Министерство цифрового развития, связи и массовых коммуникаций РФ Уральский технический институт связи и информатики (филиал)

ФГБОУ ВО «Сибирский государственный университет

телекоммуникаций и информатики» в г. Екатеринбурге

(УрТИСИ СибГУТИ)

Отчет

по учебной практике

по МДК.04.01«Технология выполнения работ по профессии «Оператор электронно-вычислительных и вычислительных машин»»

студента 3 курса 084 группы Фамилия Вотинов Имя, отчество Юрий Александрович Факультет Инфокоммуникаций, информатики и управления Специальность 09.02.03 «Программирование в компьютерных системах»

Екатеринбург, 2023

Отзыв руководителя

Содержание

[Введение 4](#_Toc132225802)

[1 Организация процесса обновления в информационной системе 5](#_Toc132225803)

[1.1 Регламенты обновления 5](#_Toc132225804)

[1.2 Криптография 6](#_Toc132225805)

[1.3 Классификация криптосистем 8](#_Toc132225806)

[1.4 Симметричные криптосистемы 8](#_Toc132225807)

[1.5 Ассиметричные криптосистемы 10](#_Toc132225808)

[1.6 Цифровая подпись 11](#_Toc132225809)

[Заключение 20](#_Toc132225810)

[Библиография 21](#_Toc132225811)

Введение

Целью учебной практики по МДК 04.01 «Технология выполнения работ по профессии «Оператор электронно-вычислительных и вычислительных машин»» является улучшение старых и приобретение новых практических навыков работы с документами.

В соответствии с целью были поставлены следующие задачи:

- рассмотреть теоретический материал по теме;

- отработать навыки оформления документов различной сложности в текстовом редакторе;

- создать контрольные вопросы;

- разработать тест на проверку знаний;

- оформить документы в соответствии с образцом.

# 1 Организация процесса обновления в информационной системе

# 1.1 Регламенты обновления

-развитие информационной системы под требования бизнеса только за счет собственных разработок;

- увеличение количества собственных разработок приводит только к установке нот и обновлений, устраняющих ошибки и необходимых для выполнения требований изменения законодательства. Со временем установка таких обновления становится все более трудоемкой;

- увеличение стоимости поддержки информационных систем;

- завершение поддержки производителей устаревших баз данных и операционных систем;

- снижение общего уровня безопасности системы.

Типы обновлений:

1) Частичное обновление.

Каждое частичное обновление, выданное разработчиком, должно иметь ссылку на задачу, в которой описана проблема. Обновление ставится сначала на тестовую базу.

Проверяется работоспособность функционала, по задаче, созданной на ресурсе. После установки обновления на тестовую базу, в случае соответствия функционала, описанному в задаче, обновление устанавливается на рабочую базу и ожидает проверки конечного пользователя.

Частичное обновление выкладывается в случае возникновения критической ошибки в работе функционала, а также при потребности передачи функционала до установки полного обновления.

2) Полное обновление.

В зависимости от потребности может собираться как полное квартальное обновление, так и полное промежуточное.

3) Промежуточное (содержит описание и список задач по фильтру).

В первый рабочий день обновление устанавливается на тестовую базу данных. Срок тестирования 2 дня. В случае обнаружения критических ошибок срок установке сдвигается до их исправления.

4) Квартальное.

Обновление выкладывается в отдельную задачу для установки на тестовую базу. В течение 3х дней обновление должно быть установлено на тестовую базу.

Тестовую базу перед установкой обновления следует актуализировать до состояния рабочей базы данных на текущий момент. Со дня установки релиза начинается тестирование согласно Приложению 1 к регламенту Тестирования и установки обновлений (срок тестирования 15 рабочих дней).

5) Частичное обновление.

6) Простое обновление

Процесс обновления систем заключается в последовательном выполнении следующих этапов:

- Обследование. На этом этапе определяется уровень обновлений системы, подключение дополнительных функциональных возможностей. Проводится сбор информации об объеме внедрения бизнес-процессов, операций по ним и определяется объем тестирования. Также осуществляется анализ объема, модифицированного ПО и собственных разработок.

- Подготовка плана перехода. Производится подготовка тестовой системы (копия продуктивной), ее обновление, анализ и корректировка затронутого модифицированного ПО; тестирование работы системы, регистрация и решение проблем; создание перечня мероприятий для перехода. Затем проводится повторное разворачивание тестовой системы, ее обновление, тестирование и применение плана мероприятий.

