа к данным из ненадежных источников. Сочетание возросшего использования Интернета и ценности данных для хакеров делает данные более доступными и желательными, чем когда-то, и повышает потребность в защите. Кроме того, многие предприятия сталкиваются с требованиями правил защиты данных, такими как использование шифрования, которые необходимо соблюдать. Тип используемого шифрования зависит от того, как и кем предполагается получить доступ к данным.

Закрытый ключ шифрования (симметричный)

Симметричное шифрование использует один закрытый ключ для шифрования и дешифрования. Это более быстрый метод, чем асимметричное шифрование, и его лучше всего использовать отдельным лицам или в закрытых системах. Использование симметричных методов с несколькими пользователями в открытых системах, например, по сети, требует передачи ключа и создает возможность для кражи. Наиболее часто используемым типом симметричного шифрования является AES.

Открытый ключ шифрования (асимметричный).

Асимметричное шифрование использует парные открытые и закрытые ключи, которые математически связаны и могут использоваться только вместе. Любой ключ может быть использован для шифрования данных, но для его расшифровки необходимо использовать парный ключ. Асимметричное шифрование используется несколькими пользователями и в открытых сетях, таких как Интернет, поскольку открытый ключ может свободно использоваться без риска кражи данных. Наиболее часто используемыми типами асимметричного шифрования являются ElGamal, RSA, DSA и PKCS.

Правильное использование алгоритмов шифрования, несомненно, принесет пользу в глазах регулирующих органов. Например, если вы столкнутся с нарушением, которое затрагивает зашифрованные данные, даже не нужно сообщать об этом в контролирующие органы, поскольку данные считаются адекватно защищенными [20-22]. По этой причине, метод шифрования считается как самим безопасным методом защиты данных.

1.3.4 Псевдонимизация

Псевдонимизация — это еще один метод, который повышает безопасность персональных данных и не только персональных. Он хорошо работает с большими наборами данных и состоит из извлечения идентифицирующей информации из фрагментов данных. Например, заменять имена лиц случайно сгенерированными строками. Наиболее очевидным преимуществом псевдонимизации является сокрытие личности субъектов данных от какой-либо третьей стороны (т. е. помимо субъекта псевдонимизации) в контексте конкретной операции обработки данных. Тем не менее, псевдонимизация может выйти за рамки сокрытия реальных идентификационных данных и поддержать цель защиты данных-отсутствие связи, т.е. Снизить риск того, что данные, относящиеся к конфиденциальности, могут быть связаны между различными доменами обработки данных. Кроме того, псевдонимизация (сама по себе являющаяся методом минимизации данных) может способствовать реализации принципа минимизации данных в соответствии с общими правилами защиты данных (ОПЗД), например, в тех случаях, когда контролеру не нужно иметь доступ к реальной личности субъектов данных, а только к их псевдонимам. Наконец, еще одним важным преимуществом псевдонимизации, которое не следует недооценивать, является точность данных (более подробный анализ роли псевдонимизации).

Распространенный сценарий псевдонимизации данных-это когда данные собираются непосредственно от субъектов данных и псевдонимизируются контроллером данных для последующей внутренней обработки. Псевдонимизация также требуется при проведении научных или статистических исследований, поэтому многие учреждения и даже школы осведомляют своих учеников о правильной псевдонимизации своих данных.

1.3.5 Контроль доступа

Внедрение контроля доступа в рабочий процесс является очень эффективным методом снижения рисков. Чем меньше людей имеют доступ к данным, тем меньше риск (непреднамеренного) их нарушения или потери.

Организации или предприятии должны обеспечить, чтобы доступ к конфиденциальным данным предоставлялся только заслуживающим доверия сотрудникам, у которых есть веские основания для доступа к ним. Рекомендуется регулярно проводить предварительные учебные курсы и повышения квалификации по вопросам обработки данных, особенно после приема на работу новых сотрудников.

В настоящее время организации находятся на очень разных этапах своего пути к ОПЗД. Это означает, что существует повышенный спрос на ответы на вопросы подотчетности жестких данных, такие как:

- Почему мы храним персональные данные?
- Как мы их получили?
- Как долго проводится сбор данных?
- Насколько безопасны данные с точки зрения доступности и шифрования?
- Передаем ли мы эти данные третьим лицам?

Ответы на эти вопросы, особенно на последние два, требуют надежного и надежного подхода к ограничению доступа к персональным данным со ссылкой на четкий контрольный след того, когда и кем был получен доступ к данным. Это лишь один из многих шагов на пути к соблюдению принципа подотчетности GDPR, который требует от организаций демонстрировать и документировать четкое соблюдение принципов защиты данных при ведении бизнеса-независимо от того, где работают ваши пользователи и какие устройства они используют в данный момент.

С помощью сотрудника, ответственного за защиту данных, разработать четкую и краткую политику защиты данных, определяющую методы, роли и

обязанности каждого сотрудника (или группы сотрудников).

1.3.6 Очистка данных

Может наступить время, когда данные, которые у вас есть, должны быть уничтожены. Уничтожение данных может на первый взгляд показаться не методом защиты, но на самом деле это так. Таким образом, данные защищены от несанкционированного восстановления и доступа. В соответствии с юридическими правилами о защите персональных данных, вы обязаны удалять данные, которые вам не нужны, а конфиденциальные данные требуют более комплексных методов уничтожения.

Процесс очистки данных содержит определенные фазы, такие как:

– Анализ данных.

– Техника отображения и процесс преобразования.

– Проверка дубликата.

– Преобразование.

– Очищение обратного потока данных.

Анализ данных - для определения того, какие типы ошибок и несоответствий необходимо преодолеть, требуется детальный анализ данных.

Помимо этого, анализ данных также следует использовать для получения информации о данных и выявления проблем с качеством данных.

Техника отображения и рабочий процесс преобразования – этот процесс зависит от количества источников данных и загрязненности данных, для очистки данных необходимо выполнить большое количество шагов.

Проверка дубликата – это процесс, при котором проверяются различные типы данных после переноса данных из разных источников. Эта проверка выполняется для определения точности и согласованности данных по сравнению с первичным источником данных.

Преобразование – после применения методов очистки данных теперь его очередь преобразовывать данные таким образом, который поможет в

применении алгоритма машинного обучения к набору данных.

Очищенный обратный поток данных – после очистки данных обновленные данные также должны заменить нечистые данные в первичных источниках, чтобы предоставить новые предварительно обработанные данные устаревшим приложениям. В этой статье мы обсудим некоторые методы обнаружения и исправления ошибок и несоответствий в нашем наборе данных.

Жесткие диски чаще всего уничтожаются с помощью размагничивания, в то время как бумажные документы, компакт-диски и ленточные накопители разбиваются на мелкие кусочки. Уничтожение данных на месте рекомендуется для конфиденциальных данных. Зашифрованные данные можно легко удалить, просто уничтожив ключи дешифровки, гарантируя, что данные будут нечитаемыми, по крайней мере, в течение следующих нескольких десятилетий, после чего они, скорее всего, все равно устареют.

1.4 Правила конфиденциальности и обеспечение защиты мобильных данных

Организации в любой отрасли, от банковского дела до розничной торговли, здравоохранения и многого другого, обязаны применять правила защиты мобильных данных, установленные правительствами, которые налагают огромные штрафы в случае их несоблюдения.

До начала 2000-х годов управлять потоками данных было проще, поскольку доступ к информации осуществлялся в основном с компьютеров. С тех пор компании оцифровали свои фреймворки и сервисы, создав облачный и мобильный мир и значительно увеличив объем данных, передаваемых между мобильными устройствами, компьютерами и серверами. В результате корпоративные и персональные данные теперь широко доступны на смартфонах и планшетах, что делает их весьма уязвимыми для атак, нацеленных на мобильные устройства.

В связи с этими изменениями в том, как клиенты и другие сотрудники используют данные, организации теперь сталкиваются с проблемой обеспечения того, чтобы их мобильные платформы не противоречили правилам защиты данных. Это означает, что данные должны собираться точно и надежно для ограниченных, четко заявленных целей. Кроме того, он должен храниться не дольше, чем это необходимо.

Ниже приведены три шага, которые руководители службы безопасности должны предпринять для обеспечения того, чтобы корпоративная мобильность не нарушала конфиденциальность персональных данных, обрабатываемых вашими сотрудниками и клиентами:

1. Оценка воздействия мобильных устройств и уровней риска

То, как организация обрабатывает персональные данные, имеет ли она мобильный флот, позволяет ли мобильным работникам подключаться к горячим точкам или разрабатывает мобильные приложения, будет определять степень, в которой ее мобильная платформа предоставляет данные. На этапе оценки руководители служб безопасности должны перечислить все данные, обрабатываемые сотрудниками и клиентами, чтобы определить, являются ли они личными. Затем они должны определить ширину мобильной платформы для количественной оценки подверженности риску.

2. Оценка мер безопасности

Возможно, вы установили политику мобильной безопасности, запрещающую вашим сотрудникам загружать приложения из сторонних магазинов, и внедрили корпоративное управление мобильностью для обеспечения безопасности вашего мобильного парка. Но достаточно ли этих мер, чтобы по-настоящему понять уровень воздействия ваших данных? Этот этап посвящен диагностике вашего мобильного фреймворка, чтобы убедиться, что персональные данные, обрабатываемые вашими мобильными пользователями, эффективно защищены от утечки и кражи.

3. Адаптация мер безопасности к риску

Проверяет, соответствует ли текущий уровень безопасности вашей

организации правилам защиты мобильных данных. Руководители служб безопасности должны принять новые меры для соблюдения правовых стандартов конфиденциальности. Руководители служб безопасности должны предоставлять единую платформу для управления мобильными устройствами, приложениями и данными [1].

Данная технология плавно интегрируется с платформами управления, добавляя им недостающие возможности безопасности. Это позволяет группам безопасности выявлять и блокировать угрозы в режиме реального времени на устройствах пользователей, а также автоматически обновлять статус соответствия устройств и приложений.

Решения для тестирования безопасности мобильных приложений выявляют поведение и уязвимости, которые могут поставить под угрозу конфиденциальность данных. Это дает аналитикам четкое представление о том, какие данные собирают и обрабатывают приложения.

Выводы к главе 1

В первой главе рассматривается анализ и классификация угроз, возникающих при работе с персональными данными в информационных системах. В области информационных технологий в любой стране одним из национальных интересов является обеспечение доступности и защита конфиденциальности персональных данных. В связи с этим особое внимание в настоящее время уделяется организации обработки и обеспечению безопасности персональных данных в информационных системах.

Решение проблемы обеспечения безопасности персональных данных невозможно без выявления и классификации потенциальных угроз персональным данным в информационных системах.

Соответственно, в данной работе был анализирован ряд основных угроз для персональных данных и полученный результат может служить основой для реализации модели угроз конкретной информационной системы, предназначенной для обработки персональных данных.

Глава 2 Анализ методов защиты данных

2.1 Антивирусы

В этом пункте представлены антивирусная защита, ее определение и различные типы. Это показывает, как важно, чтобы эта программа защищала данные находящихся в мобильных устройствах и компьютерах. Поскольку злоумышленник распространяет вирусы по всему миру, людям нужна сильная и эффективная антивирусная программа для защиты компьютеров от этих вирусов. В этом отчете будет упомянуто представление о типах антивирусной защиты, о том, как она работает и какие методы используют, а также о преимуществах этой программы.

Компьютерный вирус — это компьютерная программа, которая может копировать себя и заражать компьютер. Он также используется для обозначения других типов вредоносных программ, в том числе программ для показа рекламы и программ-шпионов, которые не имеют репродуктивной способности. Фактически, мир стал свидетелем значительного развития в компьютерном мире, и большинство предприятий стали сильно зависеть от компьютера. Поскольку большинство мобильных устройств и компьютеров в настоящее время подключены к Интернету, увеличивается вероятность распространения этих вирусов, что потребовало наличия мощного программного обеспечения для защиты компьютеров от этих угроз. Антивирусное программное обеспечение является простым в использовании инструментом, но оно имеет большой эффект. Он ищет на вашем компьютере вредоносные файлы, вирусы и шпионские программы, которые где-то спрятаны.

Антивирусное программное обеспечение — это программа, которая используется для предотвращения, обнаружения и удаления вредоносных программ, в том числе компьютерных вирусов, червей и троянских программ. Такие программы также могут предотвращать и удалять рекламные,

шпионские и другие вредоносные программы. Это программное обеспечение сканирует компьютер, который ищет вирусы, чтобы удалить его, прежде чем вирус начнет повреждать мобильные и компьютерные данные в файлах. Существуют различные типы антивирусного программного обеспечения, разработанного на протяжении многих лет, чтобы справиться с текущей проблемой вирусов, такие как обычный дисковый сканер, резидентные сканеры памяти, обнаружение на основе поведения и сканеры запуска. Некоторые из этих программ могут быть запущены по запросу пользователей, а другие предназначены для запуска при каждой загрузке мобильных устройств или ПК.

Как работает антивирус?

Антивирусные программы предназначены для защиты данных находящихся на компьютере или мобильных устройств от вирусов. Эти программы обеспечивают два уровня функциональности при защите от вирусов, которые представляют собой защиту в режиме реального времени и проверку файлов, хранящихся на дисках компьютера и мобильных устройств. Антивирусные программы могут обнаруживать вирусы двумя способами. Первый способ — это след вирусной программы (Footprint of the virus program), и этот метод является распространенным методом идентификации вирусов. Целью этого метода является сравнение вирусного следа с библиотекой известных следов, которые соответствуют вирусам. Также при использовании этого метода вирусы должны быть как вирусы, а затем добавляться в библиотеку следов. У следа вирусной программы есть один недостаток. Существует период времени, когда вирус выпускается, когда библиотека известных следов обновляется. Вирус не будет распознаваться в течение этого периода, и это может повлиять на компьютер. Кроме того, характеристики программы — это второй способ обнаружения вирусов с мобильных устройств и компьютера. Этот метод называется эвристическим сканированием, и он проверяет действия, которые программа пытается предпринять или может предпринять. Он рассматривает тип системных

вызовов функций, включенных в исполняемый код. Если оно выглядеть слишком подозрительно, может пометить программу как возможный вирус и попросить вмешательства пользователя.

