

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине «Информационная безопасность и защита данных»

Направление подготовки	15.04.04 Автоматизация технологических процессов и производств
Направленность (профиль)	Информационно-управляющие системы
Год начала обучения	2026
Форма обучения	заочная
Реализуется в семестре	5

Невинномысск, 2026 г.

Содержание

Введение	3
Лабораторная работа №1 Пороговое разделение секрета.....	4
Лабораторная работа №2 Криптография на базе эллиптических кривых.....	9
Лабораторная работа №3 Электронная цифровая подпись ГОСТ Р 34.10-2018	11
Лабораторная работа №4 Парольная защита.....	15
Лабораторная работа № 5 Криптографические методы аутентификации	20
Лабораторная работа № 6 Защита на канальном уровне	24
Лабораторная работа № 7 Защита на сетевом уровне	26
Лабораторная работа № 8 Защита на сеансов уровне	30
Приложение 1	34
Приложение 2	36
Приложение 3	38
Литература	39

Введение

Целью изучения дисциплины является формирование у студента профессиональных компетенций по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств, а также приобретение теоретических знаний и практических навыков по использованию средств защиты для обеспечения информационной безопасности и защиты информации от несанкционированного использования ресурсов АСУ ТП..

Задачи изучения дисциплины заключаются:

- приобретении студентами знаний и практических навыков в области, определяемой основной целью дисциплины;
- приобретение практических навыков работы с алгоритмами защиты информации.

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-3. Способен собирать и анализировать исходные данные для проектирования средств и систем автоматизации	ИД-1 ПК-3. Собирает и анализирует исходные данные для проектирования средств и систем автоматизации	Производит сбор и анализ исходных данных для проектирования средств и систем автоматизации с встроенными механизмами обеспечения информационной безопасности и защиты данных.
	ИД-2 ПК-3. Оформляет техническое задание и обосновывает его для заказчика	Производит оформление технического задания для проектирования средств и систем автоматизации с встроенными механизмами обеспечения информационной безопасности и защиты данных
	ИД-3 ПК-3. Использует современные информационные технологии для сбора и анализа исходных данных для проектирования средств и систем автоматизации	Имеет практический опыт использования современных информационных технологий для сбора и анализа исходных данных для проектирования средств и систем автоматизации

Лабораторная работа №1 Пороговое разделение секрета

Цель работы: исследовать возможности порогового разделения секрета.

Краткие сведения из теории

Разработка схем пространственного разделения секрета первоначально была направлена на сохранение секретного ключа от потери. На данном этапе развития информационных технологий область применения схем разделения секрета расширилась на пороговое разделение информации, динамическое распределение нагрузки передачи данных между компьютерами в сети, закрытую передачу данных, электронное голосование.

1. Пороговая схема разделения секрета Миньотта. Пороговая схема разделения секрета Миньотта использует специальные последовательности целых чисел, названных последовательностями Миньотта.

Пусть n будет целым числом, $n \geq 2$, и $2 \leq k \leq n$. (k, n) -последовательность Миньотта – последовательность положительных целых чисел $m_1 < \dots < m_n$ таких, что $(m_i, m_j) = 1$, для всех $1 \leq i < j \leq n$, и $m_{n-k+2} \cdots m_n < m_1 \cdots m_k$.

С заданной (k, n) -последовательностью Миньотта схема работает следующим образом:

- секрет S выбран как случайное целое число такое, что $\beta < S < \alpha$, где $\alpha = m_1 \cdots m_k$ и $\beta = m_{n-k+2} \cdots m_n$;
- части секрета $I_i = S \bmod m_i$, для всех $1 \leq i \leq n$;
- дано k различных частей I_1, \dots, I_k , секрет S восстанавливается с использованием стандартной Китайской теоремы об остатках, как уникальное решение системы по модулю m_1, \dots, m_k

$$\begin{cases} x \equiv I_1 \pmod{m_1} \\ \vdots \\ x \equiv I_k \pmod{m_k} \end{cases}$$

2. Обобщенная схема Миньотта позволяет использовать модули, которые не обязательно попарно взаимно простые.

Пусть n будет целым числом, $n \geq 2$, и $2 \leq k \leq n$. Обобщенная (k, n) -последовательность Миньотта – последовательность m_1, \dots, m_n положительных целых чисел таких, что $\max_{1 \leq i_1 < \dots < i_{k-1} \leq n} (\lceil \{i_1, \dots, i_{k-1}\} \rceil) < \min_{1 \leq i_1 < \dots < i_k \leq n} (\lceil \{i_1, \dots, i_k\} \rceil)$.

Просто увидеть, что каждая (k, n) -последовательность Миньотта является обобщенной (k, n) -последовательностью Миньотта. Кроме того, если мы умножаем каждый элемент (k, n) -последовательности Миньотта на фиксированный элемент $\delta \in Z$, $(\delta, m_1, \dots, m_n) = 1$ мы получаем обобщенную (k, n) -последовательность Миньотта. Обобщенная схема Миньотта работает подобно схеме Миньотта, с $\alpha = \min_{1 \leq i_1 < \dots < i_k \leq n} (\lceil \{i_1, \dots, i_k\} \rceil)$ и $\beta = \max_{1 \leq i_1 < \dots < i_{k-1} \leq n} (\lceil \{i_1, \dots, i_{k-1}\} \rceil)$.

3. Пороговая схема разделения секрета Асмута-Блума. Эта схема, предложенная Асмутом и Блумом, использует специальные последовательности целых чисел: последовательность попарно взаимно простых положительных целых чисел $r, m_1 < \dots < m_n$, выбранных так, что $r \cdot m_{n-k+2} \cdots m_n < m_1 \cdots m_k$.

С заданной последовательностью, схема работает следующим образом:

- тайна S выбирается как случайный элемент множества Z_r ;
- части $I_i = (S + \gamma \cdot r) \bmod m_i$, для всех $1 \leq i \leq n$, где γ – произвольное целое число такое, что $S + \gamma \cdot r \in Z_{m_1 \dots m_k}$;
- дано k отличных частей I_{i_1}, \dots, I_{i_k} , секрет S может быть получен как $S = x_0 \bmod r$, где x_0 получен с использованием стандартной Китайской теоремы об остатках, как уникальный решение системы по модулю m_{i_1}, \dots, m_{i_k}

$$\begin{cases} x \equiv I_{i_1} \pmod{m_{i_1}} \\ \vdots \\ x \equiv I_{i_k} \pmod{m_{i_k}} \end{cases}$$

4. Обобщенная схема Асмута-Блума допускает модули, которые не обязательно попарно взаимно-простые. Можно использовать любую последовательность $r, m_1 < \dots < m_n$ такую, что $r \cdot \max_{1 \leq i_1 < \dots < i_{k-1} \leq n} (\lceil \{i_1, \dots, i_{k-1}\} \rceil) < \min_{1 \leq i_1 < \dots < i_k \leq n} (\lceil \{i_1, \dots, i_k\} \rceil)$.

