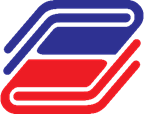
**Министерство образования и науки Российской Федерации**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ УПРАВЛЕНИЯ»**



|  |  |
| --- | --- |
| Институт | Институт информационных систем |
| Кафедра | Информационных систем |

**Методические указания по выполнению практической (контрольной работы)**

|  |  |  |  |
| --- | --- | --- | --- |
| по дисциплине | Информационная безопасность | | |
|  |  | | |
| Направление подготовки | 38.03.05 |  | Бизнес-информатика | |
| (код) |  | (наименование) | |
| Образовательная программа | «Бизнес-информатика» | | |
| (название образовательной программы) | | |
|  | | |

Форма обучения – заочная

Москва, 2023

|  |  |  |
| --- | --- | --- |
| **№**  **ПЗ** | **Наименование практических работ** | **Количество часов** |
| **1** | Построение системы информационной безопасности организации. Этап I. | 2 |
| **2** | Построение системы информационной безопасности организации. Этап II. | 2 |
| **3** | Механизмы контроля целостности данных (ЭЦП) | 2 |
| **4** | Построение системы информационной безопасности организации. Этап III. | 2 |
| **5\*** | Практическая работа «Механизмы контроля целостности данных» | - |
| ***ИТОГО:*** | | 8 |

# 5\* - работа является выполняемой по желанию. В качестве дополнительной.

# В рамках учебной дисциплины «Информационная безопасность» при проведении практических занятий, в частности, при выполнении групповой работы на тему «Построение системы информационной безопасности организации», обучающиеся получают навыки командной работы, межличностных коммуникаций, принятия коллегиальных решений, выработке лидерских качеств.

# Обучающимся необходимо разделиться по группам (командам) для выполнения задания. Деление по командам производится как произвольно, так и может распределить преподаватель, если обучающиеся не пришли к какому-то соглашению. Команды должны быть не более 5-ти человек, по желанию, могут выполнять задания индивидуально. Выполнение работы предполагает последовательное выполнение ряда шагов, взаимоувязанных между собой единой, конечной целью выполнения. Студенты распределяют выполнение отдельных частей работы между собой и выполняя их безусловно должны общаться и делится результатами выполнения, поддерживая и стимулируя друг друга на качественный и быстрый результат. Как показывает практика выполнения, в группе выделяется лидер, идейный вдохновитель и руководитель, контролирующий весь ход работы и достижения ее цели. Качественное и выполненное в срок задание является допуском к зачету. По результатам работы команды готовят презентацию и защищают результаты работы перед остальной частью студенческой аудитории (группы). Ход выполнения работы описан в разделе 7.6. данной программы.

В том числе, в рамках данного курса обучающимся предлагается написать эссе на темы: «Аспекты информационной безопасности. Политика информационной безопасности» и «Методологии оценки рисков и угроз информационной безопасности» для очной формы обучения, а также на следующие темы : «Законодательное и нормативное обеспечение информационной безопасности. Стандарты информационной безопасности», «Методологии оценки рисков и угроз информационной безопасности», «Аспекты информационной безопасности», « Политика информационной безопасности», «Методы и средства защиты информации», «Реализация стратегии обеспечения безопасности информационных систем»

для заочной формы обучения.

***Эссе*** представляет собой творческое мини-сочинение по конкретной проблеме. Обучающиеся должны кратко изложить свой взгляд на проблему и обосновать его, обратившись к соответствующим  терминам и понятиям, теоретическим положениям и выводам, а также к фактам, почерпнутым из социального или личного опыта. В эссе как и в реферате, нет содержания (плана), но по тексту должно быть обязательно введение, непосредственно дан анализ проблемы, заключение и список литературы. *Введение* является обязательной составной частью эссе и отражает прагматическую ценность изучения данной учебной дисциплины (модуля) в целом, а также актуальность выбранной темы. *Аналитическая* *часть* – должна раскрывать суть выбранной темы. При выполнении работы необходимо привести практические примеры по рассматриваемой проблеме, а также, сделать выводы. Выводы – есть *заключение*.