Преимущества антивирусной защиты

Загрузка или покупка любой антивирусной программы дает людям возможность купить любой компьютер (настольный или ноутбук) или купить любой модель мобильных устройство. Антивирусная программа – одна из лучшая безопасная мера, чтобы остановить и минимизировать риск и любые последствия. Существуют различные уровни защиты, и они зависят от конкретной антивирусной программы, предлагаемой надежными поставщиками. Однако есть много преимуществ, которые предлагают все антивирусные программы. Прежде всего, это предотвращает любой вирус, связанный с повреждением. Любая антивирусная программа помогает предотвратить повреждение операционной системы и других функций от любого вируса, который подключен к компьютеру или телефону. Во-вторых, антивирусная программа поддерживает безопасность мобильных устройств и ПК. Это происходит путем обновления антивирусного пакета или создания брандмауэра для повышения общей безопасности. Это помогает поддерживать работоспособность операционной системы, доступ к интернет-ресурсам и возможность просмотра. В-третьих, все антивирусные программы защищают данные и информацию. Вся информация, важные данные, презентации, файлы, документы, фотографии и другие материалы, хранящиеся на устройстве, защищены от вирусных атак.

Таким образом, использование антивирусной программы защищает компьютеры от вирусной атаки. Это помогает предотвратить атаку на данные и информацию. Антивирусная программа — это программное обеспечение, которое устанавливается на компьютер и используется для сканирования мобильных устройств и ПК с целью поиска любых вирусов, способных повредить компьютер. Существуют различные типы антивирусных программ, разработанных для использования в производстве. Существует множество

мощных антивирусных программ, построенных с высоким качеством защиты, таких как Norton и Mcafee. Кроме того, эта программа может обнаружить любой вирус двумя способами, которые являются следом (footprint) и характеристиками. Этот вид программы имеет много преимуществ использования, он помогает предотвратить любой вирус, который связан с повреждением телефона или компьютера, поддерживать безопасность ЦП и самое главное защищает данные и информацию.

2.2 Системы предотвращения вторжений

Система предотвращения вторжений (IPS), представляет собой технологию, которая отслеживает любые вредоносные действия, пытающиеся использовать известную уязвимость.

Почему следует использовать системы предотвращения вторжений (IPS)?

Технологии IPS могут обнаруживать или предотвращать атаки сетевой безопасности, такие как атаки методом грубой силы, атаки типа «отказ в обслуживании» (DoS) и эксплойты уязвимостей. Уязвимость - это слабое место в программной системе, а эксплойт - это атака, которая использует эту уязвимость для получения контроля над системой. Когда объявляется эксплойт, у злоумышленников часто появляется возможность воспользоваться этой уязвимостью до того, как будет применено исправление безопасности. В этих случаях можно использовать систему предотвращения вторжений, чтобы быстро заблокировать эти атаки [25].

Поскольку технологии IPS отслеживают потоки пакетов, их также можно использовать для принудительного использования безопасных протоколов и запрета использования небезопасных протоколов, таких как более ранние версии SSL или протоколы, использующие слабые шифры.

Как работают системы предотвращения вторжений?

Технологии IPS имеют доступ к пакетам там, где они развернуты, либо

как системы обнаружения сетевых вторжений (NID), либо как системы обнаружения хостовых вторжений (HID). Сетевой IPS имеет более широкий обзор всей сети и может быть развернут как встроенный в сеть, так и автономный в сети в качестве пассивного датчика, принимающего пакеты от сети TAP или порта SPAN.

В чем разница между IDS и IPS?

Ранние реализации этой технологии были развернуты в режиме обнаружения на специальных устройствах безопасности. По мере того как технология созрела и перешла в интегрированные брандмауэры следующего поколения или устройства UTM, данные технологии устанавливаются по умолчанию для предотвращения вредоносного трафика.

В некоторых случаях решение об обнаружении и принятии или предотвращении трафика основывается на уверенности в конкретной защите IPS. Когда существует более низкая уверенность в защите IPS, то существует более высокая вероятность ложных срабатываний. Ложное срабатывание-это когда IDS идентифицирует действие как атаку, но это действие является приемлемым поведением. По этой причине многие технологии IPS также имеют возможность захватывать последовательности пакетов из события атаки. Затем они могут быть проанализированы для определения наличия реальной угрозы и дальнейшего улучшения защиты IPS.

Существует ряд различных угроз:

– Атака типа отказа в обслуживании (DoS).
– Распределенная атака типа «отказ в обслуживании» (DDoS).
– Черви.
– Вирусы.

Системы предотвращения вторжений сканирует пакеты в режиме online. После завершения сканирования, в случае обнаружения подозрительные или вредоносные пакеты, выполняется одно из ниже рассмотренных действий:

Происходить блокировка доступа ко всем приложениям, после завершения эксплуатируемого сеанса TCP.

Выполняется перенастройка брандмауэра таким образом, чтобы была предотвращена подобная атака в будущем.

Происходить замена или удаление любой вредоносный контент, который остается в сети после атаки.

Типы профилактики

Система предотвращения вторжений обычно настроена на использование ряда различных подходов для защиты сети от несанкционированного доступа. К ним относятся:

На основе сигнатур - в подходе на основе сигнатур используются заранее определенные сигнатуры известных сетевых угроз. Когда инициируется атака, которая соответствует одной из этих сигнатур или шаблонов, система предпринимает необходимые действия.

На основе аномалий - подход на основе аномалий отслеживает любое ненормальное или неожиданное поведение в сети. При обнаружении аномалии система немедленно блокирует доступ к целевому хосту.

На основе политик - этот подход требует, чтобы администраторы настраивали политики безопасности в соответствии с политиками безопасности организации и сетевой инфраструктурой. Когда происходит действие, которое нарушает политику безопасности, выдается предупреждение и отправляется системным администраторам.

2.3 Сканеры уязвимости

Всем предприятиям нужен способ обнаружения уязвимостей в своих сетях. Это особенно актуально для крупных предприятий и компаний с конфиденциальными данными: банковское дело, правительство, финансы, юриспруденция, здравоохранение и образование — это отрасли, в которых защита сетевых данных и инфраструктуры имеет первостепенное значение. Но малые предприятия также должны обеспечить безопасность своей информации, не затрачивая все свое время и ресурсы на решение этой задачи

[15].

Сканеры уязвимостей веб-приложений — это автоматизированные инструменты, которые сканируют веб-приложения, обычно извне, для поиска уязвимостей безопасности, таких как межсайтовый скриптинг, SQL-инъекция, внедрение команд, обход пути и небезопасная конфигурация сервера. Эту категорию инструментов часто называют инструментами динамического тестирования безопасности приложений. Доступно большое количество коммерческих и открытых инструментов этого типа, и все эти инструменты имеют свои сильные и слабые стороны.

Основы управления уязвимостями

Знаете ли вы, защищена ли ваша ИТ-инфраструктура? Даже если конечные пользователи в настоящее время могут получить доступ к своим файлам и подключение к сети кажется нормальным, вы не можете гарантировать безопасность своей сети. В каждой сети есть дыра в безопасности, которую могут использовать злоумышленники или вредоносные программы. Цель состоит в том, чтобы как можно меньше свести к минимуму эти уязвимости, что является постоянной задачей, учитывая, что ваша сеть постоянно используется и изменяется, а угрозы безопасности постоянно развиваются.

Управление уязвимостями имеет много компонентов. Например, вы можете подумать, что достаточно установить антивирусное программное обеспечение, хотя на самом деле это приводит к тому, что вы проигрываете контроль повреждений. В первую очередь важно принять превентивные меры, чтобы исключить проблемы безопасности. Инструменты сканирования уязвимостей могут иметь значение.

По сути, программное обеспечение для сканирования уязвимостей может помочь администраторам ИТ-безопасности выполнять следующие задачи.

Выявление уязвимостей. Администраторы должны иметь возможность выявлять дыры в безопасности в своей сети на рабочих станциях, серверах,

брандмауэрах и т.д. Требуется автоматизированное программное обеспечение, чтобы поймать как можно больше таких уязвимостей. В то время как очень маленькие офисы, обладающие надежными ИТ-ресурсами, могут испытывать искушение управлять безопасностью сети вручную, предприятия любого размера выиграют от помощи, предоставляемой автоматизированным инструментом, для экономии времени.

Оценка рисков. Не все уязвимости одинаково актуальны. Инструменты сканирования могут классифицировать и классифицировать уязвимости, чтобы помочь администраторам расставить приоритеты по наиболее проблемным вопросам.

Решение проблем - После того, как вы определили приоритетные риски, их устранение может оказаться сложной задачей. Правильный инструмент может помочь вам автоматизировать процесс подготовки устройств.

Сообщение о пробелах в безопасности. Даже после устранения уязвимостей администраторам по-прежнему важно демонстрировать соблюдение соответствующих правил. Программное обеспечение для сканирования может облегчить создание отчетов о состоянии безопасности сети.

2.4 Методы шифрования данных

До 1970-х годов криптография использовалась почти исключительно в дипломатических, военных и правительственных приложениях. В течение 1980-х годов в финансовой и телекоммуникационной отраслях были развернуты аппаратные криптографические устройства. Первым массовым криптографическим приложением стала цифровая мобильная телефонная система конца 1980-х годов.

Сегодня все используют криптографию ежедневно: примеры включают разблокировку автомобиля или двери гаража с помощью устройства дистанционного управления, подключение к беспроводной локальной сети,

покупку товаров с помощью кредитной или дебетовой карты в обычном магазине или в Интернете, установка обновления программного обеспечения, совершение телефонного звонка по протоколу передачи голоса по IP или оплата проезда в общественном транспорте. Нет сомнений в том, что новые области приложений, такие как электронное здравоохранение, автомобильная телематика и интеллектуальные здания, сделают криптографию еще более повсеместной [29].

Криптология - увлекательная дисциплина на стыке компьютерных наук, математики и электротехники. Поскольку криптология быстро развивается, трудно успевать за всеми разработками. За последние 25 лет теоретические основы области были усилены. Теперь у нас есть твердое понимание определений безопасности и способов подтверждения безопасности конструкций. Также в области прикладной криптографии мы наблюдаем очень быстрое развитие: старые алгоритмы ломаются и отзываются, появляются новые алгоритмы и протоколы.

Шифрование - это способ скритые данных, чтобы только уполномоченные стороны могли понять информацию [14]. С технической точки зрения, это процесс преобразования читаемого человеком открытого текста в непонятный текст, также известный как зашифрованный текст.

Проще говоря, шифрование берет читаемые данные и изменяет их так, чтобы они выглядели случайными. Шифрование требует использования криптографического ключа: набора математических значений, согласованных как отправителем, так и получателем зашифрованного сообщения (рисунок 1).

Рисунок 1 — Общий алгоритм шифрования

Хотя зашифрованные данные кажутся случайными, шифрование происходит логическим и предсказуемым образом, позволяя стороне, которая получает зашифрованные данные и владеет правильным ключом, дешифровать данные, превращая их обратно в открытый текст. По-настоящему безопасное шифрование будет использовать ключи, достаточно сложные, чтобы третья сторона вряд ли расшифрует или взломает зашифрованный текст грубой силой - другими словами, угадав ключ.

Криптографический ключ - это строка символов, используемая в алгоритме шифрования для изменения данных, чтобы они выглядели случайными. Как и физический ключ, он блокирует (шифрует) данные, так что только тот, у кого есть правильный ключ, может их разблокировать (расшифровать) [28].

Системы, которые обеспечивают безопасность и конфиденциальность данных всегда будут востребованы и пользоваться большим спросом.

Всегда есть вероятность перехвата данных третьей стороной, после их отправки. Современные угрозы конфиденциальность данных требуют современных решений. Стоит отметить тот факт, что алгоритмом шифрованием в свое время использовали только военные и правительственные организации для распространения конфиденциальной информации, но в настоящее время данным методом пользуются почти все частные и государственные компании.

Двумя основными видами шифрования являются симметричное шифрование и асимметричное шифрование. Асимметричное шифрование также известно, как шифрование с открытым ключом.

В симметричном шифровании есть только один ключ, и все взаимодействующие стороны используют один и тот же (секретный) ключ как для шифрования, так и для дешифрования (рисунок 2).