- Производится планирование сроков этапов перехода, оценка рисков и возможность дополнительных мероприятий по их снижению. В итоге определяется период неработоспособности продуктивной системы, разрабатывается и утверждается документ «План перехода»

- Выполнение плана перехода. Заключается в последовательном выполнении мероприятий, описанных в документе "План перехода".

- Поддержка пользователей. После переноса обновлений в продуктивную систему заказчика осуществляется оперативная поддержка пользователей и решение оставшихся проблем.

7) Миграция

Процесс миграции систем включает в себя следующие этапы:

* Обследование. На этом этапе определяется перечень мероприятий.

- Подготовка плана миграции. Производится применение перечня мероприятий, подготовка стенда, проверяется работоспособность системы. Затем проводится тестовая миграция, в ходе которой уточняется, обновляется перечень мероприятий, а также определяется их длительность. На основе результатов этого процесса производится планирование сроков этапов миграции, оценка рисков и возможность дополнительных мероприятий по их снижению. В итоге определяется период неработоспособности продуктивной системы, разрабатывается и утверждается документ «План перехода»

- Выполнение плана миграции. Заключается в последовательном выполнении мероприятий, описанных в документе.

- Поддержка пользователей. После миграции осуществляется оперативная поддержка пользователей и решение оставшихся проблем.

# 1.2 Криптография

Специалисты считают криптографическое закрытие информации наиболее эффективным и надёжным средством защиты информации.

Криптография — это наука о защите информации от прочтения ее посторонними.

Защита достигается шифрованием, т.е. преобразованием, которое делает защищенные данные трудно раскрываемыми (бесполезными) без знания специальной ключевой информации — ключа.

Ключ — легко изменяемая часть криптосистемы, хранящаяся в тайне и определяющая, какое шифрующее преобразование из возможных выполняется в данном случае. Криптосистема — семейство выбираемых с помощью ключа обратимых преобразований, которые преобразуют защищаемый открытый текст в шифрограмму и обратно.

Методы шифрования должны обладать минимум двумя свойствами:

• законный получатель имеет возможность выполнить обратное преобразование и расшифровать сообщение;

• криптоаналитик, перехвативший сообщение, не сможет восстановить по нему исходное сообщение без таких затрат времени и средств, которые сделают эту работу нецелесообразной.

Осуществляться шифрование может либо вручную (что представляет сложную и кропотливую процедуру), либо автоматически, с помощью специальных аппаратных средств (шифраторов) или специального программного обеспечения.

Основные виды шифров:

• шифры перестановок (символы шифруемого текста переставляются по определенному правилу);

• шифры замены (символы шифруемого текста заменяются символами того же или другого алфавита по определенной схеме);

• шифры гаммирования (символы шифруемого текста складываются с символами некоторой случайной последовательности, называемой гаммой);

• шифры, основанные на аналитических преобразованиях (шифруемый текст преобразуется по некоторому аналитическому правилу – формуле).

Широкое распространение получили комбинированные шифры, когда исходный текст последовательно преобразуется с использованием двух или даже трех различных шифров. Например, комбинированное применение замены и гаммирования или перестановки и гаммирования и т.п.

В качестве примера рассмотрим шифр Цезаря, который является частным случаем шифра замены. Римский император Гай Юлий Цезарь использовал этот шифр около 50 года до н.э. При шифровании каждая буква исходного текста заменялась путем смещения по алфавиту на 3 буквы от исходной. Так, известное послание Цезаря Аминтию «VENI VIDI VICI» («Пришел, увидел, победил») в зашифрованном виде выглядело бы «YHQL YLGL YLFL».

Этот, казалось бы, несложный шифр является основой единственного абсолютно надежного шифра (т.е. шифра, который нельзя вскрыть при использовании неограниченных вычислительных возможностей) — одноразовой системы шифрования. Каждый i-тый символ исходного текста заменяется путем смещения по алфавиту на Ki буквы (где Ki – i-тый элемент ключевой последовательности). Для реализации этой системы применяют иногда одноразовый блокнот, на каждой странице которого напечатана таблица со случайными числами Ki. Один экземпляр блокнота находится у отправителя, другой – у получателя. Для каждого i-го символа шифруемого текста используют свой ключ Ki только один раз. После шифровки сообщения страница удаляется из блокнота и уничтожается, каждое новое сообщение шифруется с новой страницы. Применение системы ограничено, в основном, необходимостью передачи получателю по секретному каналу случайной ключевой последовательности с длиной, не меньшей длины сообщения. Такое требование практически неосуществимо для современных систем обработки информации, в которых требуется шифровать многие миллионы символов.