Просто увидеть, что, если мы умножаем каждый элемент обычной последовательности Асмута-Блума за исключением r на фиксированный элемент $\delta \in Z$, $(\delta, m_1, \dots, m_n) = 1$, мы получаем обобщенную последовательность Асмута-Блума.

5. Схема Ито-Саито-Нишизеки. Ито, Саито, и Нишизеки ввели так называемую методику совокупного массива для монотонных структур доступа.

Пусть A будет монотонной структурой санкционированного доступа размера n и пусть B_1, \dots, B_m будут соответствующими максимальными множествами несанкционированного доступа. Совокупный массив для структуры доступа A , обозначенной

C^A , является $n \times m$ матрица, $C^A = (C_{i,j}^A)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$, где $C_{i,j}^A = \begin{cases} 0, & \text{если } i \in B_j \\ 1, & \text{если } i \notin B_j \end{cases}$, для всех

$1 \leq i \leq n$ и $1 \leq j \leq m$. Давайте рассмотрим теперь произвольную (m, m) -схему порогового разделения секрета с секретом S и соответствующими тенями s_1, \dots, s_m . В A -схеме разделения секрета, тени I_1, \dots, I_n соответствующие секрету S будут определены как $I_i = \{s_j \mid C_{i,j}^A = 1\}$ для всех $1 \leq i \leq n$ и $1 \leq j \leq m$.

Пример. Пусть $n = 4$ и $A_{\min} = \{\{1, 2\}, \{3, 4\}\}$. В этом случае, мы получим, что $\bar{A}_{\max} = \{\{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\}$ и $m = 4$. Совокупный массив для структуры доступа A

$$C^A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

В этом случае $I_1 = \{s_3, s_4\}$, $I_2 = \{s_1, s_2\}$, $I_3 = \{s_2, s_4\}$ и $I_4 = \{s_1, s_3\}$, где s_1, s_2, s_3, s_4 – тени $(4, 4)$ -схемы порогового разделения секрета S .

6. Схема Бенало-Лихтера. Бенало и Лихтер представили структуры доступа, используя формулы. Более точно, для монотонной структуры санкционированного доступа A размера n , они определили множество F_A как множество формул на множестве переменных $\{v_1, v_2, \dots, v_n\}$ такое, что для каждого $F \in F_A$ интерпретация F относительно присваивания переменных является истиной, если и только если истинные переменные соответствуют множеству $A \in A$. Они отметили, что такие формулы могут использоваться как шаблоны для того, чтобы описать, как секрет может быть

разделен относительно данной структуры доступа. Поскольку формулы могут быть выражены, используя только операторы \wedge и \vee , достаточно указать, как "разбить" секрет поперек этих операторов. Таким образом, мы можем определить части секрета S относительно формул F следующим образом

$$\text{Части}(S, F) = \begin{cases} (S, i), & \text{если } F = v_i, 1 \leq i \leq n; \\ \bigcup_{i=1}^k \text{Части}(S, F_i), & \text{если } F = F_1 \vee F_2 \vee \dots \vee F_k; \\ \bigcup_{i=1}^k \text{Части}(s_i, F_i), & \text{если } F = F_1 \wedge F_2 \wedge \dots \wedge F_k, \end{cases}$$

где, для случая $F = F_1 \wedge F_2 \wedge \dots \wedge F_k$, мы можем использовать любую (k, k) -пороговую схему разделения секрета для получения некоторых частей s_1, \dots, s_k соответствующих секрету S и, наконец, части как $I_i = \{s \mid (s, i) \in \text{Части}(S, F)\}$, для всех $1 \leq i \leq n$, где F – произвольная формула из множества F_A .

Пример. Пусть $n = 3$ и структура санкционированного доступа A задана $A_{\min} = \{\{1, 2\}, \{2, 3\}\}$. Например, формула $F = (v_1 \wedge v_2) \vee (v_2 \wedge v_3)$ находится во множестве F_A . В этом случае $\text{Части}(S, F)$, для некоторого секрета S , может быть получена, как

$$\begin{aligned} \text{Части}(S, F) &= \text{Части}(S, v_1 \wedge v_2) \cup \text{Части}(S, v_2 \wedge v_3) = \\ &= \text{Части}(s_1, v_1) \cup \text{Части}(s_{2,1}, v_2) \cup \text{Части}(s_{2,2}, v_2) \cup \text{Части}(s_3, v_3) = \\ &= \{(s_1, 1), (s_{2,1}, 2), (s_{2,2}, 2), (s_3, 3)\}, \end{aligned}$$

где $s_1, s_{2,1}$ и, соответственно, $s_{2,2}, s_3$ – тени секрета S относительно двух произвольных $(2, 2)$ -пороговых схем. Таким образом, части, соответствующие секрету S относительно структуры доступа A – $I_1 = \{s_1\}$, $I_2 = \{s_{2,1}, s_{2,2}\}$ и $I_3 = \{s_3\}$.

Задание на лабораторную работу

Исследовать пороговую схему разделения секрета в соответствии с вариантом (таблица 1). Модули выбрать из Приложения 1.

Таблица 1 – Варианты для лабораторной работы № 1

Вариант	Пороговая схема	Тип схемы
1	Пороговая схема разделения секрета Миньотта	3-из-5
2	Обобщенная схема Миньотта	3-из-5
3	Пороговая схема разделения секрета Асмута-Блума	3-из-5
4	Обобщенная схема Асмута-Блума	3-из-5
5	Схема Ито-Сайто-Нишизеки	3-из-5
6	Схема Бенало-Лихтера	3-из-5
7	Пороговая схема разделения секрета Миньотта	2-из-3
8	Обобщенная схема Миньотта	2-из-3
9	Пороговая схема разделения секрета Асмута-Блума	2-из-3
10	Обобщенная схема Асмута-Блума	2-из-3
11	Схема Ито-Сайто-Нишизеки	2-из-3
12	Схема Бенало-Лихтера	2-из-3

Содержание отчета

В отчете указать цель работы, представить результаты исследований.

Контрольные вопросы

1. Назначение пороговой схемы.
2. Сравните энтропию частного ключа для схем Миньотта и Асмута-Блума.
3. Китайская теорема об остатках. Численный пример.
4. За счет чего пороговая схема обеспечивает надежное хранение секретной информации.

Лабораторная работа №2 Криптография на базе эллиптических кривых

Цель работы: исследовать криптографические примитивы схем защиты данных на базе алгебры точек эллиптической кривой

Краткие сведения из теории

Операции над точками эллиптической кривой определяются над полем Галуа $GF(p)$, где p – простое число ($p > 3$). Все арифметические операции выполняются по модулю p . Эллиптическая кривая E задается выражением

$$y^2 = x^3 + ax + b,$$

где $4a^2 + 27b^2 \neq 0$ и $x, y, a, b \in GF(p)$. Также существует один элемент, называемый бесконечной точкой и обозначаемый символом « O », который выступает в роли аддитивной единицы: $\forall P(x, y) \in E : P + O = P$.