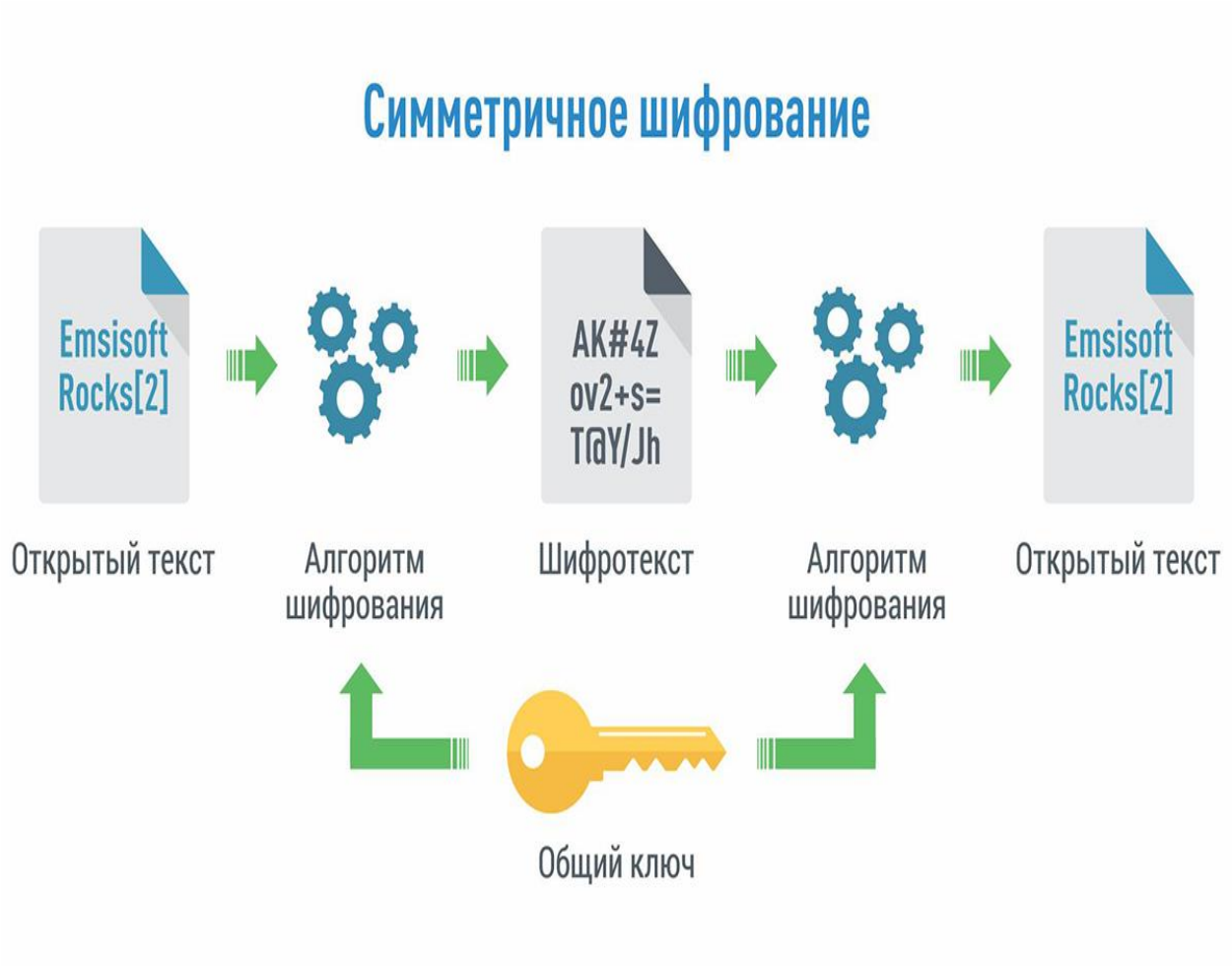

Рисунок 2 — Алгоритм симметричного шифрования

В асимметричном шифровании, или шифровании с открытым ключом, есть два ключа: один ключ используется для шифрования, а другой ключ используется для дешифрования.

Ключ дешифрования остается закрытым (отсюда и название «закрытый ключ»), в то время как ключ шифрования является общедоступным для использования кем угодно (отсюда и название «открытый ключ»). Асимметричное шифрование - это основополагающая технология TLS (часто называемого SSL) (рисунок 3).

Рисунок 3 - Алгоритм асимметричного шифрования

На сегодняшний день существует множество различных алгоритмов шифрования. Наиболее известными из которых являются следующие:

– AES. Расширенный стандарт шифрования (AES) - это надежный стандартный алгоритм, используемый правительством Соединенных Штатов, а также другими организациями. Хотя AES чрезвычайно эффективна в 128-битной форме, она также использует 192 - и 256-битные ключи для очень сложных целей шифрования. AES широко считается неуязвимым для всех атак, за исключением грубой силы. Несмотря на это, многие эксперты по интернет-безопасности считают, что AES в конечном итоге будет рассматриваться как стандарт шифрования данных в частном секторе.

– Triple DES. Triple DES является преемником оригинального алгоритма Стандарта шифрования данных (DES), созданного в ответ на хакеров, которые выяснили, как взломать DES. Это симметричное

шифрование, которое когда-то было наиболее широко используемым симметричным алгоритмом в отрасли, хотя оно постепенно прекращается. TripleDES применяет алгоритм DES три раза к каждому блоку данных и обычно используется для шифрования паролей UNIX и PIN-кодов ATM.

- RSA. RSA-это асимметричный алгоритм шифрования с открытым ключом и стандарт шифрования информации, передаваемой через Интернет. Шифрование RSA является надежным и надежным, потому что оно создает огромную кучу тарабарщины, которая расстраивает потенциальных хакеров, заставляя их тратить много времени и энергии на взлом систем.
- Blowfish. Blowfish – это еще один алгоритм, который был разработан для замены DES. Этот симметричный инструмент разбивает сообщения на 64-битные блоки и шифрует их по отдельности. Иглобрюх зарекомендовал себя за скорость, гибкость и нерушимость. Он находится в общественном достоянии, так что это делает его бесплатным, что еще больше повышает его привлекательность. Blowfish обычно используется на платформах электронной коммерции, для защиты платежей и в инструментах управления паролями.
- Twofish. Twofish – преемник Blowfish. Это безлицензионное симметричное шифрование, которое расшифровывает 128-битные блоки данных. Кроме того, Twofish всегда шифрует данные в 16 раундах, независимо от размера ключа. Twofish идеально подходит как для программных, так и для аппаратных сред и считается одним из самых быстрых в своем роде. Многие современные программные решения для шифрования файлов и папок используют этот метод.

2.4.1 Стандарт шифрования данных DES

Стандарт шифрования данных DES был самым популярным блочным шифром на протяжении большей части последних 30 лет. Несмотря на то, что в настоящее время он не считается защищенным от решительного злоумышленника, поскольку пространство ключей DES слишком мало, оно все еще используется в устаревших приложениях.

Кроме того, трехкратное шифрование данных с помощью DES - процесс, называемый 3DES или тройной DES - дает очень безопасный шифр, который все еще широко используется сегодня. Алгоритм шифрования DES на сегодняшний день является наиболее изученный симметричный алгоритм, принципы его построения вдохновили на создание многих современных шифров.

Анализируем примитивные операции в DES, которые могут быть применены для достижения надежного шифрования.

По мнению известного теоретика информации Клода Шеннона, существуют две примитивные операции, с помощью которых можно построить надежные алгоритмы шифрования:

Конфузия (путаница) - это операция шифрования, при которой скрывается связь между ключом и зашифрованным текстом. Сегодня обычным элементом для достижения путаницы является замещение, которое встречается как в DES, так и в AES.

Диффузия (распространение) - это операция шифрования, при которой влияние одного символа открытого текста распространяется на множество символов зашифрованного текста с целью сокрытия статистических свойств открытого текста.

Простым диффузионным элементом является битовая перестановка, которая часто используется в DES. AES использует более продвинутую операцию Mixcolumn.

Общий процесс для DES объясняется на диаграмме ниже (рисунок 4).

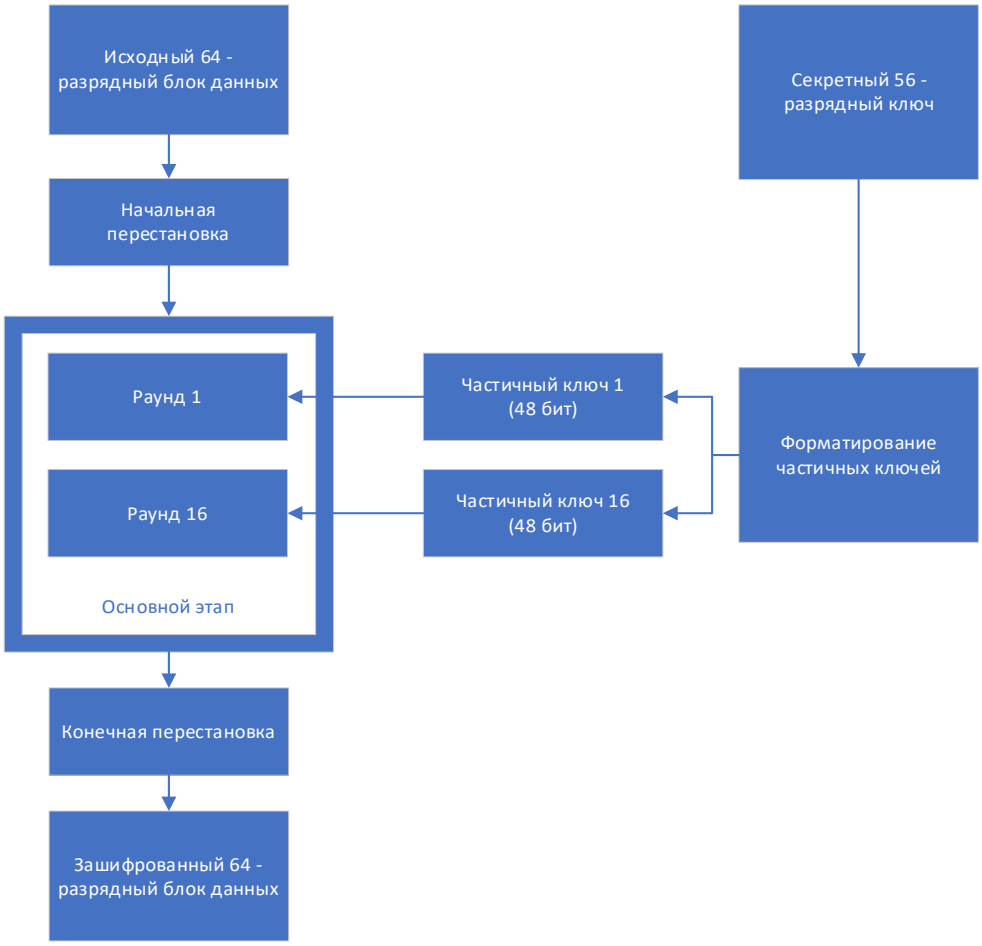

Рисунок 4 – Процесс шифрования алгоритма DES

В DES существует 2 входа для методы шифрования — это открытый текст, которого необходимо шифровать, и соответственно ключ. Длина открытого текста должно быть 64 бита, а ключ — 56 бит. Выполняется 16 этапов идентичных операций, в результате чего мы получаем 64-битный блок шифротекста.

Современные блочные шифры обладают отличными диффузионными свойствами. На уровне шифра это означает, что изменение одного бита открытого текста в среднем приводит к изменению половины выходных битов, то есть второй зашифрованный текст выглядит статистически независимым от первого. Это важное свойство, о котором следует помнить при работе с блочными шифрами.

2.4.2 Расширенный стандарт шифрования AES

К настоящему времени алгоритм выбора для многих, многих приложений стал Advanced Encryption Standard (AES). AES с тремя ключами длиной 128, 192 и 256 бит защищен от атак методом перебора в течение нескольких десятилетий, и нет никаких известных аналитических атак с разумными шансами на успех. AES стал результатом открытого конкурса, и на последнем этапе процесса отбора было четыре других алгоритма финалиста. Это блочные шифры Mars, RC6, Serpent и Twofish. Все они криптостойкие и довольно быстрые, особенно в программном обеспечении. Основываясь на сегодняшних знаниях, все они могут быть рекомендованы.

Advanced Encryption Standard (AES) - это наиболее широко используемый сегодня симметричный шифр. Несмотря на то, что термин «Стандарт» в его названии относится только к правительственным приложениям США, блочный шифр AES также является обязательным в некоторых отраслевых стандартах и используется во многих коммерческих системах. Среди коммерческих стандартов, которые включают AES, - стандарт безопасности Интернета IPsec, TLS, стандарт шифрования Wi-Fi IEEE 802.11i, сетевой протокол защищенной оболочки SSH (Secure hell), интернет-телефон Skype и многочисленные продукты безопасности по всему миру. На сегодняшний день нет известных атак против AES.

В 1999 году Национальный институт стандартов и технологий США (NIST) указал, что DES следует использовать только для устаревших систем, а вместо этого следует использовать тройной DES (3DES). Несмотря на то, что 3DES противостоит атакам методом перебора с помощью современных технологий, у него есть несколько проблем. Во-первых, это не очень эффективно с точки зрения программных реализаций. DES уже не особенно хорошо подходит для программного обеспечения, а 3DES в три раза медленнее, чем DES. Другим недостатком является относительно небольшой размер блока в 64 бита, что является недостатком в некоторых приложениях,

например, если кто-то хочет построить хеш-функцию из блочного шифра. Наконец, если вас беспокоят атаки с использованием квантовых компьютеров, которые могут стать реальностью через несколько десятилетий, желательна длина ключа порядка 256 бит. Все эти соображения привели NIST к выводу, что необходим совершенно новый блочный шифр вместо DES.

В 1997 году NIST объявил о внесении предложений по новому усовершенствованному стандарту шифрования (AES). В отличие от разработки DES, выбор алгоритма для AES был открытым процессом, управляемым NIST. В трех последующих раундах оценки AES NIST и международное научное сообщество обсудили преимущества и недостатки представленных шифров и сузили число потенциальных кандидатов. В 2001 году NIST объявил блочный шифр Rijndael новым AES и опубликовал его в качестве окончательного стандарта (FIPS PUB 197). Rijndael был разработан двумя молодыми бельгийскими криптографами.

Ожидается, что в ближайшие несколько десятилетий AES будет доминирующим алгоритмом с симметричным ключом для многих коммерческих приложений.

Количество внутренних раундов шифра зависит от длины ключа в соответствии с таблицей 1.

Таблица 1 - Длина ключей и количество раундов для AES

Длина ключей	№ раундов
128 бит	10
192 бит	12
256 бит	14

В отличие от DES, AES не имеет структуры Фейстеля. Сети Фейстеля не шифруют весь блок за одну итерацию, например, в DES 64/2 = 32 бита шифруются за один раунд. AES, с другой стороны, шифрует все 128 бит за одну итерацию. Это одна из причин, по которой у него сравнительно небольшое количество раундов.

AES состоит из так называемых слоев. Каждый уровень управляет всеми

128 битами пути данных. Путь к данным также называется состоянием алгоритма. Есть только три разных типа слоев. Каждый раунд, за исключением первого, состоит из всех трех уровней. Более того, последний раунд не использует преобразование, что делает схему шифрования и дешифрования симметричной.

Расширенный стандарт шифрования (AES) — это доверенный стандартный алгоритм, используемый многими крупными организациями и даже правительством Соединенных Штатов. Расширенный стандарт шифрования (AES) чрезвычайно эффективен в 128-битной форме, он также использует 192 и 256-битные ключи для очень сложных целей шифрования.

Вывод к главе 2

Вторая глава посвящена исследованию и анализу эффективных методов защиты информации. Защита информации - это процесс защиты важных или конфиденциальных данных от повреждения, компрометации или потери [3]. Поскольку объем создаваемых и хранимых данных увеличивается с беспрецедентной скоростью, защита данных становится все более важной. Кроме того, бизнес-операции все больше зависят от данных, и даже короткий период простоя или небольшая потеря данных может иметь серьезные последствия [26].