Результатами написания студент может поделиться на коллоквиуме, проводимом на вышеуказанную тему. Возможно подготовить доклад по эссе с использованием программного продукта Power Point).

**Практическая работа** **«Механизмы контроля целостности данных»**

1. **Цель работы**

Изучить порядок вычисления и проверки ЭЦП (электронной цифровой подписи)

1. **Теоретические сведения**

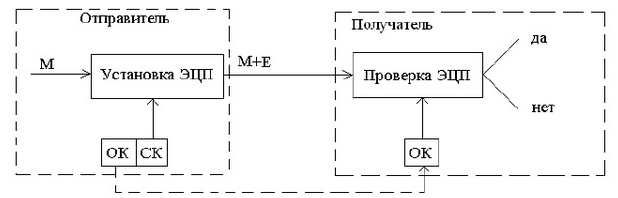
В настоящее время повсеместное внедрение информационных технологий отразилось и на технологии документооборота внутри организаций и между ними, между отдельными пользователями. Все большее значение в данной сфере приобретает электронный документооборот, позволяющий отказаться от бумажных носителей (или снизить их долю в общем потоке) и осуществлять обмен документами между субъектами в электронном виде. Однако переход от бумажного документооборота к электронному ставит ряд проблем, связанных с обеспечением целостности (подлинности) передаваемого документа и аутентификации подлинности его автора.

Следует отметить, что известные в теории информации методы защиты сообщений, передаваемых по каналам связи, от случайных помех не работают в том случае, когда злоумышленник преднамеренно реализует угрозу нарушения целостности информации. Например, контрольные суммы, используемые для этой цели передатчиком и приемником, могут быть пересчитаны злоумышленником так, что приемником изменение сообщения не будет обнаружено. Для обеспечения целостности электронных документов и установления подлинности авторства необходимо использовать иные методы, отличные от контрольных сумм. Для решения данных задач используют технологию электронно-цифровой подписи.

Электронно-цифровая подпись (ЭЦП) сообщения является уникальной последовательностью, связываемой с сообщением, подлежащей проверке на принимающей стороне с целью обеспечения целостности передаваемого сообщения и подтверждения его авторства.

Процедура установки ЭЦП использует секретный ключ отправителя сообщения, а процедура проверки ЭЦП – открытый ключ отправителя сообщения (рис. 1). Здесь

M – электронный документ, E – электронно-цифровая подпись.

Рис. 1 – Схема использования ЭЦП

В технологии ЭЦП ведущее значение имеют однонаправленные функции хэширования. Использование функций хэширования позволяет формировать криптографически стойкие контрольные суммы передаваемых сообщений.

Функцией хэширования H называют функцию, сжимающую сообщение произвольной длины M, в значение фиксированной длины H(M) (несколько десятков или сотен бит), и обладающую свойствами необратимости, рассеивания и чувствительности к изменениям. Значение H(M) обычно называют дайджестом сообщения M.

**Схема установки ЭЦП (рис. 2):**

1. Для документа М формируется дайджест H с помощью заданного алгоритма хэширования.

2. Сформированный дайджест H шифруют на секретном ключе отправителя сообщения. Полученная в результате шифрования последовательность и есть ЭЦП.

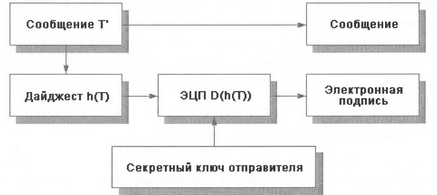
3. Сообщение М и его ЭЦП передаются получателю сообщения.

Рис. 2 – Схема установки ЭЦП.

**Схема проверки ЭЦП (рис. 3):**

1. Получатель для проверки ЭЦП должен иметь доступ к самому сообщению М и его ЭЦП.