Для сложения точек эллиптической кривой существуют следующие правила:

- $O = -O$,
- $P(x, y) + O = P(x, y)$,
- $P(x, y) + P(x, -y) = O$.

Операция сложения двух произвольных точек эллиптической кривой выполняется следующим образом:

$$P(x_1, y_1) + P(x_2, y_2) = P(x_3, y_3),$$

где $x_3 = \lambda^2 - x_1 - x_2$; $y_3 = \lambda(x_1 - x_3) - y_1$; $\lambda = (y_2 - y_1)/(x_1 - x_2)$ – угловой коэффициент касательной к эллиптической кривой, используемой для определения результата сложения.

Операция удвоения точки:

$$P(x_1, y_1) + P(x_1, y_1) = P(x_3, y_3),$$

где $x_3 = \lambda^2 - 2x_1$; $y_3 = \lambda(x_1 - x_3) - y_1$; $\lambda = (3(x_1)^2 + a)/(2y_1)$.

Умножение точки $P(x, y) \in E$ на скаляр k над $GF(p)$ определяется серией сложений:

$$Q = [k]P = \underbrace{P + P + \dots + P}_{k \text{ раз}}.$$

Умножение точки на скаляр лежит в основе криптографических алгоритмов на базе группы точек эллиптической кривой.

При разработке криптографических алгоритмов на эллиптической кривой иногда требуется сопоставить данному открытому тексту некоторую точку кривой, при этом обратное отображение должно позволять однозначно определить открытый текст. Один из способов – для фиксированного уравнения кривой $y^2 = f(x)$ с размером задачи l бит над полем K в качестве x -координаты использовать $(n - k)$ -разрядный текст, дополненный k двоичными разрядами так, что число $f(x)$ – квадратный вычет в поле K . Варьируя число k , можно изменять скорость шифрования и вероятность успешного шифрования текста. Такой способ целесообразен для кривых, над простыми полями, поскольку для нахождения «добавки» к открытому тексту нужно вычислять значения квадратичного характера, а эта операция удобно выполняется в простом поле – достаточно найти символ Якоби.

Задание на лабораторную работу

В соответствии с вариантом выбрать параметры эллиптической кривой из Приложения 2. Исследовать процесс встраивания открытого текста (Приложение 3) в координату x точки заданной эллиптической кривой.

Содержание отчета

В отчете указать цель работы, представить результаты исследования.

Контрольные вопросы

1. Вычисление символа Якоби.
2. Извлечение квадратных и кубических корней в конечном поле.
3. Умножение точки эллиптической кривой на число. Численный пример.
4. Проективные координаты.
5. Эллиптические кривые над конечным полем и над расширением конечного поля.

Лабораторная работа №3 Электронная цифровая подпись ГОСТ Р 34.10-2018

Цель работы: исследовать процесс формирования и проверки электронной цифровой подписи по ГОСТ Р 34.10-2018

Краткие сведения из теории

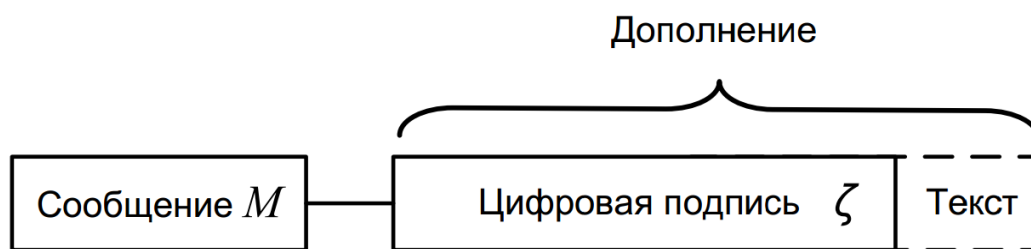
Общепризнанная схема (модель) цифровой подписи (см. ИСО/МЭК 14888–1) охватывает следующие процессы:

- генерация ключей (подписи и проверки подписи);
- формирование подписи;
- проверка подписи. В настоящем стандарте процесс генерации ключей (подписи и проверки подписи) не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами, которые устанавливают соответствующие параметры по взаимному согласованию. Механизм цифровой подписи определяется посредством реализации двух основных процессов:

- формирование подписи;
- проверка подписи.

Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:

- осуществление контроля целостности передаваемого подписанного сообщения,
- доказательное подтверждение авторства лица, подписавшего сообщение,
- защита сообщения от возможной подделки.



Риснук 1 – Схема подписанного сообщения

Поле «Текст», показанное на рисунке 1 и дополняющее поле «Цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в ГОСТ Р 34.10-2018 схема цифровой подписи реализована с использованием операций группы точек эллиптической кривой, определённой над конечным простым полем, а также хэш-функции. Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритмы вычисления хэш-функции установлены в ГОСТ Р 34.11-2018.

Цифровая подпись, представленная в виде двоичного вектора длиной 512 или 1024 бита.

Задание на лабораторную работу

Исследовать процесс формирования ЭЦП для заданного варианта текста:

- а) выполнить процесс формирования ЭЦП для введенного текста, получить результаты по всем этапам формирования ЭЦП на экране дисплея;
- б) выполнить процесс проверки соответствия ЭЦП введенному тексту, получить результаты по всем этапам проверки ЭЦП на экране дисплея;
- в) внести изменения в исходный текст, выполнить процесс проверки ЭЦП для модифицированного текста, убедиться в несоответствии ЭЦП модифицированному тексту;
- г) повторить пункты а–в для текстов различной длины и новых исходных числовых значений для формирования ЭЦП;

Провести сеанс формирования ЭЦП и проверки ее подлинности по следующему протоколу:

- а) студент А – подписант электронного документа, самостоятельно вычисляет ключи для формирования и проверки подлинности ЭЦП;
- б) студент А передает по открытому каналу связи (публично объявляет, передает по локальной сети, копирует на флэш-диск) ключ проверки подлинности ЭЦП студенту В. Секретный ключ для формирования ЭЦП сохраняется им в тайне от других студентов, выполняющих лабораторную работу;

в) студент А составляет электронный документ $m \in M$, вычисляет для него хэш-значение и ЭЦП;

г) студент А передает по открытому каналу связи (по локальной сети, копирует на дискету) в адрес студента В электронный документ с ЭЦП;

д) студент В – получатель электронного документа, защищенного ЭЦП, используя известную функцию хэширования и открытый ключ ЭЦП, проверяет ее подлинность и убеждается в целостности полученного электронного документа;

е) студент С – выполняя роль "злоумышленника", на этапе передачи электронного документа с ЭЦП от студента А к студенту В осуществляет его модификацию и/или подделку ЭЦП посредством подбора секретного ключа для ее вычисления. Полученный электронный документ с ЭЦП передается студенту В;

ж) студент В, осуществляя проверку ЭЦП, убеждается в ее несоответствии полученному электронному документу. Результаты исследования объявляются студентам А и С.