Итак, в данной работе рассмотрен и исследован ряд методов и программных продуктов, которые предназначены для защиты данных. Выявлены основные преимущества и недостатки. Были сделаны определенные выводы касательно эффективности алгоритмы защиты данных. Необходимо подчеркнуть, что не один метод защиты не может гарантировать полную конфиденциальность и безопасность данных, но может существенно уменьшить риск потери.

Глава 3 Анализ алгоритмов защиты персональных данных

Основным соображением при разработке алгоритма шифрования должна быть безопасность алгоритма от нежелательных атак. Однако в реальном мире производительность и стоимость внедрения также являются важными проблемами. В данной работе безопасность алгоритмов от атак не сравнивалась. Основное внимание уделяется сравнению алгоритмов шифрования на основе их производительности и простоты реализации. Конфиденциальность информации является важнейшей задачей каждой организации. Поэтому для решения данной задачи используются различные методы защиты данных. «Зашифрованные данные безопасны в течение некоторого времени, но никогда не думайте, что они постоянно безопасны».

На сегодняшний день реализовано много алгоритмов шифрования и у каждого есть свой процесс создания ключа. Ключ шифрования выполняет важнейшую роль в общем процессе обработки информации (рисунок 5).

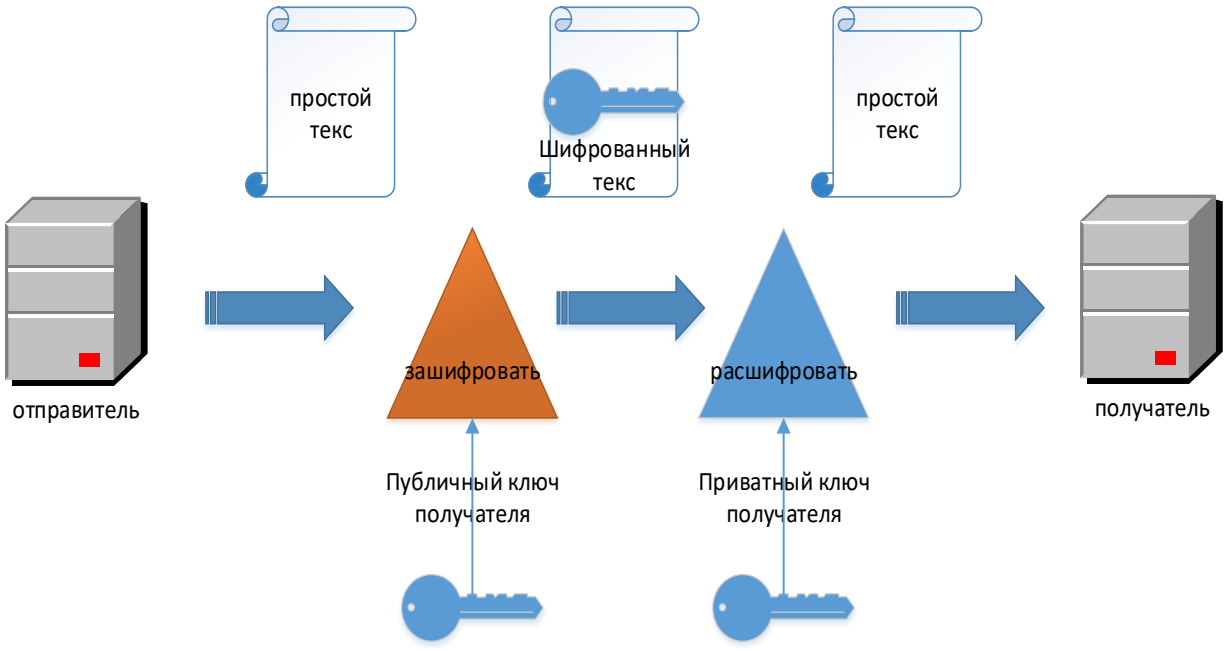

Рисунок 5 – Процесс шифрования и дешифрования

В данной главе исследуем и анализируем различные алгоритмы и методы шифрования для улучшения защиты данных, информационной безопасности с использованием шифрования. Проведем сравнение алгоритмов шифрования на основе их производительности, размера ключа, эффективности аппаратного и программного обеспечения, доступности, методов реализации и скорости.

Измерим быстродействие (скорость) шифрования, используя разные методы защиты, которые доступны в качестве стандарта в Oracle JDK (Eclipse IDE, IntelliJ IDEA). Далее проведем детальный анализ разных характеристик методов защиты данных. Рассматриваются алгоритмы шифрования Blowfish, IDEA, AES, Triple DES и DES.

Сравниваем время потраченное на шифрование разных чисел 16-байтовых блоков информации используя алгоритмов Blowfish, AES, Triple DES и DES. Результат показано на рисунке 6.

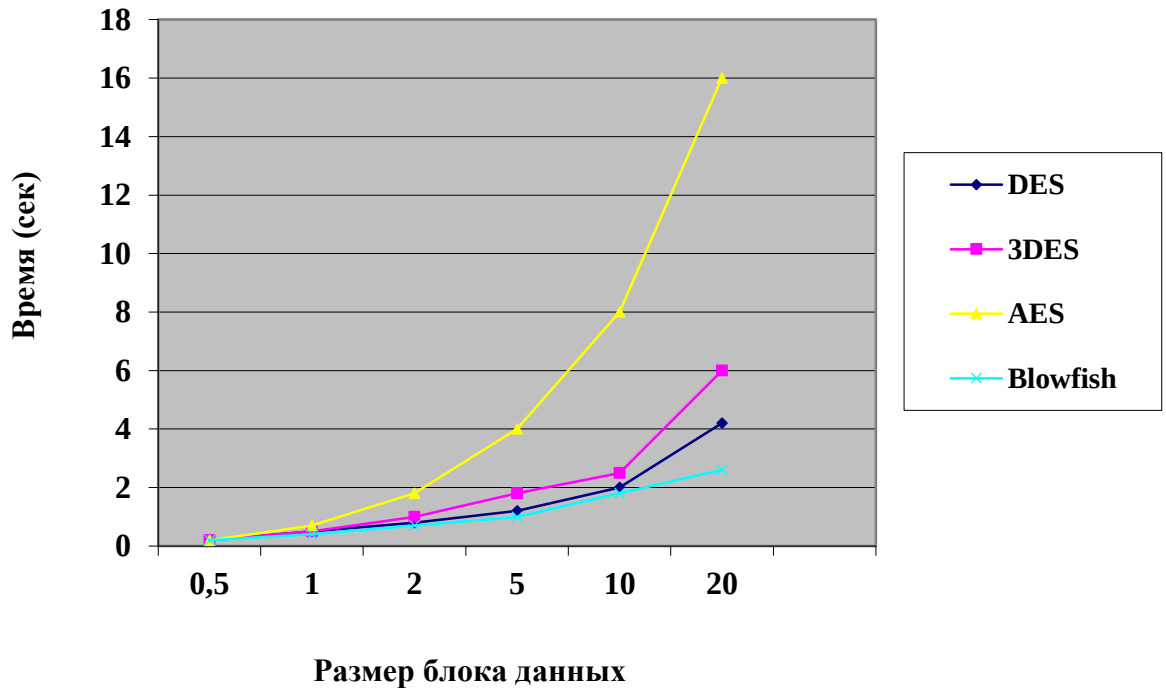

Рисунок 6 – Время шифрования алгоритмов Blowfish, AES, Triple DES и DES

Важно с самого начала отметить, что за каким-то нелепым моментом не стоит жертвовать скоростью ради безопасности. Однако измерения все равно помогут нам принять определенные решения.

Рассмотрим стандарт шифрования данных (DES).

DES (стандарт шифрования данных) в настоящее время является наиболее широко используемым блочным шифром в мире. В мае 1973 года NIST (затем NBS) призвал к использованию возможных алгоритмов шифрования в неклассифицированном принятом алгоритме шифрования, который входит во многие стандарты по всему миру (например, австралийский стандарт AS2805.5-1985).

Одним из крупнейших пользователей DES является банковский сектор. Именно для этого использования DES был в первую очередь стандартизирован, а ANSI подтвердил его использование на 5-летний период - в будущем он будет заменен на AES. Хотя стандарт DES является общедоступным, используемые критерии проектирования засекречены. Дизайн вызвал серьезные разногласия, особенно по поводу выбора 56-битного ключа.

Рассмотрим Международный алгоритм шифрования данных (IDEA).

IDEA - это блочный шифр, разработанный Джеймсом Мэсси и Сюэцзя Лай и впервые описанный в 1991 году. Он использует 128-битный ключ, который работает с 64-битными блоками.

Он состоит из серии из восьми идентичных преобразований, основанных на побитовых модулях «исключающее ИЛИ», сложении и умножении. Он основан на симметричном шифре и имеет очень слабый метод разработки ключей, поэтому уровень безопасности алгоритма очень низкий по сравнению с DES. IDEA не становился такой популярной из-за своей сложной структуры

Рассмотрим алгоритм Blowfish.

Большинство алгоритмов шифрования сегодня недоступны для общественности - многие из них защищены патентами (например, Khufu, REDOC II и IDEA) или держатся в секрете правительствами (например,

Skipjack и Capstone охраняются правительством США).

Многие другие алгоритмы доступны только частично (например, RC2, RC4 и ГОСТ). Брюс Шнайер - один из ведущих криптологов мира и президент крупной консалтинговой фирмы, специализирующейся на криптографии и компьютерной безопасности, - разработал алгоритм Blowfish и сделал его общедоступным. Blowfish - это 64-битный блочный шифр с ключом переменной длины. С самого начала он стремился создать этот новый алгоритм шифрования, чтобы предоставить миру новый стандарт шифрования.

Алгоритм Blowfish был впервые представлен в 1993 году и еще не был взломан. Также стоит отметить, что этот алгоритм можно оптимизировать в аппаратных приложениях, хотя он, как и большинство других шифров, часто используется в программных приложениях.

Рассмотрим алгоритм «Тройной DES (3DES)».

Алгоритм тройного DES (3DES) был необходим в качестве замены DES из-за достижений в поиске ключей. 3DES - это предложение, основанное на существующем DES, стандартизированное в ANSI X9.17, ISO 8732 и PEM для управления ключами. Он также был предложен ANSI X9 для общего стандарта EFT.

Он обратно совместим с существующим одиночным DES (когда K1 = K2 = K3). Алгоритм 3DES использует два или три 56-битных ключа. Таким образом, эффективная длина ключа составляет до 168 бит. 3DES определяется следующей функцией:

$$C = DES_{k3}\{DES\__i k2\{DES_{k1}(P)\}\} \quad (1)$$

Рассмотрим расширенный стандарт шифрования (AES).

В сентябре 1997 года NIST США объявила о призыве к кандидатским шифрам для своего нового расширенного стандарта шифрования (AES), поскольку в то время явно требовалась замена DES. Кандидатские шифры

должны были быть представлены к июню 1998 года, а финалист был выбран в октябре 2000 года. В общей сложности 15 кандидатов были приняты в июне 98 (6 были отклонены как неполные), а 5 были включены в короткий список в августе 99.

Наконец, Риндаэль (Rijmen) был выбран финалистом AES в октябре 2000 года.

NIST опубликовал все материалы и несекретные анализы. Кандидаты AES - это последнее поколение блочных шифров, у которых значительно увеличен размер блока - от старого стандарта 64 бит до 128 бит; и ключи от 128 до 256 бит.

Частично это было вызвано публичными демонстрациями исчерпывающего поиска ключей DES и RC-5 (на 64-битных).

После исчерпывающего анализа и оценки, Rijndael, разработанный Rijmen & Daemen в Бельгии, был выбран финалистом AES. Он имеет следующие атрибуты:

а) 128-битный размер блока;

б) размер ключа 128, 192 или 256 бит;

в) итеративный, а не шифр Файстеля (как ИДЕЯ);

г) обрабатывает данные как 4 группы по 4 байта;

д) имеет 9, 11 или 13 раундов, где каждый раунд состоит из:

- шаг подстановки байтов (используется 1 Sbox на каждом байте);
- шаг сдвига строк (перетасовка байтов между группами);
- шаг смешивания столбцов;
- шаг добавления круглого ключа.

Все операции могут быть объединены в поиск xor и таблиц - следовательно, реализация может быть очень быстрой и эффективной (рисунок 7).

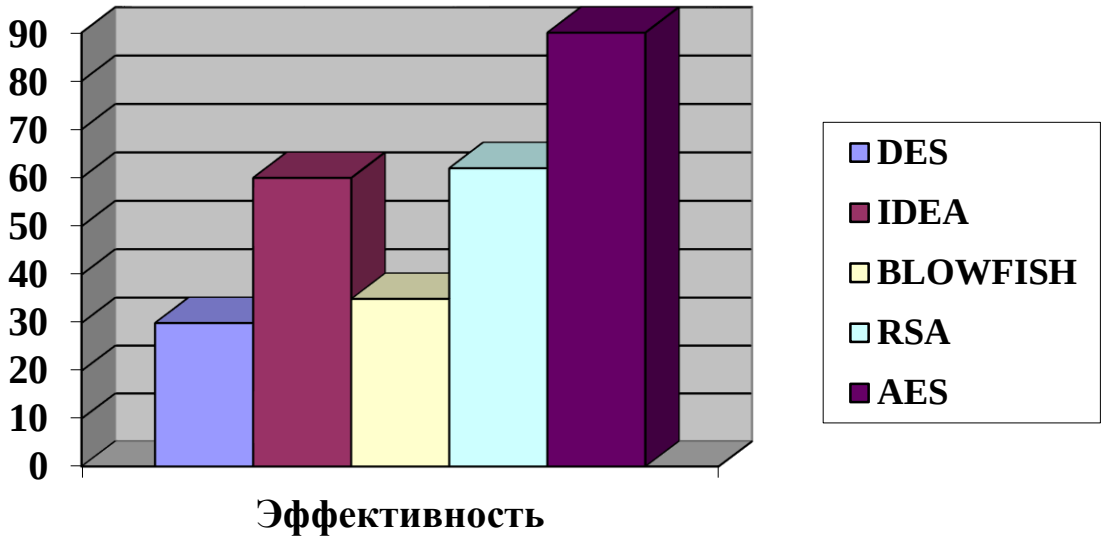

Рисунок 7 - Сравнение шифрования на основе процентной эффективности

Как известно для симметричных шифров один ключ как для шифрования, так и для дешифрования.