2. Зная алгоритм хэширования, который был использован при установке ЭЦП, получатель получает дайджест H1 присланного сообщения М.

3. Зная открытый ключ отправителя, получатель дешифрует ЭЦП, в результате чего получает дайджест H2, сформированный на этапе установки ЭЦП.

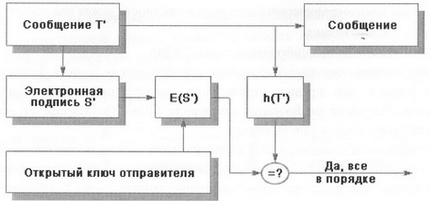
4. Критерием целостности присланного сообщения М и подтверждения его автора является совпадение дайджестов H1 и H2. Если это равенство не выполнено, то принимается решение о некорректности ЭЦП.

Рис. 3 – Схема проверки ЭЦП.

1. **Задание**

Сформировать ЭЦП к сообщению M' (см. вариант) и произвести проверку целостности принятого сообщения.

**Порядок выполнения работы:**

1. Разделить лист на две части: слева – сторона отправителя сообщения, справа – получателя.
2. На стороне отправителя выполнить следующие действия:
   1. Записать сообщение M (см. вариант).
   2. Сформировать профиль сообщения M’ с помощью упрощенной функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения.
   3. Создать ЭЦП шифрованием профиля сообщения h(M’) закрытым ключом отправителя Da (значение ключа (d, n) см. в таблице с вариантами задания), т.е. Da (h(M’)) (см. вариант).
3. На стороне получателя выполнить следующие действия:
   1. Записать сообщение М (его получает получатель вместе с ЭЦП) и ЭЦП Da (h(M’)).
   2. Сформировать профиль принятого сообщения, M’ с помощью той же функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения (Получателю известен алгоритм хэширования, применяемый на стороне отправителя).
   3. Создать профиль дешифрованием ЭЦП открытым ключем отправителя (Ea (Da (h(M’)) = h(M’)) (значение ключа (е, n) см. в таблице с вариантами задания).
   4. Сравнить два профиля сообщения h(M’) (п.3.2 и 3.3). Убедиться в их совпадении.
4. **Содержание отчета**
5. Титульный лист
6. Содержание
7. Задание
8. Лист расчета и проверки ЭЦП
9. Выводы
10. **Варианты**

**Вариант – номер по списку в журнале.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Номер варианта | p | q | е | d | М |
| 1 | 3 | 11 | 7 | 3 | 5523 |
| 3 | 17 | 11 | 7 | 23 | 8866 |
| 3 | 13 | 7 | 5 | 29 | 3565 |
| 4 | 101 | 113 | 3533 | 6597 | 6546 |
| 5 | 3 | 11 | 7 | 3 | 8562 |
| 6 | 17 | 11 | 7 | 23 | 9795 |
| 7 | 13 | 7 | 5 | 29 | 8462 |
| 8 | 17 | 11 | 7 | 23 | 7785 |
| 9 | 13 | 7 | 5 | 29 | 2123 |
| 10 | 101 | 113 | 3533 | 6597 | 3145 |
| 11 | 7 | 11 | 37 | 13 | 2566 |
| 12 | 101 | 113 | 3533 | 6597 | 3782 |
| 13 | 3 | 11 | 7 | 3 | 3465 |
| 14 | 17 | 11 | 7 | 23 | 3895 |
| 15 | 13 | 7 | 5 | 29 | 4132 |
| 16 | 17 | 11 | 7 | 23 | 5123 |
| 17 | 13 | 7 | 5 | 29 | 4416 |
| 18 | 101 | 113 | 3533 | 6597 | 7895 |
| 19 | 3 | 11 | 7 | 3 | 7459 |
| 20 | 17 | 11 | 7 | 23 | 5654 |
| 21 | 13 | 7 | 5 | 29 | 2456 |
| 22 | 17 | 11 | 7 | 23 | 3585 |
| 23 | 13 | 7 | 5 | 29 | 2652 |
| 24 | 101 | 113 | 3533 | 6597 | 5656 |
| 25 | 3 | 11 | 7 | 3 | 6685 |
| 26 | 17 | 11 | 7 | 23 | 5566 |
| 27 | 13 | 7 | 5 | 29 | 4652 |
| 28 | 17 | 11 | 7 | 23 | 8666 |
| 29 | 13 | 7 | 5 | 29 | 4556 |
| 30 | 101 | 113 | 3533 | 6597 | 9266 |