Содержание отчета

В отчете указать цель работы, схему функции хэширования с параметрами, соответствующими варианту индивидуального задания, схемы алгоритмов исследованных функции хэширования и ЭЦП, результаты, полученные при апробировании процессов хэширования и формирования ЭЦП, анализ полученных результатов и выводы по лабораторной работе.

Контрольные вопросы

1. Для каких целей служит функция хэширования и какими основными свойствами она обладает?
2. В чем заключаются методы реализации функции хэширования, основанные на алгоритмах симметричного блочного шифрования?
3. В чем заключаются методы реализации функции хэширования, основанные на числовых корректирующих кодах?
4. На каких математических принципах и задачах (проблемах) основана ЭЦП по алгоритму ГОСТ Р 34.10–2018?
5. Как задается эллиптическая кривая над простым полем?
6. Что называется инвариантом эллиптической кривой?

7. Как определяются коэффициенты эллиптической кривой?
8. Какую длину имеет хэш-значение, полученное по ГОСТ Р 34.10–2018?
9. Как реализуется функция хэширования по ГОСТ Р 34.11–2018? В чем ее преимущество по сравнению с другими типами хэш-функций?
10. Какие длины ключей (исходных значений) рекомендованы для использования на практике при формировании ЭЦП ГОСТ Р 34.10–2018?
11. Каким условиям должны удовлетворять параметры ЭЦП по ГОСТ Р 34.10–2018?
12. Какие отличительные особенности, достоинства и недостатки характерны для ЭЦП по ГОСТ Р 34.10–2018?

Лабораторная работа №4 Парольная защита

Цель работы: исследовать меры противодействия угрозам парольной защиты.

Краткие сведения из теории

Наиболее распространенные методы аутентификации основаны на применении многозначных или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации: по хранимой копии пароля или его свёртке (plaintext-equivalent); по некоторому проверочному значению (verifier - based); без непосредственной передачи информации о пароле проверяющей стороне (zero - knowledge); с использованием пароля для получения криптографического ключа (cryptographic)

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя. Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации. Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "тroyанский конь"). Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и

криптографических преобразований и может быть строго доказана.