Стоит отметить тот факт, что принято считать достаточным длины ключей для конфиденциальности данных, включая уровень "секретно".

Но для данных входящих в уровень "Совершенно секретно" требуется либо 192, либо 256-битных длин ключей.

Существует 10 раундов для 128-битных ключей, 12 раундов для 192-битных ключей и 14 раундов для 256-битных ключей.

Каждый раунд содержит несколько стадии реализации, которые включают подстановку, транспозицию и смешивание входного открытого текста, и преобразование его в конечный вывод зашифрованного текста (рисунок 8).

Рисунок 8 - Процесс преобразования AES-шифрования

На следующем рисунке показаны все этапы шифрования от простого текста до зашифрованного текста (рисунок 9).

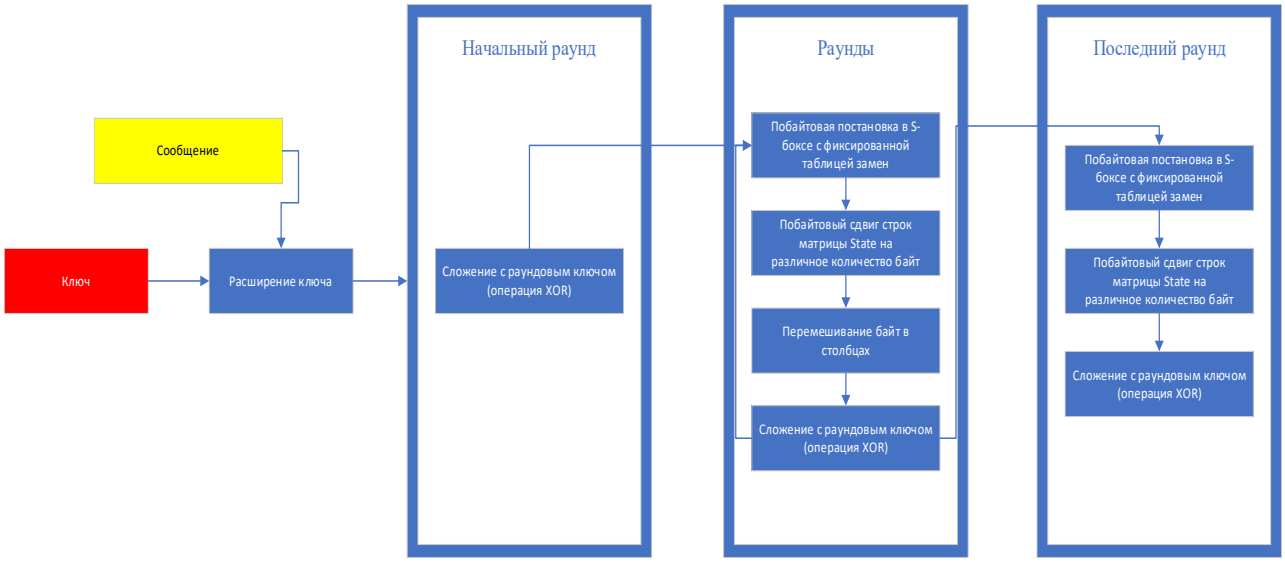

Рисунок 9 – Этапы каждого раунда шифрования

Фаза шифрования AES может быть разбита на три фазы: начальный раунд, основные раунды и заключительный раунд. Все фазы используют одни и те же подоперации в различных комбинациях как показано на рисунке 3.4.

Выводы к главе 3

Третья глава посвящена анализу алгоритмов защиты данных. Изучение различных алгоритмов показывает, что сила и прочность алгоритма зависит от управления ключами, типа криптографии, количества ключей, количества битов, используемых в ключе. Все ключи основаны на математических свойствах. Ключи, имеющие большее количество битов, требуют большего времени вычислений, что просто указывает, что системе требуется больше времени для шифрования данных.

Таким образом, после сравнения методов защиты данных, получение результаты говорят о том, что защиты данных AES является более математически эффективным и элегантным криптографическим алгоритмом, но его основная сила заключается в возможности использования ключей различной длины. AES позволяет вам выбрать 128-битный, 192-битный или 256-битный ключ, что делает его экспоненциально сильным. AES использует перестановку-подстановку, которая включает в себя ряд шагов подстановки и перестановки для создания зашифрованного блока.

Глава 4 Оценка эффективности алгоритмов защиты информации персональных данных в мобильных клиентах при доступе к удаленным ИС

Термин криптография определяется как шифрование конфиденциальной информации, такой как данные, изображения и другие. Методы криптографии менялись на протяжении многих лет, основываясь на разработках программного обеспечения для шифрования и алгоритмов шифрования. Конфиденциальные данные должны быть защищены от кражи и чтения посторонними лицами, независимо от того, хранятся ли эти данные на жестких дисках, флэш-памяти, ноутбуках, настольных компьютерах или других устройствах хранения. Процесс криптографии включает в себя преобразование стандартного текста (называемого обычным текстом) во что-то неразборчивое (называемое шифрованным текстом) [4]. Расшифровка-это противоположность шифрованию; это процесс преобразования непонятного языка в обычный текст.

В 1977 году правительству США потребовался метод, который позволил бы безопасно хранить их конфиденциальную информацию [10]. Решение их проблемы было найдено благодаря выпуску Стандарта шифрования данных (DES) в том же году. DES-это 56-битная длина ключа с 64-битным размером блока.

Наблюдение за работой DES показало, что она была беззащитна перед атаками грубой силы. По этой причине Национальный институт стандартов и технологий обратился с публичным запросом о разработке нового стандарта шифрования. В общей сложности пятнадцать алгоритмов были получены и представлены двенадцатью различными странами. Из этих пятнадцати были выбраны только пять алгоритмов: MARS, RC6, Serpent, Rijndael и Twofish. Rijndael был лучшим алгоритмом и назывался Advanced Encryption Standard (AES). Вторым лучшим вариантом была Serpent, за которой следовали Twofish.

Твердотельные диски (SSD) широко используются государственными

органами и службами безопасности. В основном они используют флэш-память на основе NAND, в которой информация представлена электронами, захваченными плавающим затвором между нормальным затвором и каналом транзисторной ячейки, что исключает механическую вращающуюся головку в старых жестких дисках (HDD). Технологии развивались с годами. Флэш-память SSD с одноуровневой ячейкой (SLC) была основной технологией, используемой в первом поколении SSD, и до сих пор используется благодаря своей высокой надежности и широкому диапазону чтения; он хранит один бит (0, 1) в одной ячейке, где ячейка с захваченным электроном представляет «0», а отсутствие электрона означает «1».

Существует также флэш-память SSD с многоуровневыми ячейками (MLC), в которой хранятся два бита (00, 01, 10. 11) на одну ячейку, и флэш-память SSD третьего поколения с трехуровневыми ячейками (TLC), хранящая три бита. (000, 001, ..., 110, 111) в одной ячейке. Хотя твердотельные накопители на базе флэш-памяти 3D TLC NAND стремительно набирают популярность, в настоящее время флэш-память NAND MLC на основе твердотельных накопителей все еще доминирует на рынке хранилищ из-за постоянного увеличения емкости, снижения цены и высоких скоростей чтения и записи.

Жесткий диск (HDD), как и старая технология, основанная на магнитном поле, использует головку записи/чтения, которая охватывает один или несколько дисков для доступа к хранящейся информации. Скорость жесткого диска измеряется в оборотах в минуту (об / мин). Частота вращения жесткого диска может достигать 5400 об / мин и 15000 об / мин. Преимущество использования жесткого диска заключается в том, что он дает возможность хранить большой объем данных и его дешевую цену по сравнению с SSD.

Твердотельный гибридный накопитель (SSHD)-это интегрированная технология, которая сочетает в себе технологию NAND flash SSD и HDD. Цель NAND flash SSD на гибридном диске-ускорить процесс загрузки или, в некоторых редких случаях, выступать в качестве кэша для данных, хранящихся

на жестком диске.

Поскольку эти устройства хранения данных являются портативными и легкими, они подвержены высокому риску потери или кражи и доступа к ним посторонних лиц. Шифрование гарантирует, что данные в устройствах хранения останутся конфиденциальными от несанкционированного доступа и изменения данных.

В настоящее время разработано несколько программных средств шифрования для обеспечения конфиденциальности данных на устройствах хранения. Например, TrueCrypt - это программное обеспечение для шифрования дисков с открытым исходным кодом. Это программное обеспечение может работать в различных операционных системах. TrueCrypt может превращать файл в зашифрованный виртуальный диск.

С другой стороны, BestCrypt - это лицензионное программное обеспечение для шифрования, созданное разработчиком приложения Греем. BestCrypt широко используется в правительстве, военных ведомствах, организациях здравоохранения, страховых компаниях и других организациях. Функциональность BestCrypt аналогична программному обеспечению шифрования TrueCrypt в том, что оно способно хранить файлы в контейнере, похожем на жесткий диск [9]. И TrueCrypt, и BestCrypt поддерживают 256-битные алгоритмы шифрования AES, Serpent и Twofish.

В 2009 году Эльминаам и др. сравнили производительность различных алгоритмов симметричного шифрования, включая DES, 3DES, AES, RC4 и RC6. Также было изучено влияние алгоритмов шифрования на использование процессора и время автономной работы ноутбуков. Кроме того, было проведено сравнение времени шифрования и дешифрования этих алгоритмов на основе различных размеров пакетов и типов данных (таких как текстовый файл и изображение). Исследователи пришли к выводу, что Blowfish работает лучше, чем другие алгоритмы, из-за изменения размера пакета. Кроме того, они определили, что RC4, RC6 и Blowfish отнимают больше времени при шифровании и дешифровании изображений, чем другие алгоритмы. Наконец,

они упомянули, что изменение ключей шифрования AES на самый высокий ключ (256 бит) увеличит потребление энергии и времени.

В 2014 году Кансал и Миттал упомянули о значительном использовании шифрования в электронных транзакциях через Интернет. Исследователи изучили различные алгоритмы симметричного шифрования, включая DES, 3DES и AES. Исследование было основано на различных параметрах и типах данных, таких как текстовый файл и изображение на процессоре i7. Они пришли к выводу, что AES требует меньшего времени шифрования и дешифрования по сравнению с DES и 3DES. Однако 3DES использует меньше памяти, чем другие алгоритмы.

В 2018 году Слиман и др. предложили криптосистему изображений на основе хэш-ключа с использованием 2D-логистических карт и клеточных автоматов для обеспечения безопасности мультимедийных данных. Основываясь на данных, собранных в ходе статистических тестов, пространстве ключей, информации об энтропии и дифференциальных атаках, они пришли к выводу, что их криптосистема быстра и эффективна для шифрования. Аналогичным образом, в 2018 году Юань и др. предложили разработать и внедрить высокопроизводительную систему шифрования на основе алгоритма AES. Предлагаемая ими криптосистема поддерживает все три режима, включая AES-128, -192 и -256, разделенные на 4 этапа для каждой операции раунда как для шифрования, так и для дешифрования. Основным преимуществом предложенной выше криптосистемы является производительность и пропускная способность за счет реализации 4-ступенчатых конвейеров.

Чтобы еще больше повысить безопасность очистки данных в недорогой флэш-памяти MLC, Lin et. al. предложили схему быстрой дезинфекции. Схема обеспечивает быструю очистку старых данных с нулевыми накладными расходами на копирование данных в реальном времени при создании новых данных. Конструкция позволяет очищать верхнюю или нижнюю страницу без нарушения данных на связанной нижней или верхней странице и устраняет

необходимость в резервном копировании данных.

Кроме того, в 2019 году исследователи Мейер и Ван Гастел проанализировали аппаратное шифрование всего диска нескольких твердотельных накопителей (SSD), выпущенных тремя производителями в период с 2014 по 2018 год, с использованием внутренних интерфейсов SATA и NVMe или внешнего интерфейса USB. Анализ прошивки этих устройств проводился методом RE (обратный инжиниринг). Они пришли к выводу, что критические недостатки безопасности во многих из этих моделей из-за спецификации, дизайна или реализации, позволяющие полностью восстановить данные злоумышленником, даже если данные были защищены с помощью Microsoft Windows Integrated, BitLocker на этих моделях.

Учитывая недавние оценки и сосредоточив внимание на распространенных устройствах хранения, в этой статье исследуется производительность шифрования 256-битных ключей AES, Serpent и Twofish на жестких дисках, SSHD и SSD-дисках NAND MLC с использованием TrueCrypt и BestCrypt. Подробные экспериментальные результаты, представленные в этом документе, позволяют потребителям решений для хранения данных определить, какой алгоритм шифрования лучше всего работает на этих устройствах хранения. Кроме того, он предоставляет им подробную информацию о производительности шифрования обоих программных продуктов шифрования, что может позволить им выбрать правильный программный продукт шифрования для защиты своих устройств хранения.

Остальная часть этого документа организована следующим образом: в разделе 4.1 подробно обсуждаются оценки производительности в двух подразделах, посвященных настройке системы и результатам экспериментов; В этом подразделе в общих чертах излагаются результаты оценочных тестов и сравниваются результаты, и, наконец, раздел 4.2 завершает работу.

4.1 Оценка эффективности решений

Мы создали тестовую среду с жесткими дисками Western Digital, Seagate SSHD и Samsung 128 ГБ флэш-памяти MLC SSD в комплексной системе.

Утилиты хранения Anvil используются для сравнения скорости чтения и записи устройства хранения. Инструмент тестирования определяет скорость устройства хранения при различных схемах доступа к диску, включая 4 МБ последовательного чтения, произвольного чтения 4 КБ, последовательной записи 4 МБ и произвольной записи 4 КБ. Samsung 128 ГБ флэш-памяти MLC SSD имеет 256 МБ кэш-памяти для увеличения скорости чтения и записи устройства хранения.