# 1.3 Классификация криптосистем

По характеру шифрования известные криптосистемы можно разделить на два типа:

• симметричные (одно-ключевые, с секретным ключом) — это криптосистемы, использующие одинаковые секретные ключи в блоке шифрования и в блоке расшифровывания;

• асимметричные (двух ключевые, с открытым ключом) — это криптосистемы, использующие в блоках шифрования и расшифровывания два разных ключа, один из которых является открытым, а другой – секретным.

В первом случае в шифраторе отправителя и дешифраторе получателя используется один и тот же ключ, который хранится в тайне и передается отправителем сообщения получателя по каналу, исключающему перехват. В асимметричной системе блок секретный ключ сохраняют на месте его генерации, а открытый – передают по незащищенному каналу.

Потребность в сертификации криптографических алгоритмов, а также функциональной совместимости при работе различных пользователей привела к созданию стандартов шифрования.

# 1.4 Симметричные криптосистемы

Одним из примеров симметричных криптосистем может служить принятый в 1977 году национальным бюро стандартов США стандарт шифрования данных DES. Стандарт DES предназначен для защиты важной, но несекретной информации; в настоящее время является наиболее распространенным алгоритмом шифрования.

Основные достоинства алгоритма DES:

• используется только один ключ длиной 56 бит;

• зашифрованное DES сообщение можно расшифровать с помощью любого программного обеспечения, соответствующего стандарту DES;

• высокая скорость обработки (шифрования и дешифрования);

• достаточно высокая стойкость алгоритма;

• различные варианты исполнения DES (программный, микропрограммный и аппаратный) позволяют удов­летворять потребности разнообразных пользователей как по скоростным, так и экономическим показателям.

Недостатком DES является невысокая длина ключа и необходимость защищенного канала для передачи ключей. Несмотря на интенсивные и тщательные исследования алгоритма, не найдено уязвимых мест алгоритма, на основе которых можно было бы предложить метод криптоанализа, существенно лучший, чем полный перебор ключей. Ключ DES имеет длину 56 бит, поэтому существует 256 возможных вариантов такого ключа. Если предположить, что компьютер может испытать 1000 000 вариантов ключа в секунду, то требуется до 2285 лет для подбора ключа. Однако 19 января 1999 года зашифрованное с помощью DES сообщение было взломано за рекордно короткое время – 22 часа 15 минут. Правда, для этого понадобилась работа 100 000 энтузиастов, скорость перебора составила 245 млрд. ключей в секунду.

DES используется при хранении и передаче данных между различными вычислитель­ными системами, в почтовых системах, в электронных системах платежей и при электронном обмене ком­мерческой информацией. Ежедневно банки переводят свыше сотни миллиардов долларов с использованием алгоритма DES.

Гост 28147-89 - отечественный стандарт шифрования

В нашей стране установлен единый алгоритм криптографического преобразования данных для систем обработки информации в сетях ЭВМ, отделительных комплексах и ЭВМ, который определяется ГОСТ 28147-89. Стандарт обязателен для предприятий, организаций и учреждений, применяющих криптографическую защиту данных, хранимых и передаваемых в сетях ЭВМ, отдельных вычислительных комплексах и ЭВМ.

Алгоритм криптографического преобразования данных предназначен для аппаратной или программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации. Алгоритм криптографического преобразования предусматривает несколько режимов работы. Для шифрования данных используется ключ, который имеет размерность 256 бит (против 56 бит ключа DES). Расшифрование выполняется по тому же ключу, что и шифрование, т.е. алгоритм является симметричным.

Алгоритм ГОСТ 28147-89 предусматривает наличие у абонентов закрытых ключей и соответственно – налаженную систему генерации ключей, выпуска и распределения ключевой документации.

При использовании симметричных алгоритмов шифрования отправитель и полу­чатель информации вынуждены безоговорочно доверять друг другу, т.к. располагают одинаковыми возмож­ностями выполнять действия, связанные с обменом информации. В таких условиях каждый пользователь априори может считаться не заслужива­ющим доверия. Злоумышленником может быть как один из участников обмена, так и незаконный пользователь, имеющий доступ к линии связи.