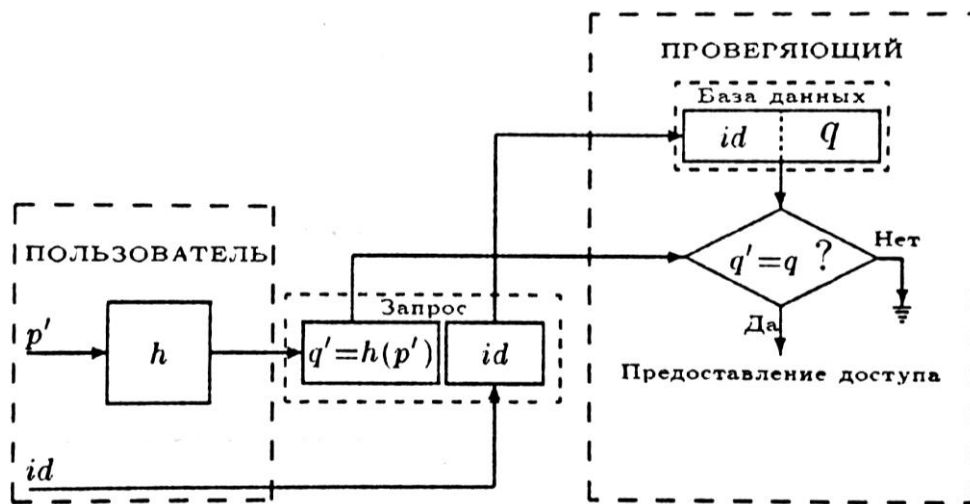


Рисунок 4.1 – Основной вариант схемы защищенных паролей

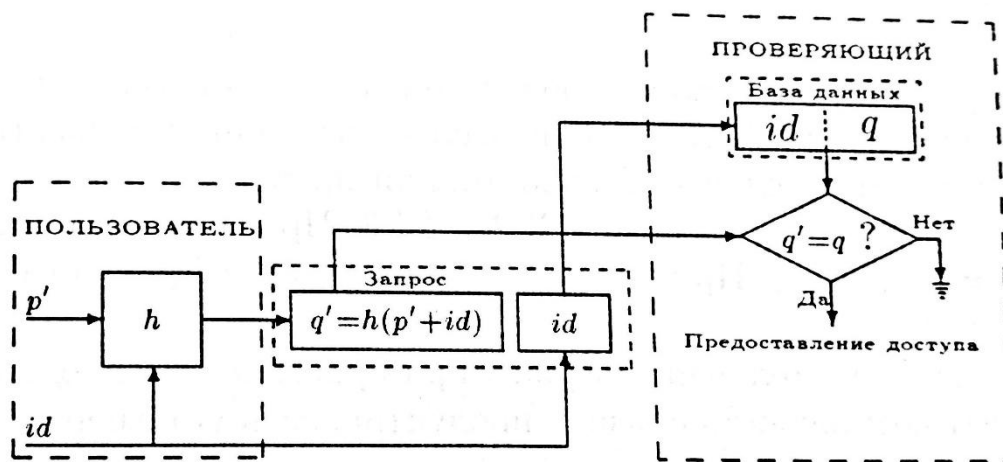


Рисунок 4.2 – Вариант схемы защищенных паролей, устойчивый к табличной атаке

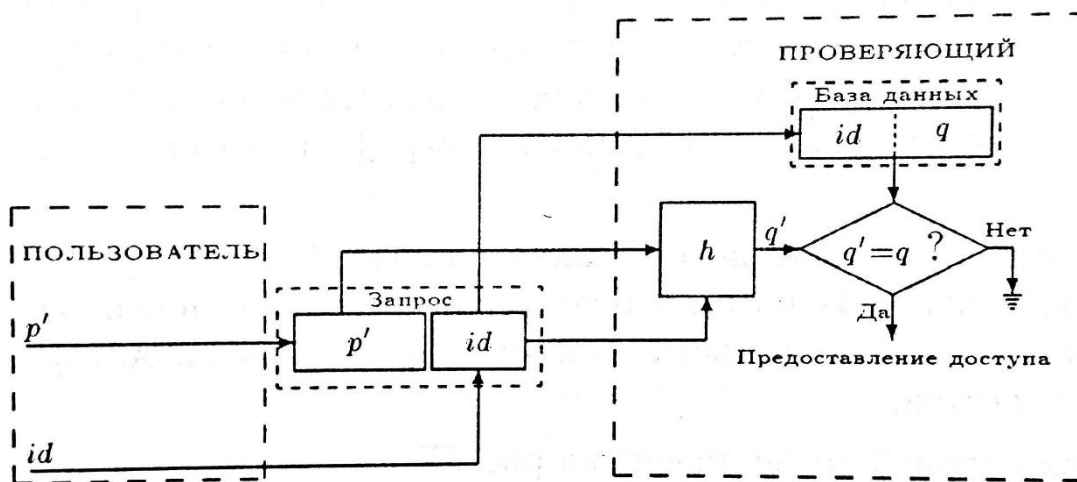


Рисунок 4.3 – Основной вариант парольной защиты при компрометации проверяющего

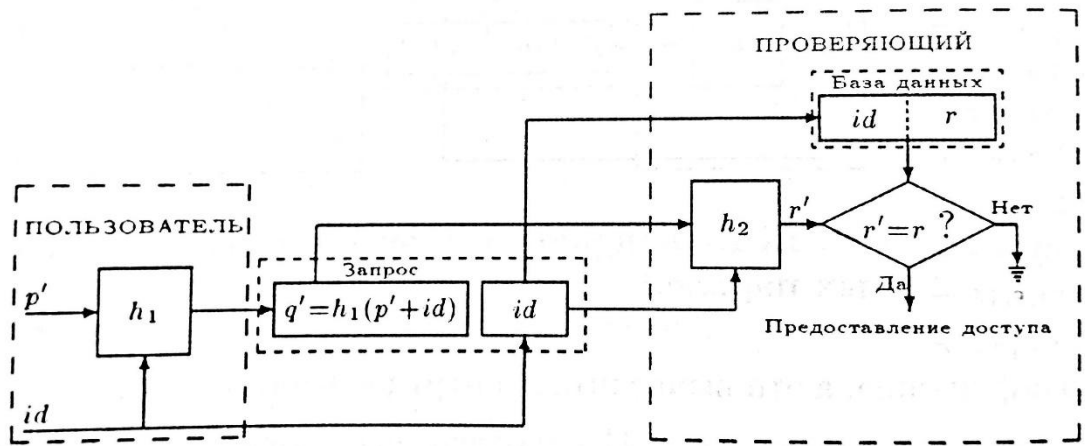


Рисунок 4.4 – Усовершенствованный вариант схемы парольной защиты при компрометации проверяющего

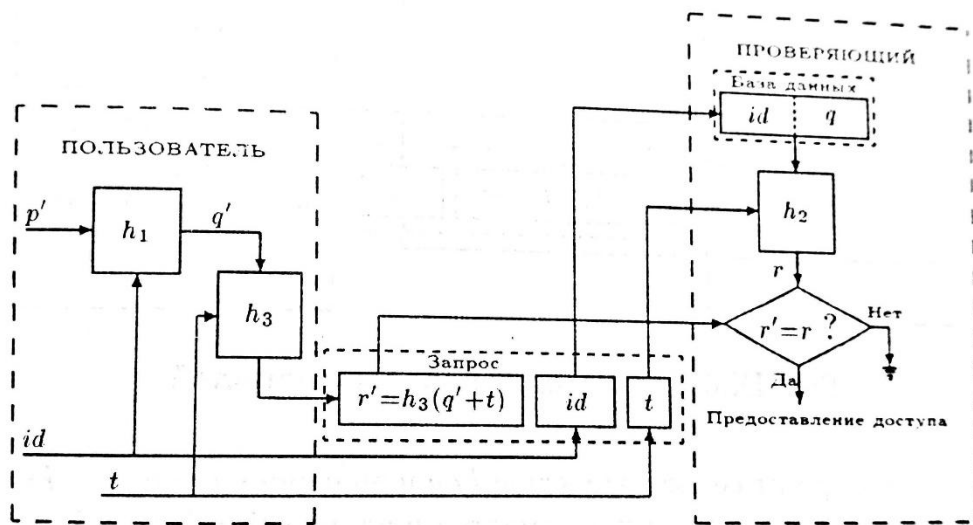


Рисунок 4.5 – Защита от несанкционированного воспроизведения

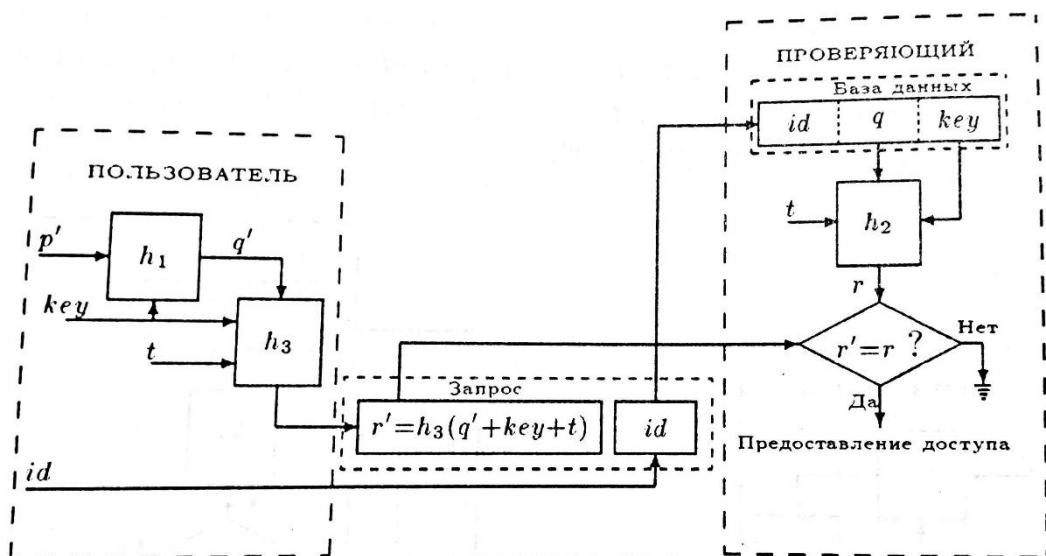


Рисунок 4.6 – Схема одноразовых паролей

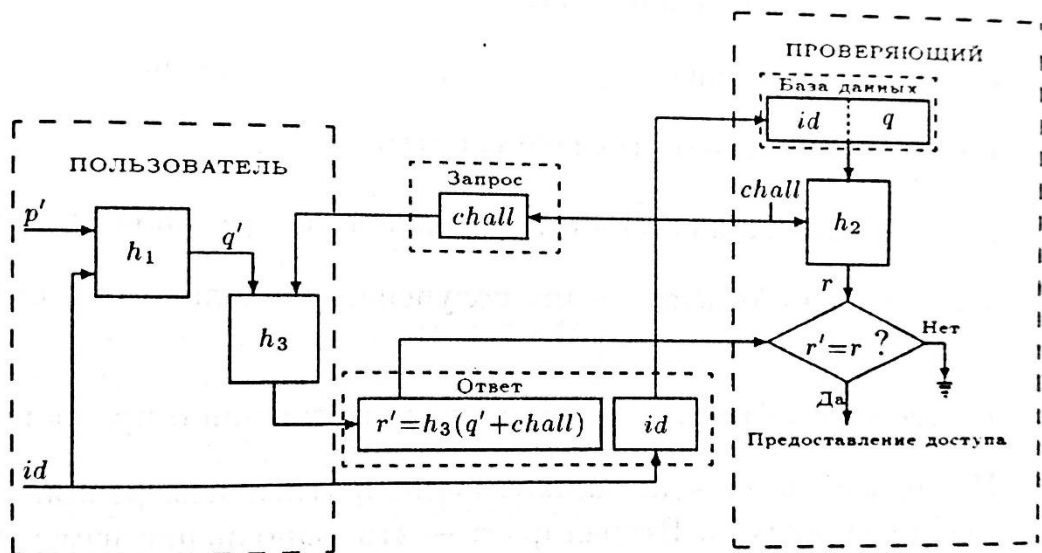


Рисунок 4.7 – Схема аутентификации по методу «запрос-ответ»