Размер тестового файла, который отправляется инструментом измерения производительности (Anvil’s Storage Utilities) на устройство хранения, составляет 1 ГБ для перезаписи кеша, который определит фактическую производительность хранилища. Для получения более точных результатов каждый эксперимент проводится 10 раз. После этого определяется средняя производительность чтения и записи каждого устройства хранения [30].

Скорость последовательного чтения 4 МБ - это схема доступа к диску, при которой блоки данных по 4 МБ считываются из соседних мест на поверхности устройства. Скорость произвольного чтения 4K - это модель доступа к диску, при которой небольшие (4 КБ) блоки данных считываются из случайных мест на поверхности тестируемого устройства.

Обычно они измеряются в МБ / с. Последовательная запись 4 МБ - это шаблон доступа к диску, при котором блоки данных по 4 МБ записываются из соседних мест на поверхности устройства.

Случайная запись 4K - это шаблон доступа к диску, при котором небольшие (4 КБ) блоки данных записываются из случайных мест на поверхности устройства хранения.

4.2 Результаты экспериментов

На рисунке 10 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к жесткому диску с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения данных с шифрованием работает лучше всего. После применения к жесткому диску с помощью BestCrypt средняя скорость последовательного чтения AES с 256 битами 4 МБ составляет 58,70 Мб / с. Для сравнения, при использовании TrueCrypt средняя скорость последовательного чтения 4 МБ AES составляет 59,14 МБ / с. Скорость последовательного чтения AES 256 бит 4 МБ при использовании TrueCrypt на 0,75% выше, чем BestCrypt.

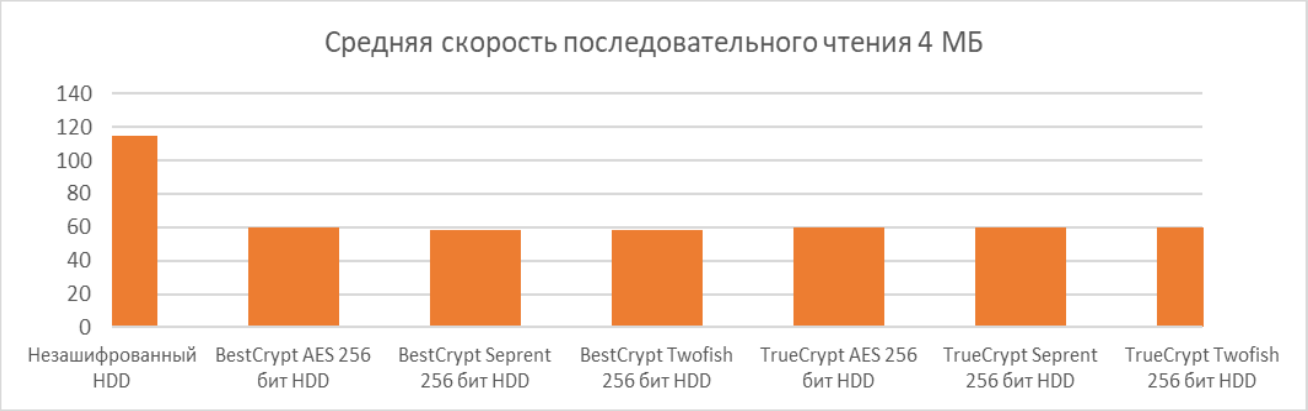

Рисунок 10 - Сравнение средней скорости последовательного чтения жесткого диска 4 МБ после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt

Точно так же скорость последовательного чтения Serpent 256-бит 4 МБ составляет 58,43 МБ / с при применении BestCrypt и 59,32 МБ / с при применении TrueCrypt, что означает, что он работает на 1,52% лучше с TrueCrypt, чем с BestCrypt. Наконец, скорость последовательного чтения Twofish 256-бит 4 МБ составляет 57,48 МБ / с при применении BestCrypt и 59,22 МБ / с при применении TrueCrypt. Это разница 3,03%.

На рисунке 11 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к жесткому диску с использованием TrueCrypt и

BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения шифрования работает лучше всего. После применения к жесткому диску с помощью TrueCrypt средняя скорость произвольного чтения AES в 256-битном формате 4K составляет 0,47 Мбит / с. Для сравнения, при использовании BestCrypt средняя скорость произвольного чтения 4K AES в 256-битном формате составляет 0,50 Мбит / с. Скорость произвольного чтения AES 256-битного формата 4K на 6,38% лучше при использовании BestCrypt, чем TrueCrypt. Точно так же скорость произвольного чтения Serpent 256-бит 4K составляет 0,43 Мбит / с при применении TrueCrypt и 0,49 Мбит / с при применении BestCrypt, что означает, что на BestCrypt он работает на 13,95% лучше, чем на TrueCrypt.

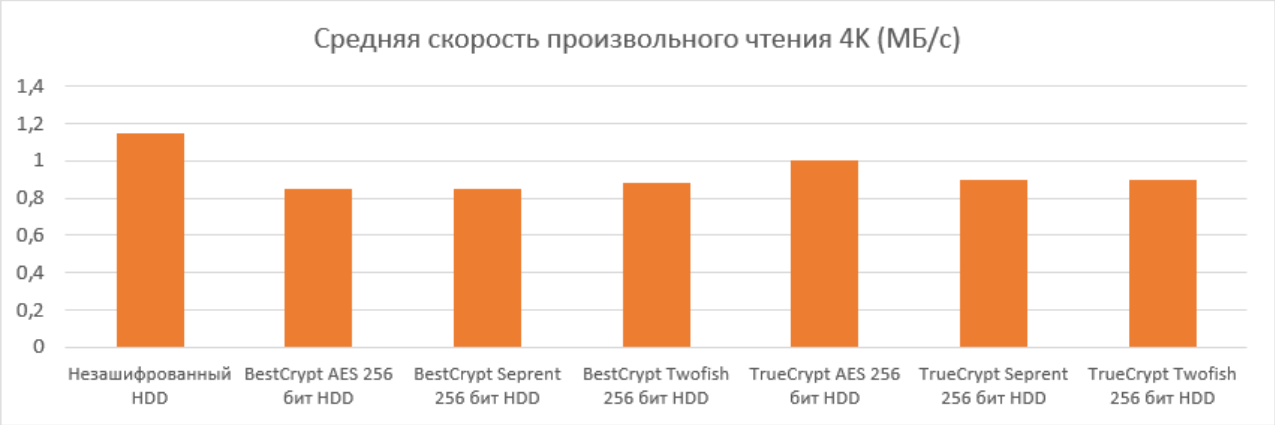

Рисунок 11 - Сравнение средней скорости произвольного чтения 4K жесткого диска после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt

Наконец, скорость произвольного чтения 256-битного 4K Twofish составляет 0,42 Мбит / с при применении TrueCrypt и 0,49 Мбит / с при применении BestCrypt. Это разница в 16,67%. На рисунке 3 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к жесткому диску с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо каждый из них работает, и определить, какой тип программного обеспечения для хранения шифрования работает лучше всего. После применения к жесткому диску с помощью BestCrypt, средняя скорость

последовательной записи AES 256-бит 4 МБ составляет 51,13 МБ / с. Для сравнения, при использовании TrueCrypt средняя скорость последовательной записи 4 МБ AES составляет 51,64 МБ / с. Скорость последовательной записи AES 256 бит и 4 МБ на 1,00% выше при использовании TrueCrypt, чем BestCrypt. Точно так же скорость последовательной записи Serpent 256-бит 4 МБ составляет 51,08 МБ / с при применении BestCrypt и 51,99 МБ / с при применении TrueCrypt, что означает, что он работает на 1,78% лучше с TrueCrypt, чем с BestCrypt. Наконец, скорость последовательной записи Twofish 256-бит 4 МБ составляет 51,45 МБ / с при применении BestCrypt и 52,00 МБ / с при применении TrueCrypt. Это разница на 1,07% (рисунок 12).

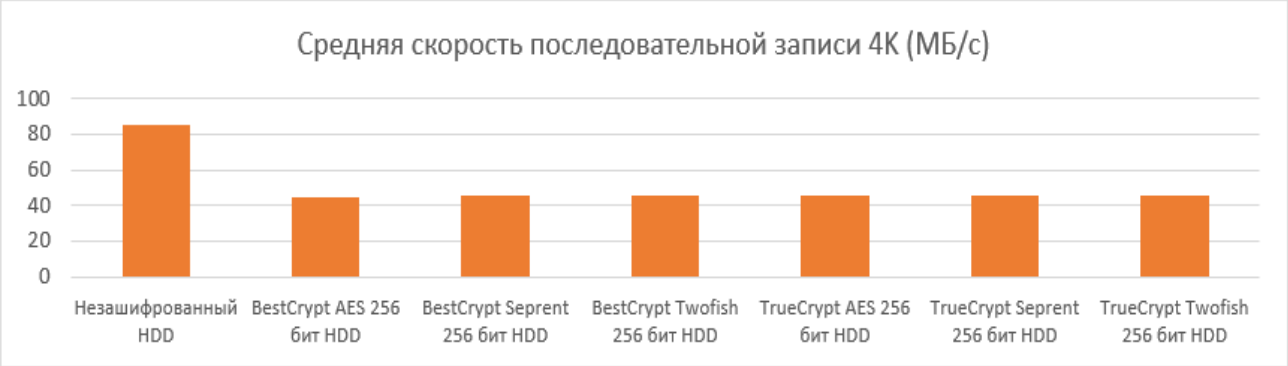

Рисунок 12 - Сравнение средней скорости последовательной записи на жестком диске 4 МБ после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt

На рисунке 13 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к жесткому диску с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения данных с шифрованием работает лучше всего. После применения к жесткому диску с помощью BestCrypt средняя скорость произвольной записи 256-битного AES в формате 4K составляет 0,93 Мб / с. Для сравнения, при использовании TrueCrypt средняя скорость произвольной записи 4K AES в 256-битном формате составляет 1,01 Мбит / с. 256-битная скорость произвольной записи 4K AES при использовании TrueCrypt на 8,60% лучше, чем BestCrypt. Точно так же

скорость произвольной записи Serpent 256-бит 4K составляет 0,91 МБ / с при применении BestCrypt и 0,99 МБ / с при применении TrueCrypt, что означает, что на TrueCrypt он работает на 8,79% лучше, чем на BestCrypt. Наконец, скорость произвольной записи Twofish 256-бит 4K составляет 0,92 МБ / с при применении BestCrypt и 0,99 МБ / с при применении TrueCrypt. Это разница

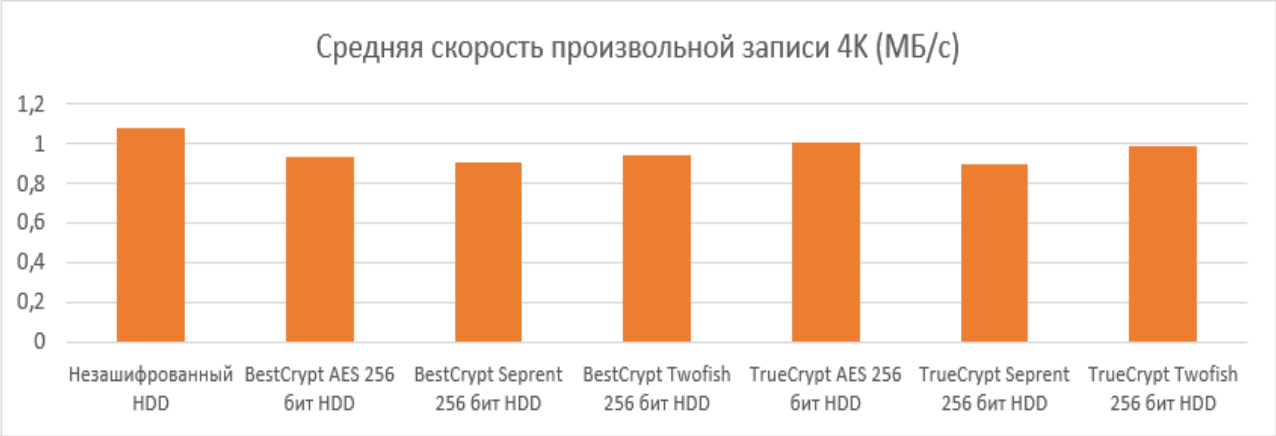

Рисунок 13 - Сравнение средней скорости случайной записи 4K на жестком диске после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt.

На рисунке 14 показано, что к устройству хранения SSHD применяются три различных алгоритма шифрования с использованием True Crypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения данных с шифрованием работает лучше всего. После применения к устройству хранения SSHD с использованием TrueCrypt, средняя скорость последовательного чтения AES с 256 битами 4 МБ составляет 64,55 Мбит / с. Для сравнения, при использовании BestCrypt средняя скорость последовательного чтения 4 МБ AES составляет 75,95 МБ / с. Скорость последовательного чтения AES 256 бит 4 МБ на 17,66% выше при использовании BestCrypt, чем TrueCrypt. Точно так же скорость последовательного чтения Serpent 256-бит 4 МБ составляет 65,94 МБ / с при применении TrueCrypt и 71,90 МБ / с при применении BestCrypt, что означает,

что на BestCrypt он работает на 9,04% лучше, чем на TrueCrypt. Наконец, скорость последовательного чтения Twofish 256-бит 4 МБ составляет 68,76 МБ / с при использовании TrueCrypt и 82,24 МБ / с при применении BestCrypt. Это разница 19,60%.