Главное препятствие шифрованию составляет защищенный обмен ключами или управление ключами шифрования. Одним из решений этой проблемы стали системы с открытыми ключами (например, типа RSA). Эти системы позволяют наиболее просто реализовать цифровую подпись и имитозащиту (т.е. защиту от преднамеренного искажения) информации, передаваемой по линиям связи.

# 1.5 Ассиметричные криптосистемы

Концепция асимметричных криптосистем основана на применении однонаправленных функций. Пусть X и Y – некоторые произвольные множества. Функция является однонаправленной, если для всех x можно легко вычислить функцию y = f(x), и в тоже время для большинства y достаточно сложно получить значение x, такое, что f(x) = y (при этом полагают, что существует по крайней мере одно такое значение).

На практике находят применение односторонние функции с лазейкой, т.е. функции, для которых легко найти обратное значение при знании лазейки – дополнительной информации, например ключа секретного ключа дешифрования Dk. Примером таких функций, близких по свойствам к односторонним, является дискретное возведение в степень (обратная функция – отыскание дискретного логарифма), перемно­жение простых чисел (обратная функция — разложение на простые множители) и ряд других.

В качестве примера рассмотрим целочисленное умножение. Прямая задача – вычисление произведения двух очень больших чисел P и Q, т.е. нахождение значения N = P \* Q, является несложной задачей для ЭВМ. Обратная задача – разложение на множители большого целого числа, т.е. нахождение сомножителей (делителей) P и Q большого целого числа N, является практически неразрешимой задачей при достаточно больших значениях N. По современным оценкам теории чисел, при целом значении задача нахождения сомножителей (делителей) P и Q практически неразрешима на современных ЭВМ.

Недостатком асимметричных алгоритмов является низкая скорость обработки (шифрования и дешифрования) по сравнению с симметричными.

Первым полноценным асимметричным алгоритмом является алгоритм RSA, предложенный в 1978 году Р.Райвестом, А.Шамиром и А.Адлерманом. Надежность RSA основана на трудности факторизации больших чисел и вычисления дискретных логарифмов. RSA может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи.

# 1.6 Цифровая подпись

Цифровая подпись сообщения — это процесс, обеспечивающий определение подлинности (аутентификацию) сообщения и юридическую ответственность лица, подписавшего сообщение (аутентификацию источника данных). Физически цифровая подпись представляет собой блок данных, добавляемый к сообщению и формируемый при помощи асимметричного криптографического алгоритма.

Аутентификация (проверка подлинности) — проверка идентификации пользователя, устройства или другого компонента в информационной системы (ИС).

Асимметричные криптосистемы используются для формирования цифровой подписи и шифрования (формирования) симметричных ключей при их рассылке по каналам связи. Среди методов цифровой подписи наибольшее применение нашли RSA-подобные алгоритмы и алгоритмы на основе метода Эль-Гамаля (разработан в 1985 году, основан на вычислении дискретных логарифмов в конечном поле), стандартизованные в ряде стран.

Отечественный стандарт цифровой подписи обозначается как ГОСТ Р 34.10-94. Алгоритм цифровой подписи, определенный этим стандартом, является развитием метода цифровой подписи Эль-Гамаля. Следует отметить, что в отечественном стандарте сомножитель имеет длину 256 бит (в западных стандартах - примерно 160 бит), что отражает стремление к получению более безопасной подписи.

Рассмотрим механизм использования асимметричной криптосистемы и цифровой подписи.

Шифрование сообщений. Пусть имеется владелец ключевой пары Ek, Dk и некоторый пользователь, которому известен открытый ключ Ek. Пользователь может зашифровать на ключе Ek свое сообщение и отправить его владельцу. Никто кроме владельца, знающего секретный ключ Dk, не может дешифровать сообщение, т.е. обеспечивается конфиденциальность передачи.

Цифровая подпись сообщения. Владелец может преобразовать на ключе Dk свое сообщение и отправить его пользователю. Любой пользователь, которому известен открытый ключ Ek, может выполнить обратное преобразование на открытом ключе. В дан­ном случае конфиденциальность сообщения не обеспечивается. Однако пользователь может быть уверен, что сообщение поступило именно от владельца, поскольку кроме него никто не знает секретного ключа Dk, на котором было выполнено преобразование сообщения.

Контрольные вопросы:

Перечислите типы обновлений информационной системы.

Что такое криптосистема?

На какие типы делятся криптосистемы по характеру шифрования?