Задание на лабораторную работу

Исследовать механизм парольной защиты.

Вариант	Схема
1	Рисунок 4.1
2	Рисунок 4.2
3	Рисунок 4.3
4	Рисунок 4.4
5	Рисунок 4.5
6	Рисунок 4.6
7	Рисунок 4.7
8	plaintext-equivalent
9	verifier-based
10	zero-knowledge
11	cryptographic
12	One-Time Password System (N. Haller, C. Metz)

Содержание отчета

В отчете указать цель работы, представить результаты исследований.

Контрольные вопросы

1. Основной вариант схемы защищенных паролей.
2. Вариант схемы защищенных паролей, устойчивый к табличной атаке.

3. Основной вариант парольной защиты при компрометации проверяющего.
4. Усовершенствованный вариант схемы парольной защиты при компрометации проверяющего.
5. Защита от несанкционированного воспроизведения.
6. Схема одноразовых паролей.
7. Схема аутентификации по методу «запрос-ответ».

Лабораторная работа № 5 Криптографические методы аутентификации

Цель работы: исследовать режимы аутентификации.

Краткие сведения из теории

Многие системы аутентификации используют для самой аутентификации или представления контекста доступа алгоритм шифрования с открытым ключом RSA. Способы аутентификации, основанные на RSA, сводятся к следующему алгоритму.

- Система А генерирует последовательность байтов, обычно случайную, кодирует ее своим ключом и посылает системе В.
- Система В декодирует ее своим ключом. Это возможно, только если системы владеют парными ключами.
- Системы тем или иным способом обмениваются "правильными" значениями зашифрованной посылки.

Для примера рассмотрим принцип RSA-аутентификации в пакете ssh – Secure Shell. Пакет представляет собой функциональную замену программ rlogin/rsh и соответствующего этим программам демона rshd. В пакет входят программы ssh (клиент) и sshd (сервер), а также утилиты для генерации ключей RSA и управления ими. ssh использует RSA для прозрачной аутентификации пользователя при входе в удаленную систему. Кроме того, ssh/sshd могут осуществлять шифрование данных, передаваемых по линии во время сеанса связи и выполнять ряд других полезных функций.

Когда из удаленной системы-клиента приходит запрос на аутентификацию, sshd запрашивает публичный ключ. Если полученный ключ совпадает с хранящимся в файле значением для этой системы, сервер генерирует случайную последовательность из 256 бит, шифрует ее публичным ключом и посылает клиенту. Клиент расшифровывает посылку своим личным ключом, вычисляет 128-битовую контрольную сумму и возвращает ее серверу. Сервер сравнивает полученную последовательность с правильной контрольной суммой и принимает аутентификацию в случае совпадения. Теоретически контрольные суммы могут совпасть и в случае несовпадения ключей, но вероятность такого события крайне мала.

Система групповой работы Lotus Notes также использует для аутентификации открытый ключ. При создании учетной записи пользователя генерируются 621-битный приватный и соответствующий ему публичный ключи. Публичный ключ размещается в доменной адресной книге. Приватный ключ подвергается шифрованию закрытым ключом, который потом запрашивается у пользователя в качестве пароля, и сохраняется в идентификационном файле.

Чтобы аутентифицироваться в системе, пользователь должен указать идентификационный файл и набрать пароль, который позволит расшифровать хранящийся в файле приватный ключ. После этого все пакеты, которыми пользователь обменивается с сервером Notes, снабжаются цифровой подписью на основе этого ключа. Сервер может проверить аутентичность подписи, используя хранящийся в его адресной книге публичный ключ.

Более сложная ситуация возникает, когда пользователь должен аутентифицироваться в другом домене, в адресных книгах которого он не числится. Чтобы сделать такую авторизацию возможной, Notes вводит еще одно понятие: сертификат домена. Этот сертификат также представляет собой пару ключей, пароль к приватному ключу которой известен только администраторам домена. Каждый идентификационный файл, создаваемый в домене, подписывается приватным ключом этого сертификата.

Регистрируясь в чужом домене, пользователь предъявляет свои имя и публичный ключ, подписанные сертификатом своего домена. Если принимающий домен не знает такого сертификата, аутентификация отвергается. Чтобы домен мог признать чужой сертификат, его администратор должен провести кросс-сертификацию, а попросту говоря создать в доменной адресной книге документ, в котором хранится публичный ключ сертификата домена.

Методы, основанные на RSA и других алгоритмах шифрования, не могут решить проблемы распространения прорыва безопасности между доверяемыми системами: проникший в доверяемую систему взломщик получает доступ к приватным ключам и может использовать их для немедленной регистрации в любой из доверяющих систем или даже скопировать ключи для проникновения в эти системы в более удобное время. Шифрование приватного ключа паролем несколько усложняет осуществление такой операции, но в этом случае взломщик может осуществить

словарную атаку. Однако, как уже говорилось ранее, это является практически неизбежной платой за разрешение автоматической регистрации в нескольких системах. В то же время криптографические методы практически устраняют опасность имитации доверяемой системы путем подмены сетевого адреса и значительно увеличивают надежность других методов аутентификации. Например, передача пароля по сети в зашифрованном виде, особенно при использовании двухключевого шифрования или динамических ключей, практически устраняет возможность раскрытия пароля с помощью его подслушивания и т. д.

Задание на лабораторную работу

Исследовать криптографические методы аутентификации. При совпадении вариантов методов аутентификации алгоритмы шифрования должны различаться.