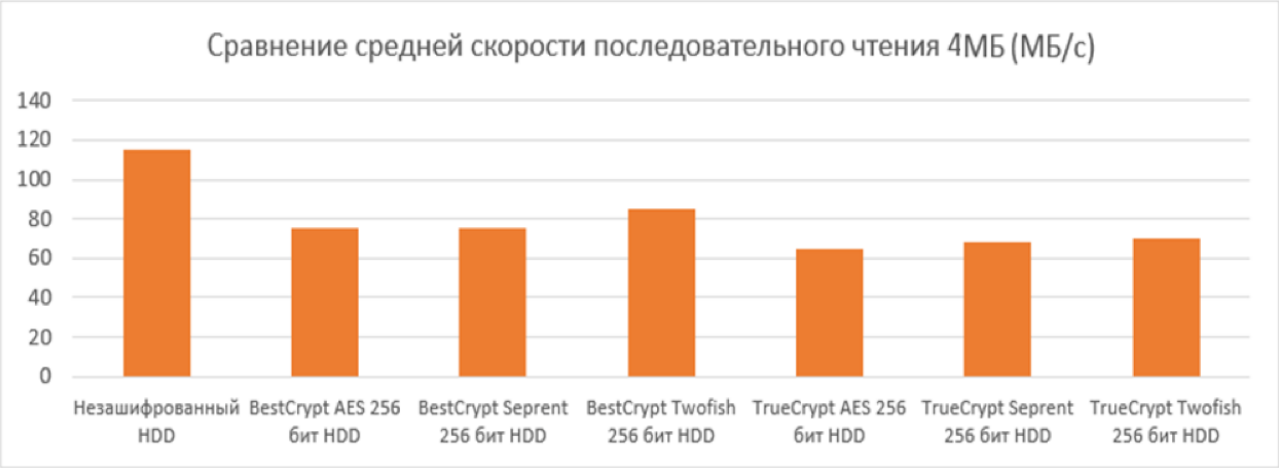

Рисунок 14 - Сравнение средней скорости последовательного чтения SSHD 4 МБ после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt

На рисунке 15 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к устройству хранения SSHD с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения шифрования работает лучше всего. После применения к устройству хранения SSHD с помощью TrueCrypt средняя скорость произвольного чтения 256-битного AES 4K составляет 0,65 Мбит / с. Для сравнения, при использовании BestCrypt средняя скорость произвольного чтения 4K AES в 256-битном формате составляет 0,68 Мбит / с. Скорость произвольного чтения AES 256-битного формата 4K на 4,61% лучше при использовании BestCrypt, чем TrueCrypt. Точно так же скорость произвольного чтения Serpent 256-бит 4K составляет 0,59 Мбит / с при применении TrueCrypt и 0,67 Мбит / с при применении BestCrypt, что означает, что на BestCrypt он работает на 13,56% лучше, чем на TrueCrypt. Наконец, скорость произвольного чтения 256-битного 4K Twofish

составляет 0,70 Мбит / с при применении TrueCrypt и 0,78 Мбит / с при применении BestCrypt. Это разница в 11,43%.

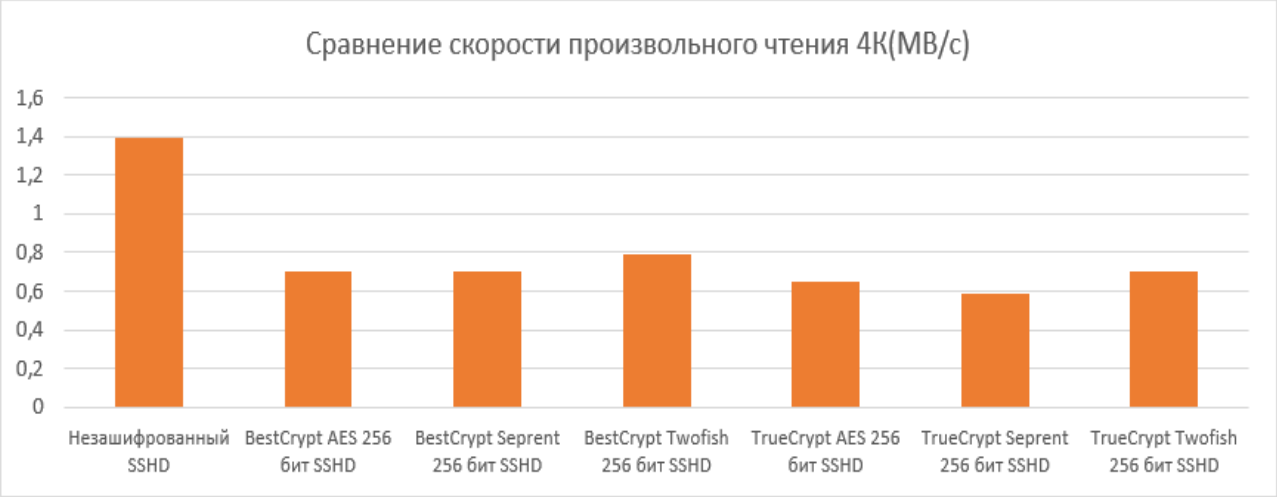

Рисунок 15 - Сравнение средней скорости произвольного чтения 4K SSHD после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt

На рисунке 16 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к устройству хранения SSHD с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения шифрования работает лучше всего. После применения к устройству хранения SSHD с помощью BestCrypt средняя скорость последовательной записи AES 256-бит 4 МБ составляет 74,61 МБ / с. Для сравнения: при использовании TrueCrypt средняя скорость последовательной записи 4 МБ AES составляет 91,97 МБ / с. Скорость последовательной записи AES 256 бит 4 МБ на 23,27% лучше при использовании TrueCrypt, чем BestCrypt. С другой стороны, скорость последовательной записи Serpent 256-бит 4 МБ составляет 62,39 МБ / с при применении TrueCrypt и 73,80 МБ / с при применении BestCrypt, что означает, что на BestCrypt он работает на 18,29% лучше, чем на TrueCrypt. Наконец, скорость последовательной записи Twofish 256-бит 4 МБ составляет 69,99 МБ / с при использовании BestCrypt и 80,20 МБ / с при применении TrueCrypt. Это

разница 14,59%.

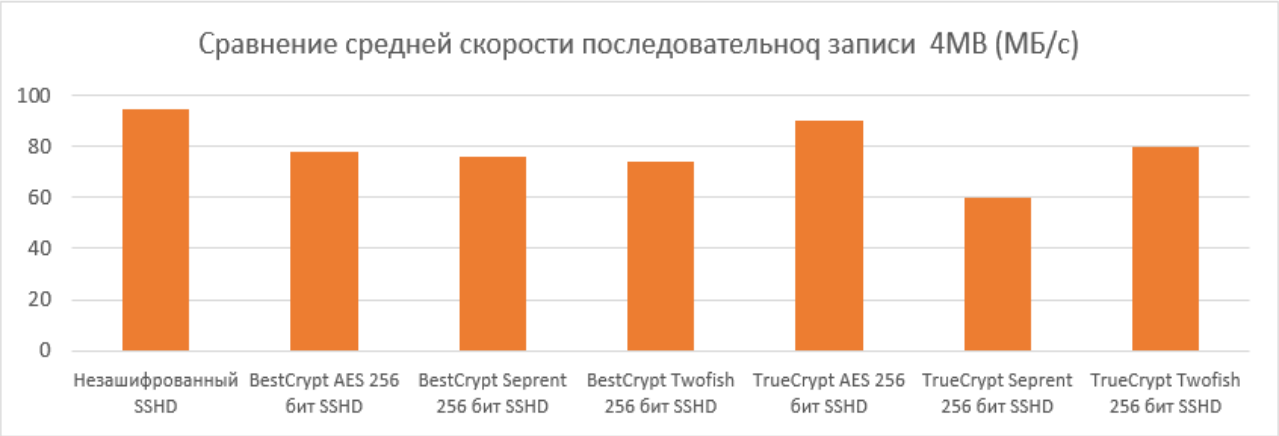

Рисунок 16 - Сравнение средней скорости последовательной записи SSHD в 4 МБ после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt

На рисунке 17 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к устройству хранения SSHD с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения шифрования работает лучше всего. После применения к устройству хранения SSHD с помощью BestCrypt средняя скорость произвольной записи 256-битного AES в формате 4K составляет 1,13 Мбит / с. Для сравнения, при использовании TrueCrypt средняя скорость произвольной записи 4K AES в 256-битном формате составляет 2,28 Мбит / с. При использовании TrueCrypt скорость произвольной записи 4K AES с 256 битами на 101,77% выше, чем BestCrypt. С другой стороны, скорость произвольной записи Serpent 256-бит 4K составляет МБ / с при применении TrueCrypt и 1,46 МБ / с при применении BestCrypt, что указывает на то, что на BestCrypt он работает на 19,67% лучше, чем на TrueCrypt. Наконец, скорость произвольной записи Twofish 256-бит 4K составляет 1,07 Мб / с при применении BestCrypt и 1,69 Мб / с при применении TrueCrypt. Это 57,94% разницы.

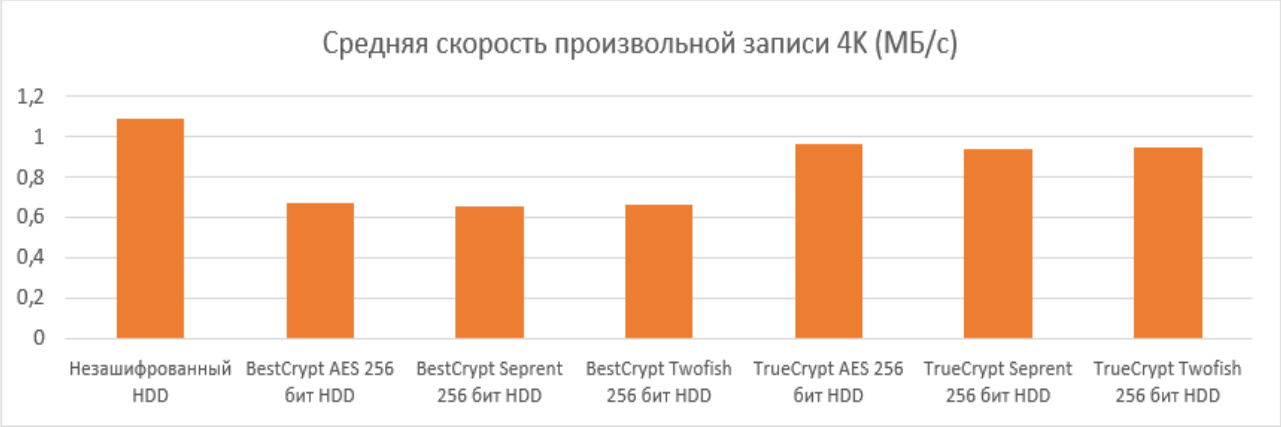

Рисунок 17 - Сравнение средней скорости случайной записи 4K SSHD после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и

На рисунке 18 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к флеш-накопителю NAND MLC на основе SSD с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения шифрования работает лучше всего. После применения к флеш-накопителю NAND MLC на основе SSD с помощью BestCrypt средняя скорость последовательного чтения AES 256 бит 4 МБ составляет 389,54 Мбит / с. Для сравнения, средняя скорость последовательного чтения 4 МБ AES 256-бит составляет 410,47 МБ / с при использовании True-Flash после применения 256-битных AES, Serpent и Twofish с использованием BestCrypt и TrueCrypt.

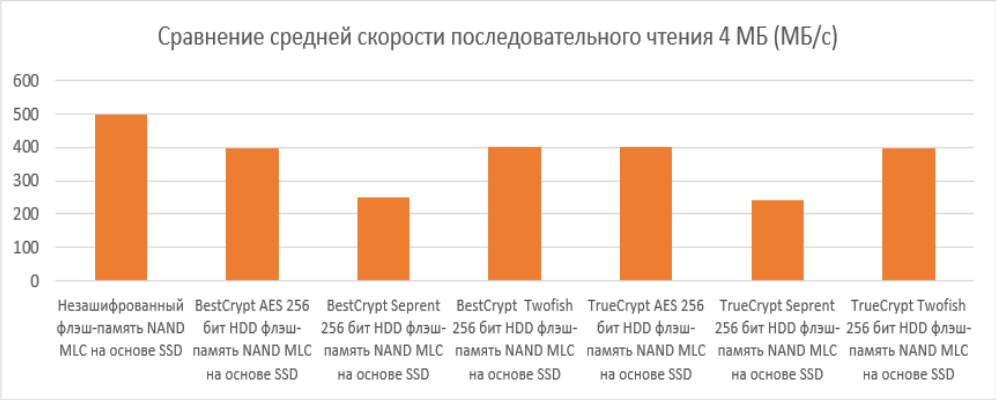

Рисунок 18 - Сравнение средней скорости последовательного чтения 4 МБ флэш-памяти NAND MLC на основе SSD после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt

Вместо этого применяется крипта. Скорость последовательного чтения бит и 4 МБ на 5,37% выше при использовании TrueCrypt, чем BestCrypt. С другой стороны, скорость последовательного чтения Serpent 256-бит 4 МБ составляет 251,00 МБ / с при применении TrueCrypt и 254,55 МБ / с при применении BestCrypt, что означает, что он работает на 1,41% лучше с BestCrypt, чем с TrueCrypt. Наконец, скорость последовательного чтения Twofish 256-бит 4 МБ составляет 385,73 МБ / с при применении TrueCrypt и 413,73 МБ / с при применении BestCrypt. Это разница 7,26%.

На рисунке 19 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к флеш-накопителю NAND MLC на основе SSD с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения шифрования работает лучше всего. После применения к запоминающему устройству NAND MLC на основе SSD с использованием TrueCrypt средняя скорость произвольного чтения 256-битного AES 4K составляет 13,11 Мбит / с. Для сравнения, при использовании BestCrypt средняя скорость произвольного чтения 4K AES в 256-битном формате составляет 18,65 Мбит / с. Скорость произвольного чтения AES 256-битного формата 4K на 42,26% лучше при использовании BestCrypt, чем TrueCrypt. Точно так же скорость произвольного чтения Serpent 256-бит 4K составляет 12,95 МБ / с при применении TrueCrypt и 16,09 МБ / с при применении BestCrypt, что означает, что на BestCrypt он работает на 24,25% лучше, чем на TrueCrypt. Наконец, скорость произвольного чтения 256-битного 4K Twofish составляет 13,01 Мбит / с при применении TrueCrypt и 17,88 Мбит / с при применении BestCrypt. Это разница 37,43%.