**Практическая работа** **«Построение СИБ организации»**

**III этапа**

Для выполнения работы студенты используют ранее предоставленным им теоретическим материалом.

***Этапы выполнения работы:***

* 1. Описание объекта защиты и анализ информационной инфраструктуры организации;
* 2. Анализ рисков и угроз, источников их возникновения . Выбор методологии оценки рисков и оценка рисков
* 3. Выбор методов и средств обеспечения безопасности данного объекта (рекомендации)
* Этапы ее выполнения должны быть оформлены документально и содержать КАК МИНИМУМ:
* 1. Описание  объекта защиты и анализ информационной структуры предприятия
* 2.Перечень сведений конфиденциальных документов (информации) организации.
* 3. Частные модели информационного контакта с указанием вероятности их установления.
* 4. Таблицу соответствия, содержащую описание облика нарушителя (внешнего и внутреннего, разнесенного по категориям пользователей системы) и степень риска для данного элемента системы. Она выглядит так:
* Категория пользователей Состав элементов системы, которым они угрожают Степень риска\*
* \*- оценивается  как «маловероятно», «вероятно», «весьма вероятно».
* 4. Перечень угроз с их классификацией (текстовое описание +таблица с ранжированием по степени вероятности реализации)
* 5.Оценку ущерба  (текстовое описание+таблица с величиной предполагаемого ущерба)
* 6.Оценку риска (таблица)
* 7. Перечень выбранных мер и мероприятий, сервисов, программ и т.д.
* 8. Расчет эффективности применения

ЭТАП 1. Аудит ИБ объекта. Изучение инфраструктуры и информационных потоков .Определение и анализ внешних и внутренних факторов, влияющих функционирование выбранных элементов".

* Подготовительный этап к анализу рисков. Описание  объекта защиты и анализ информационной структуры предприятия
* На этом этапе уточняется информационная структура организации и определяется степень детальности ее рассмотрения. Работа выполняется на концептуальном уровне и включает следующие моменты:
* - описание объекта защиты, выбор анализируемых объектов и идентификация активов;
* - четкое определение и обоснование цели защиты, в категориях целостности, доступности, конфиденциальности
* - определение периметра безопасности, т.е. обеспечение области безопасности системы (невозможно  безопасность обеспечить повсеместно).
* Для выполнения этой работы надо познакомиться с основными направлениями деятельности компании, учитывать специфику конкретных информационных систем, определить какие данные имеют отношение к этой деятельности, какая часть  данных наиболее важная , составить модель предметной области. Проанализировать процесс управления информацией, содержание данных, выделить категории пользователей.
* Необходимо структурировать информацию на группы по пользователям, процессам, информационным объектам и потокам, по уровню управления.
* Необходимо учитывать ценность информации. Классифицировать данные по типам и степени конфиденциальности, степени доступа к ним. Все это важно для оценки последствий нарушений.
* Далее необходимо структурировать систему  на функционально полные компоненты (основные и вспомогательные сервисы).
* Выделяют основные  сервисы. Например , для банка – основные сервисы: банковская система, система автоматизации офиса, бухгалтерская система банка и т.д. Чтобы система могла функционировать, выделяют вспомогательные сервисы  (обеспечивающая часть ВС) – серверы БД, почтовые сервисы, ОС и оборудование.
* Основной принцип ИБ: защите подлежат  все сервисы – основные, вспомогательные и коммуникации между ними. АСУ также логично рассматривать как четырехуровневую систему (см. файл презентаций по методологии).
* Описание объекта защиты предполагает процедуру идентификации активов.
* Существуют:
* - аппаратные активы: компьютеры, периферийное оборудование, сетевое оборудование;
* - программные активы: ОС, ППО,  инструментальные средства, программы управления;
* - информационные активы: данные, которые хранятся, обрабатываются и передаются по сети.