Вариант	Метод
1	Аутентификация в режиме on-line на базе симметричной криптосистемы
2	Аутентификация в режиме on-line на базе асимметричной криптосистемы
3	Аутентификация при участии нескольких серверов
4	Аутентификация в режиме off-line на базе симметричной криптосистемы
5	Аутентификация в режиме off-line на базе асимметричной криптосистемы
6	Аутентификация с привлечением арбитра на базе симметричной криптосистемы
7	Аутентификация с привлечением арбитра на базе асимметричной криптосистемы
8	Аутентификация в режиме on-line на базе симметричной криптосистемы
9	Аутентификация в режиме on-line на базе асимметричной криптосистемы
10	Аутентификация при участии нескольких серверов
11	Аутентификация в режиме off-line на базе симметричной криптосистемы
12	Аутентификация в режиме off-line на базе асимметричной криптосистемы

Содержание отчета

В отчете указать цель работы, представить результаты исследования.

Контрольные вопросы

1. Аутентификация в режиме on-line на базе симметричной криптосистемы.
2. Аутентификация в режиме on-line на базе асимметричной криптосистемы.
3. Аутентификация при участии нескольких серверов.
4. Аутентификация в режиме off-line на базе симметричной криптосистемы.
5. Аутентификация в режиме off-line на базе асимметричной криптосистемы.
6. Аутентификация с привлечением арбитра на базе симметричной криптосистемы.
7. Аутентификация с привлечением арбитра на базе асимметричной криптосистемы.

Лабораторная работа № 6 Защита на канальном уровне

Цель работы: исследовать протоколы защищенных каналов (PPTP, L2F, L2TP)

Краткие сведения из теории

Виртуальные частные сети с удаленным доступом (Virtual Private Dialup Networks — VPDN) позволяют крупным компаниям расширять свои частные сети, используя линии удаленной связи. Новые технологии снимают проблему высокой стоимости междугородней или международной связи и проблему низкой защищенности общих телефонных линий и каналов Интернет, через которые удаленный пользователь получает доступ к корпоративной сети. Новые технологии предоставляют удаленным офисам и пользователям безопасный доступ к инфраструктуре предприятия через местное подключение к сети Интернет. В настоящее время для этого используются три протокола: протокол эстафетной передачи на втором уровне (Layer 2 Forwarding — L2F), сквозной туннельный протокол (Point-to-Point Tunneling Protocol — PPTP) и туннельный протокол второго уровня (Layer 2 Tunneling Protocol — L2TP).

Протокол эстафетной передачи на втором уровне (Layer 2 Forwarding — L2F) был разработан компанией Cisco Systems. Он обеспечивает туннелирование протоколов канального уровня (то есть фреймов High-Level Data Link Control [HDLC], async HDLC или Serial Line Internet Protocol [SLIP]) с использованием протоколов более высокого уровня, например, IP. С помощью таких туннелей можно разделить местоположение сервера удаленного доступа, к которому подключается пользователь, используя местные коммутируемые линии связи, и точки, где происходит непосредственная обработка протокола удаленного доступа (SLIP, PPP), и пользователь получает доступ в сеть. Эти туннели дают возможность использовать приложения, требующие удаленного доступа с частными адресами IP, IPX и AppleTalk через протокол SLIP/PPP по существующей инфраструктуре Интернет. Поддержка таких многопротокольных приложений виртуального удаленного доступа очень выгодна конечным пользователям и независимым поставщикам услуг, поскольку позволяет разделить на всех расходы на средства доступа и базовую инфраструктуру и дает возможность осуществлять доступ через местные линии связи. Кроме того, такой подход защищает инвестиции, сделанные в существующие приложения, работающие не по протоколу

IP, предоставляя защищенный доступ к ним и в то же время поддерживая инфраструктуру доступа к Интернет.

Сквозной туннельный протокол Point-to-Point Tunneling Protocol (PPTP) создан корпорацией Microsoft. Он никак не меняет протокол PPP, но предоставляет для него новое транспортное средство. В рамках этого протокола определяется архитектура клиент/сервер, предназначенная для разделения функций, которые существуют в текущих NAS, и для поддержки виртуальных частных сетей (VPN). Сервер сети PPTP (PNS) должен работать под управлением операционной системы общего назначения, а клиент, который называется концентратором доступа к PPTP (PAC), работает на платформе удаленного доступа. PPTP определяет протокол управления вызовами, который позволяет серверу управлять удаленным коммутируемым доступом через телефонные сети общего пользования (PSTN) или цифровые каналы ISDN или инициализировать исходящие коммутируемые соединения. PPTP использует механизм общей маршрутной инкапсуляции (GRE) для передачи пакетов PPP, обеспечивая при этом контроль потоков и сетевых заторов. Безопасность данных в PPTP может обеспечиваться при помощи протокола IPSec. Протоколы L2F и PPTP имеют сходную функциональность. Компании Cisco и Microsoft согласились вместе (в рамках IETF) разработать единый стандартный протокол, который получил название туннельного протокола второго уровня (Layer 2 Tunneling Protocol — L2TP).

Задание на лабораторную работу

Исследовать протоколы туннелирования.

Содержание отчета

В отчете указать цель работы, привести результаты исследований.

Контрольные вопросы

1. Формат заголовка.
2. Типы управляющих сообщений.
3. Протокольные операции.
4. Применение протоколов туннелирования. Примеры.
5. Безопасность пакетного уровня.
6. Безопасность на конце туннеля.

Лабораторная работа № 7 Защита на сетевом уровне

Цель работы: исследование средств безопасности IPSec

Краткие сведения из теории

Безопасный протокол IP (IPSec) представляет собой набор стандартов, используемых для защиты данных и для аутентификации на уровне IP. Текущие стандарты IPSec включают независимые от алгоритмов базовые спецификации, которые являются стандартными RFC.

IPsec предназначен для безопасного взаимодействия на основе криптографии для IPv4 и IPv6. Набор сервисов безопасности включает управление доступом, целостность соединения, аутентификацию исходных данных, защиту от replay-атак (целостность последовательности), конфиденциальность (шифрование) и конфиденциальный поток трафика. Эти сервисы предоставляются на уровне IP, обеспечивая защиту для IP и/или протоколов более высокого уровня.

IPsec поддерживает две формы целостности: целостность соединения и частичную целостность последовательности. Целостность соединения является сервисом безопасности, который определяет модификацию конкретной IP датаграммы, независимо от последовательности датаграмм в потоке трафика. Частичная целостность последовательности является anti-replay сервисом, с помощью которого определяется получение дубликатов IP датаграмм.

IPsec обеспечивает сервисы безопасности на IP-уровне, выбирая нужные протоколы безопасности, определяя алгоритмы, используемые сервисами, и предоставляя все криптографические ключи требуемым сервисам. IPsec может использоваться для защиты одного или нескольких «путей» между парой хостов, между парой шлюзов безопасности или между шлюзом безопасности и хостом.

IPsec использует два протокола для обеспечения безопасности трафика – Authentication Header (AH) и Encapsulating Security Payload (ESP).

- Authentication Header (AH) обеспечивает целостность соединения, аутентификацию исходных данных и дополнительно может обеспечивать anti-replay сервис.