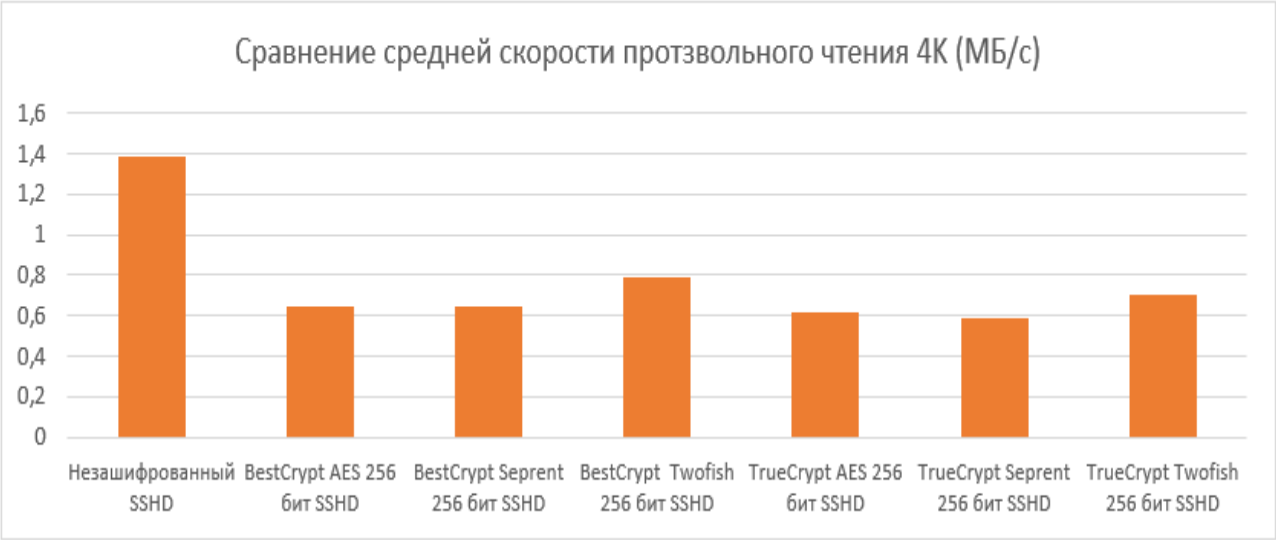

Рисунок 19 - Сравнение средней скорости случайного чтения 4K на основе SSD NAND MLC

На рисунке 20 показаны в этом эксперименте три различных алгоритма шифрования, применяемые к флеш-накопителю NAND MLC на основе SSD с использованием TrueCrypt и BestCrypt, чтобы проверить, насколько хорошо они работают, и определить, какой тип программного обеспечения для хранения шифрования работает лучше всего. После применения к флеш-накопителю NAND MLC на основе SSD с помощью BestCrypt, средняя скорость последовательной записи AES 256-бит 4 МБ составляет 360,89 МБ / с.

Для сравнения, при использовании TrueCrypt средняя скорость последовательной записи 4 МБ AES составляет 399,23 МБ / с. Скорость последовательной записи AES 256 бит 4 МБ на 53,03% лучше при использовании TrueCrypt, чем BestCrypt.

Точно так же скорость последовательной записи Serpent 256-бит 4 МБ составляет 212,64 МБ / с при применении BestCrypt и 231,77 МБ / с при применении TrueCrypt, что означает, что он работает на 9% лучше с TrueCrypt, чем с BestCrypt. Наконец, скорость последовательной записи Twofish 256-бит 4 МБ составляет 346,96 МБ / с при использовании TrueCrypt и 386,45 МБ / с при использовании BestCrypt. Это разница на 11,38%.

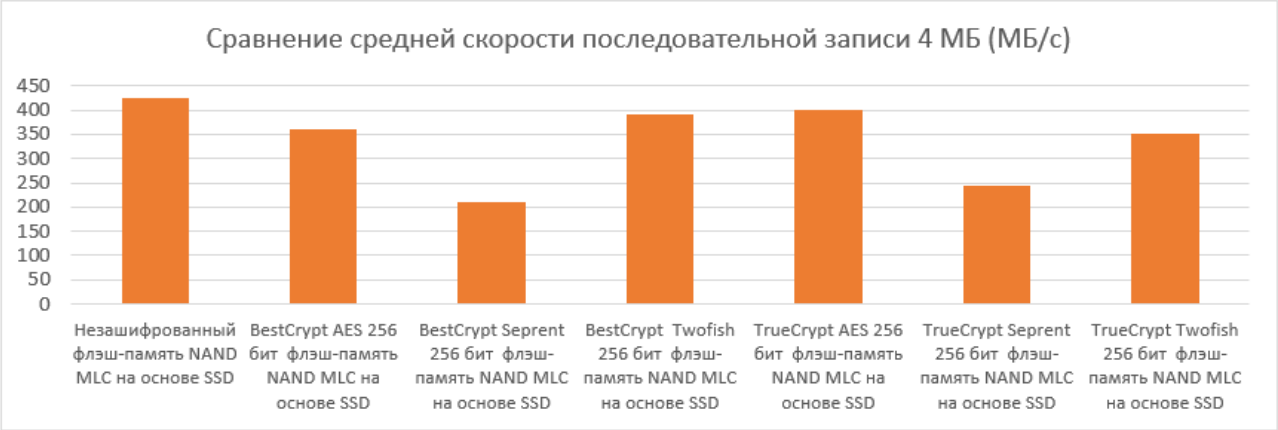

Рисунок 20 - Сравнение средней скорости последовательной записи 4 МБ флэш-памяти NAND MLC на основе SSD после применения AES, Serpent и Twofish 256 бит с использованием BestCrypt и TrueCrypt

После применения к запоминающему устройству NAND MLC на основе SSD с помощью BestCrypt средняя скорость произвольной записи 256-битного AES 4K составляет 36,20 Мб / с.

Для сравнения, при использовании TrueCrypt средняя скорость произвольной записи 4K AES в 256-битном формате составляет 36,24 Мбит / с. Скорость произвольного чтения AES 256-битного формата 4K на 0,11% лучше при использовании TrueCrypt, чем BestCrypt. С другой стороны, скорость произвольной записи 256-битного 4K Serpent составляет 26,21 МБ / с при применении TrueCrypt и 33,52 МБ / с при применении BestCrypt, что означает, что на BestCrypt он работает на 27,89% лучше, чем на TrueCrypt. Наконец, скорость произвольной записи 256-битного 4K Twofish составляет 31,11 Мб / с при применении TrueCrypt и 34,91 Мб / с при применении BestCrypt. Это разница 12,21%.

Выводы к главе 4

Для обеспечения безопасности данных в устройствах хранения в этой работе подробно изучается производительность алгоритмов симметричного шифрования на трех различных устройствах хранения с использованием BestCrypt (коммерческое программное обеспечение для шифрования данных)

и TrueCrypt (программное обеспечение для шифрования данных с открытым исходным кодом). Тремя устройствами хранения данных, рассмотренными в этой исследовательской работе, являются флэш-память HDD, SSHD и SSD на основе NAND MLC. HDD и SSHD-это формы старой технологии хранения данных, в то время как NAND MLC на основе SSD (интерфейс SATA III) - это форма текущей технологии хранения данных.

Исследование показало, что SSD-накопитель NAND MLC flash (интерфейс SATA III) имеет самый высокий уровень производительности до и после применения 256-битного ключа AES, Serpent и Twofish с использованием BestCrypt и TrueCrypt по сравнению с HDD и SSHD.

Выбор правильного алгоритма шифрования окажет значительное влияние на производительность устройства хранения данных. Тщательная оценка и выбор алгоритмов шифрования особенно важны при использовании флэш-памяти NAND на основе SSD и SSHD, поскольку производительность каждого алгоритма сильно варьируется в зависимости от того, к какому устройству он применяется. С другой стороны, производительность различных методов шифрования на жестком диске остается достаточно стабильной при различных схемах доступа к дискам.

Заключение

Одной из основных задач современной информационной технологии является обеспечение конфиденциальность, доступность и целостность персональных данных пользователей. Защита данных - это набор стратегий и процессов, которые вы можете использовать для обеспечения конфиденциальности, доступности и целостности ваших данных. Иногда это также называют безопасностью данных или конфиденциальностью информации.

Стратегия защиты данных жизненно важна для любой организации, которая собирает, обрабатывает или хранит конфиденциальные данные. Успешная стратегия может помочь предотвратить потерю, кражу или повреждение данных и может помочь минимизировать ущерб, причиненный в случае взлома или аварии. Существует много методов у которых разные стратегии для защиты данных. Каждый уникален по-своему. Одна из основных задач в данной работе заключалась в том, чтобы анализировать уникальность и эффективность стратегии которые представляют исследуемые методы защиты. В данной работе были рассмотрены самые востребованные методы и были сделаны определенные выводы.

В ходе работы была определена актуальность исследования, которая обусловлена тем, что персональные данные пользователей интернета, в связи с развитием информатизации общества, нуждаются в эффективных методах защиты. В ходе работы были рассмотрены и исследованы ряд методов и программных продуктов, которые реализованы для обеспечения конфиденциальность и защиты персональных данных. Были выявлены основные преимущества и недостатки. Были выявлены наиболее эффективные алгоритмы, которые определяют достаточные условия для конфиденциальности данных.

Стоит отметит, что в данной работе также были исследованы, анализированы и классифицированы ряд основных угроз, возникающих при работе с персональными данными в информационных системах.

Также в данной работе проведена сравнение методов и алгоритмов защиты данных. Получение результаты говорят о том, что сила и прочность алгоритма зависит от управления ключами, типа криптографии, количества ключей, количества битов, используемых в ключе. Далее в данной работе подробно изучалось производительность методов симметричного шифрования на разных устройствах, для обеспечения безопасности данных в устройствах хранения.

В результате работы были выполнены следующие задачи:

- проанализировано современное состояние проблемы исследования;
- проанализированы методы обеспечения безопасности персональных данных;
- проанализированы алгоритмы защиты персональных данных;
- подтверждена эффективность популярных алгоритмов защиты персональных данных.

Стоит отметить, что никакие методы защиты информации и никакие программные продукты не смогут гарантировать абсолютную безопасность и надежность персональных данных.

Но в тоже время можно существенно уменьшить риск потери данных, выбрав необходимый метод защиты.

Гипотеза исследования подтверждена.

Список используемой литературы и используемых источников

1. Алямкин С.Н. Персональные данные как объект правового регулирования: понятие и способы защиты // Мир науки и образования. 2016. № 4 (8). С. 4-8.

2. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность: Лабораторный практикум. М.: КноРус, 2016. 132 с.

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие. М.: Риор, 2018. 400 с.

4. Баранова Е.К., Бабаш А.В. Криптографические методы защиты информации. М.: КноРус, 2017. 220 с.

5. Бачило И. Л., Сергиенко Л. А., Кристальный Б. А., Арешев А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования. Минск: Беллітфонд, 2006. 474 с.

6. Бондаренко К.А. Взаимосвязь признаков индивидуального трудового договора и особенностей договорного регулирования трудовых отношений // Трудовое право в России и за рубежом. 2015. № 3. С. 23 - 27.

7. Буркова А.Ю. Локализация баз данных на территории Российской Федерации: первые толкования // Законодательство и экономика. 2015. № 9. С. 59 -64.

8. Головина С.Ю. Конституционные принципы и права в сфере труда и их конкретизация в трудовом законодательстве России // Российский юридический журнал. 2015. № 1.С. 132 - 145.

9. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника // Информационное право. 2017. №4. С. 35 - 38.

10. Защита конфиденциальности персональных данных с помощью обезличивания // Вестник АГГУ. 2020, №2. С. 158-162.

11. Информационная безопасность [Электронный ресурс]. URL: http://dehack.ru/ (дата обращения: 10.06.2021).

12. Лебедев В.М., Фахрутдинова Т.М., Сапфирова А.А., Агашев Д.В.

Трудовое право: Учебник. М.: Норма: НИЦ Инфра-М, 2018. 464 с.

13. Никифоров С.Н. Методы защиты информации. Пароли, скрытие, шифрование: Учебное пособие. СПб.: Лань, 2018. 124 с.

14. Никифоров С.Н. Методы защиты информации. Шифрование данных: Учебное пособие. СПб.: Лань, 2019. 160 с.

15. Партыка Т.Л., Попов И.И. Информационная безопасность: учеб. пособие. М.: ФОРУМ : ИНФРА-М, 2015. 367 с.

16. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Консультант плюс: справочно-правовая система.

17. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Консультант плюс: справочно-правовая система.

18. Терещенко Л.К. Правовой режим персональных данных и безопасность личности // Закон. 2018. №6. С. 37 -43.

19. Тимиршаяхов С.Ю., Тимиршаяхова Ю.В. Правовые проблемы защиты информации при обработке персональных данных // Правозащитная деятельность в современной России: проблемы и их решение Сборник научных трудов III Международной научно-практической конференции. 2017. С. 747–750.

20. Тогузова М.Б., Гайтова Л.Х. Ответственность за нарушение норм, обеспечивающих защиту персональных данных (в трудовых правоотношениях) // Аграрное и земельное право. 2019. № 1 (169). С. 84- 86.

21. Трофимова, И.А. Обработка и хранение персональных данных // Делопроизводство. 2015. № 3. С. 107 - 110.

22. Трудовой кодекс Российской Федерации: Федеральный закон от 30.12.2001 № 197-ФЗ (ред. от 16.12.2019) // Консультант плюс: справочно-правовая система.

23. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ (ред. от 29.07.2017) «О персональных данных» // Консультант плюс: справочно-правовая система.

24. Albrechtsen E. Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection, An intervention study. Computers & Security, 2018. PP. 432-445.

25. Baker M. Keeping a Secret. Technology Review, Academic Search Premier database.

26. Chen R. et. al. Aligning information technology and business strategy with a dynamic capabilities perspective: A longitudinal study of a taiwanese semiconductor company, International Journal of Information Management, 2017. PP. 366-378.

27. Hagen J. et. al. Implementation and effectiveness of organizational information security measures, Information Management & Computer Security, 2018. PP. 377-397.

28. Hoque S., Fairhurst M., Howells G., Deravi F. Feasibility of generating biometric encryption keys, Electronics Letters, 2005.

29. MacDermott A., Baker T., Shi Q. IoT forensics: Challenges for the IoA era, in: Proceedings of 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, PP. 1-5.

30. Phillips M. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), Human genetics, 2018. vol. 137(8). PP. 575-582.

31. Setiawati D., Hakim H., Yoga F. Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore, Indonesian Comparative Law Review. 2020.