ЭТАП 2 [«Анализ рисков информационной безопасности»](#_Toc368249634). Анализ угроз и уязвимостей. Расчет рисков

* Анализ угроз и источников их возникновения
* На этом шаге выполняется анализ угроз и их последствий.  Определение слабых мест  в защите (оценка наиболее вероятных опасностей).
* Необходимо выявить не только сами угрозы, но и источники их возникновения.   См. классификацию угроз.
* После идентификации угроз необходимо определить :
* - вероятность осуществления  угрозы
* Будем считать что, вероятность реализации  угрозы оценивается следующим образом :
* Маловероятно- 0,1;    вероятно – 0,5; весьма вероятно – 1.
* - размер потенциального ущерба. Необходимо учитывать прямые и косвенные потери.
* Теоретические отступления: (для расширения кругозора) J
* Основные методы и модели оценки уязвимости:
* - эмпирический;
* - теоретический;
* - теоретико-эмпирический;
* - экспертные оценки (включая деловые игры, ситуационные модели  поведения потенциального нарушителя и др.)
* Сущность эмпирического подхода лучше всех демонстрирует подход фирмы IBM: на основе длительного сбора информации о реальных проявлениях угроз эмпирическим путем  устанавливается зависимость между потенциально возможным ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения размера ущерба. Теоретический подход основывается на использовании основных положений теории вероятности, математической статистики и имитационном моделировании.
* Исходные данные для оценки риска могут быть получены точные (например, в денежном отношении),  могут быть использованы условные единицы. Мы будем учитывать риск
* условно по трехбальной шкале (см. ниже) или выбирайте метод оценки риска из предложенных (шаг 3).
* Предположим что:
* Уровень риска             Размер ущерба
* Низкий (равен 1) От 50 до 99 у.е.
* Средний (равен 2) От 100 до 149 у.е.
* Высокий (равен 3) От 150 до 200 у.е.

**ЭТАП 3**. ***Разработка политики и стратегии ИБ. Управление рисками.***

* 3.1.Выбор методологии оценки рисков и оценка рисков
* Когда накоплены исходные данные, можно переходить к обработке информации и , собственно,  к оценке риска, которая включает:
* - выбор методологии оценки рисков,
* - оценку рисков.
* Цель оценки: ответ на вопрос – приемлемы ли существующие риски, если нет, то какие защитные средства целесообразно и экономически выгодно использовать.
* Оценка должна быть количественной, допускающей сопоставление с заранее выбранными границами допустимости и с расходами на реализацию системы безопасности.
* Важно выбрать разумную методологию оценки рисков.
* Для недопустимо высоких рисков необходимо строить защитные механизмы (реализовывать защитные меры).
* 3.2.Логическим завершением работы по построению системы ИБ организации является
* Выбор и реализация эффективных и экономичных защитных мер.
* ШАГ 1. Разработка стратегии (политики) защиты информации. Тезисно. Также отразить в работе.
* ШАГ 2. Оценка, выбор средств защиты. Его краткая характеристика и для какого объекта в вашей организации применяется. Отразить в работе
* ШАГ 3. Реализация защитных мер.
* ШАГ 4. Проверка выбранных мер и оценка остаточного риска (необходимо оценить эффективность принятых мер – насколько риск уменьшился и как соотносятся те затраты на защиту с предполагаемым ущербом в случае реализации угрозы). Отразить в работе