Перечислите недостатки асимметричных алгоритмов.

Что такое цифровая подпись и зачем она нужна?

Тестовая проверка знаний:

Что такое криптография?

- это наука о защите информации от прочтения ее посторонними; +

- это парадигма программирования, в которой выполнение программы определяется событиями — действиями пользователя;

- это процесс, обеспечивающий определение подлинности сообщения и юридическую ответственность лица, подписавшего сообщение;

- это какой-либо объект, осуществляющий работу системы.

Выберите правильные виды шифров.

- шифры перестановок и шифры замены; +

- шифры множителя;

- шифры гаммирования; +

- шифры, основанные на аналитических преобразованиях. +

На какие типы делятся криптосистемы по характеру шифрования?

- внутренний, внешний;

- симметричный, асимметричный; +

- сложный, простой;

- теоретический, исследовательский.

Какой длины ключ в алгоритме DES?

- 102 бита;

- 13 байт;

- 56 бит; +

- 1 мегабайт.

Как называется стандарт, который устанавливает единый алгоритм криптографического преобразования данных для систем обработки информации?

- Гост 102-3;

- Гост 1332 Р 134;

- Гост 28147-89; +

- Гост 101-2134-2.

В каком году был предложен асимметричный алгоритм RSA?

- 1978; +

- 2002;

- 1999;

- 1968.

Что такое аутентификация?

- актив, который используется или потребляется в ходе выполнения процесса;

- представляет собой блок данных, добавляемый к сообщению и формируемый при помощи асимметричного криптографического алгоритма;

- криптосистемы, использующие одинаковые секретные ключи в блоке шифрования и в блоке расшифровывания;

- проверка идентификации пользователя, устройства или дру­гого компонента в информационной системе. +

Какие существуют типы обновлений?

- частичное, полное; +

- промежуточное, квартальное; +

- широкое, внешнее;

- промежуточное, внешнее.

Сколько этапов включает в себя процесс миграции систем?

- 2;

- 3;

- 4; +

- 5.

Что происходит на этапе обследования?

- определяется уровень обновлений системы, подключение дополнительных функциональных возможностей; +

- производится подготовка тестовой системы (копия продуктивной), ее обновление, анализ и корректировка затронутого модифицированного программного обеспечения;

- производится планирование сроков этапов перехода, оценка рисков и возможность дополнительных мероприятий по их снижению;

- после переноса обновлений в продуктивную систему заказчика осуществляется оперативная поддержка пользователей и решение оставшихся проблем.

Слайды презентации:

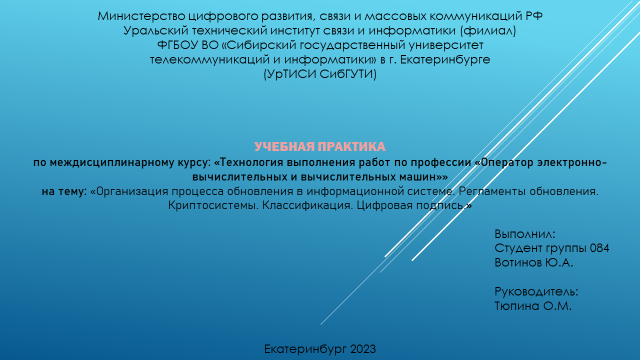


Рисунок 3 – Слайд 1

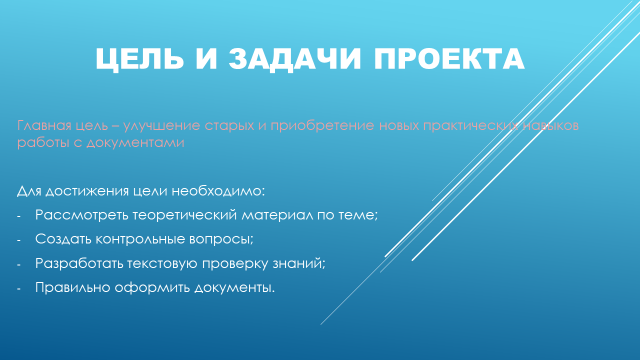


Рисунок 4 – Слайд 2

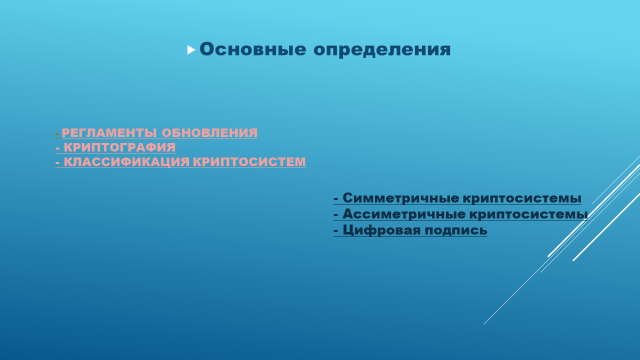


Рисунок 5 – Слайд 3

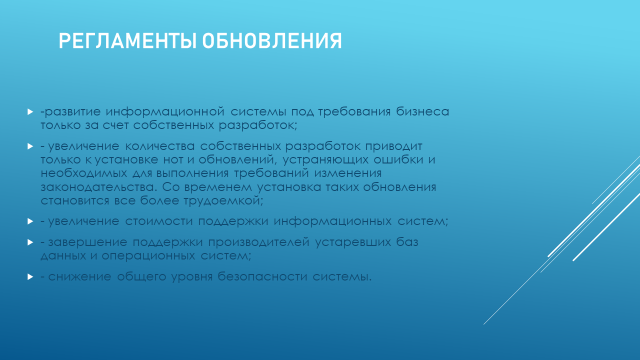


Рисунок 6 – Слайд 4

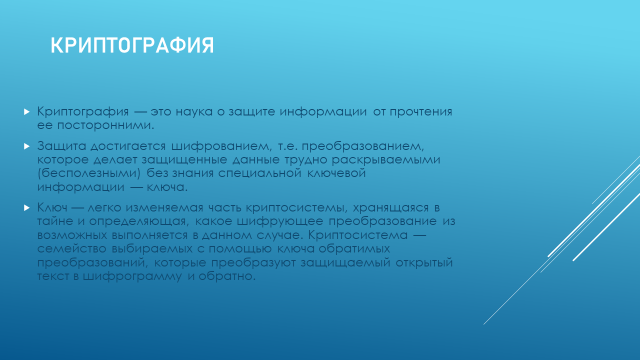


Рисунок 7 – Слайд 5

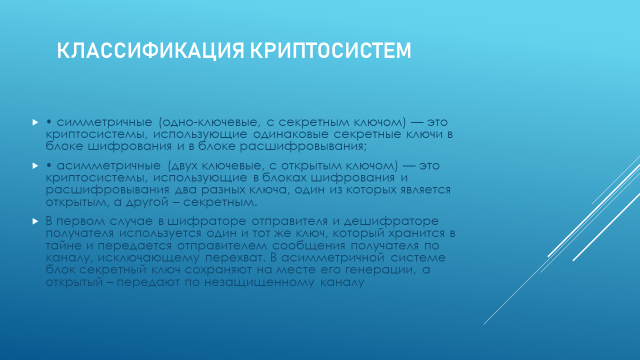


Рисунок 8 – Слайд 6

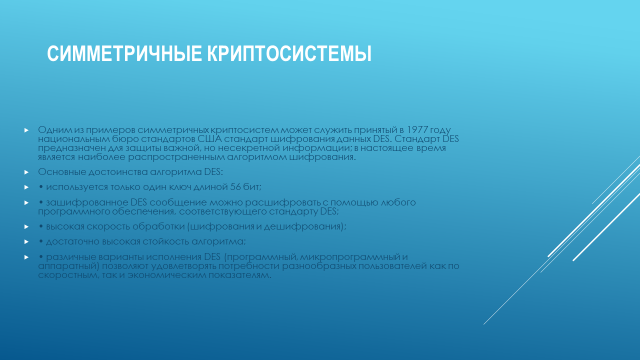


Рисунок 9 – Слайд 7

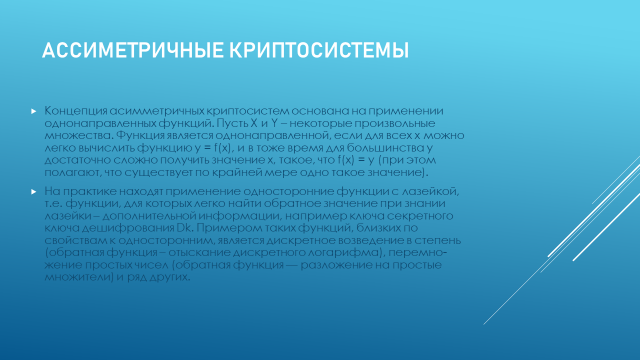


Рисунок 10 – Слайд 8

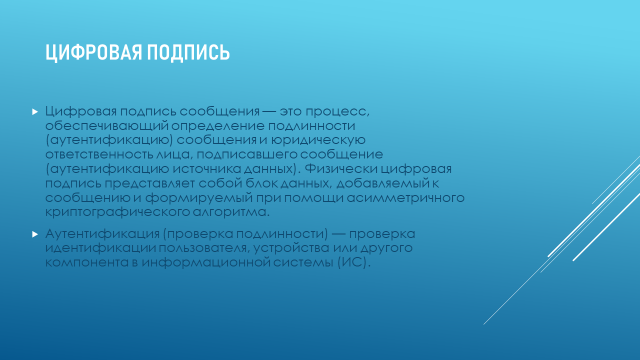


Рисунок 11 – Слайд 9



Рисунок 12 – Слайд 10

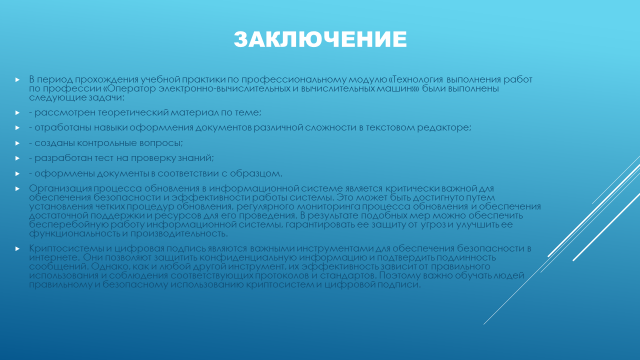


Рисунок 13 – Слайд 11

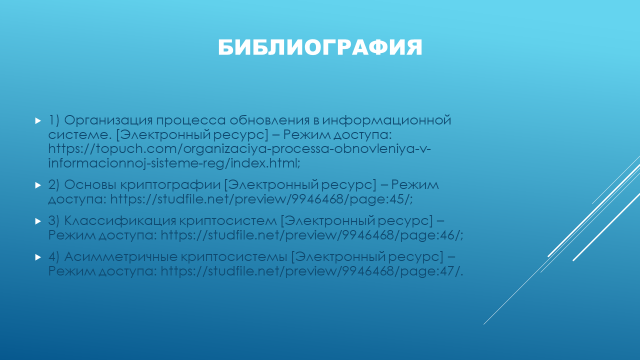


Рисунок 14 – Слайд 12

# Заключение

В период прохождения учебной практики по профессиональному модулю «Технология выполнения работ по профессии «Оператор электронно-вычислительных и вычислительных машин»» были выполнены следующие задачи:

- рассмотрен теоретический материал по теме;

- отработаны навыки оформления документов различной сложности в текстовом редакторе;

- созданы контрольные вопросы;

- разработан тест на проверку знаний;

- оформлены документы в соответствии с образцом.

Организация процесса обновления в информационной системе является критически важной для обеспечения безопасности и эффективности работы системы. Это может быть достигнуто путем установления четких процедур обновления, регулярного мониторинга процесса обновления и обеспечения достаточной поддержки и ресурсов для его проведения. В результате подобных мер можно обеспечить бесперебойную работу информационной системы, гарантировать ее защиту от угроз и улучшить ее функциональность и производительность.

Криптосистемы и цифровая подпись являются важными инструментами для обеспечения безопасности в интернете. Они позволяют защитить конфиденциальную информацию и подтвердить подлинность сообщений. Однако, как и любой другой инструмент, их эффективность зависит от правильного использования и соблюдения соответствующих протоколов и стандартов. Поэтому важно обучать людей правильному и безопасному использованию криптосистем и цифровой подписи.

# Библиография

1. Организация процесса обновления в информационной системе. [Электронный ресурс] – Режим доступа: https://topuch.com/organizaciya-processa-obnovleniya-v-informacionnoj-sisteme-reg/index.html;
2. Основы криптографии [Электронный ресурс] – Режим доступа: https://studfile.net/preview/9946468/page:45/;
3. Классификация криптосистем [Электронный ресурс] – Режим доступа: https://studfile.net/preview/9946468/page:46/;
4. Асимметричные криптосистемы [Электронный ресурс] – Режим доступа: https://studfile.net/preview/9946468/page:47/.