- Encapsulating Security Payload (ESP) протокол может обеспечивать конфиденциальность (шифрование) трафика. ESP также может обеспечивать целостность соединения, аутентификацию исходных данных и дополнительно anti-replay сервис. Целостность обеспечивается только для протоколов более высокого уровня. Хотя бы один из этих сервисов должен быть задействован при использовании ESP.

Эти протоколы могут применяться как по отдельности так и в комбинации друг с другом для обеспечения необходимого набора сервисов безопасности в IPv4 и IPv6. Каждый протокол поддерживает два режима использования: режим транспорта и режим туннелирования.

IPsec позволяет системному администратору управлять детализацией, с которой предоставляется сервис безопасности. Например, можно создать единственный зашифрованный туннель между двумя безопасными шлюзами, или для каждого TCP соединения может быть создан зашифрованный туннель между парой хостов. IPsec позволяет указывать следующие параметры:

- какие сервисы используются и в какой комбинации;
- необходимый уровень детализации применяемой защиты;
- алгоритмы, используемые для обеспечения безопасности на основе криптографии.

Протокол IPSec включает криптографические методы, удовлетворяющие потребности управления ключами на сетевом уровне безопасности. Протокол управления ключами Ассоциации безопасности Интернет (Internet Security Association Key Management Protocol — ISAKMP) создает рамочную структуру для управления ключами в сети Интернет и предоставляет конкретную протокольную поддержку для согласования атрибутов безопасности. Само по себе это не создает ключей сессии, однако эта процедура может использоваться с разными протоколами, создающими такие ключи.

Протокол определения ключей Oakley Key Determination Protocol пользуется гибридным методом Диффи-Хеллмана, чтобы создать ключи сессии Интернет для центральных компьютеров и маршрутизаторов. Протокол Oakley решает важную задачу обеспечения полной безопасности эстафетной передачи данных. Он основан на криптографических методах. Полная защита эстафетной передачи означает, что если

хотя бы один ключ раскрыт, раскрыты будут только те данные, которые зашифрованы этим ключом. Что же касается данных, зашифрованных последующими ключами, они останутся в полной безопасности.

Протоколы ISAKMP и Oakley были совмещены в рамках гибридного протокола IKE — Internet Key Exchange. Протокол IKE, включающий ISAKMP и Oakley, использует рамочную структуру ISAKMP для поддержки подмножества режимов обмена ключами Oakley. Новый протокол обмена ключами обеспечивает (в виде опции) полную защиту эстафетной передачи данных, полную защиту ассоциаций, согласования атрибутов, а также поддерживает методы аутентификации, допускающие отказ от авторства и не допускающие такого отказа. Этот протокол может, к примеру, использоваться для создания виртуальных частных сетей (VPN) и для того, чтобы предоставить пользователям, находящимся в удаленных точках (и пользующимся динамически распределяемыми адресами IP), доступ к защищенной сети.

Задание на лабораторную работу

Исследовать режимы и способы использования IPSec.

Вариант	Режим	Протокол	Тип приложение
1	Транспортный	AH	Клиент
2	Туннельный	AH	Клиент
3	Транспортный	ESP	Клиент
4	Туннельный	ESP	Клиент
5	Транспортный	AH	Сервер
6	Туннельный	AH	Шлюз
7	Транспортный	ESP	Сервер
8	Туннельный	ESP	Шлюз
9	Транспортный	AH	Сервер
10	Туннельный	AH	Шлюз
11	Транспортный	ESP	Сервер
12	Туннельный	ESP	Шлюз

Содержание отчета

В отчете указать цель работы, привести результаты исследований.

Контрольные вопросы

1. Архитектура IPSec.
2. Реализация IPSec в .NET Framework.
3. Обработка входных и выходных пакетов.
4. Протоколы IPSec.
5. Режимы IPSec.
6. Internet Key Exchange. Фазы IKE.

Лабораторная работа № 8 Защита на сеансов уровне

Цель работы: исследование протоколов SSL/TLS и SOCKS

Краткие сведения из теории

SSL – это открытый протокол, разработанный компанией Netscape. SSL определяет механизм поддержки безопасности данных на уровне между протоколами приложений (такими как Hypertext Transfer Protocol [HTTP], Telnet, Network News Transfer Protocol [NNTP] или File Transfer Protocol [FTP]) и протоколом TCP/IP. Он поддерживает шифрование данных, аутентификацию серверов, целостность сообщений и (в качестве опции) аутентификацию клиентов в канале TCP/IP. SSL был представлен рабочей группе по безопасности консорциума W3 (W3C) для утверждения в качестве стандартного средства безопасности Web-браузеров и серверов в сети Интернет.

Основная цель протокола SSL состоит в том, чтобы обеспечить защищенность и надежность связи между двумя подключенными друг к другу приложениями. Этот протокол состоит из двух уровней. Нижний уровень, который располагается поверх надежного транспортного протокола (например, TCP), называется SSL Record Protocol. SSL Record Protocol используется для встраивания различных протоколов высокого уровня. Один из таких встроенных протоколов, SSL Handshake Protocol, позволяет серверу и клиенту аутентифицировать друг друга и согласовывать алгоритм шифрования и криптографические ключи, прежде чем протокол приложения произведет обмен первыми битами данных. Одно из преимуществ SSL состоит в том, что он независим от протоколов приложений. Протокол высокого уровня может совершенно прозрачно располагаться поверх протокола SSL. Протокол SSL поддерживает безопасность связи, придавая ей следующие свойства:

- Защищенность связи. После первоначального квитирования связи применяются средства шифрования и определяется секретный ключ. Для шифрования данных используются средства симметричной криптографии (например, DES).
- Участник сеанса связи может быть аутентифицирован средствами асимметричной криптографии (например, RSA, DSS).
- Надежность связи. Транспортные средства проводят проверку целостности сообщений с помощью зашифрованного кода целостности (MAC). Для вычисления

кодов MAC используются безопасные хэш-функции (SHA, MD5).

Протокол SSL принят только в рамках HTTP. Другие протоколы доказали свою способность работать с SSL, но используют ее не часто.

SOCKS разработан для того, чтобы дать возможность приложениям клиент/сервер в доменах TCP и UDP удобно и безопасно пользоваться услугами межсетевых экранов. Он дает пользователям возможность преодолевать межсетевые экраны организации и получать доступ к ресурсам, расположенным в сети Интернет. SOCKS является «посредником уровня приложений»: он взаимодействует с общими сетевыми средствами (например, Telnet и браузер Netscape) и с помощью центрального сервера (прокси-сервера) от имени компьютера устанавливает связь с другими центральными компьютерами.

SOCKS версия 4 решает вопрос незащищенного пересечения межсетевых экранов приложениями клиент/сервер, основанными на протоколе TCP, включая Telnet, FTP и популярные информационные протоколы, такие как HTTP, Wide Area Information Server (WAIS) и GOPHER. SOCKS версия 5, RFC 1928, является дальнейшим расширением четвертой версии SOCKS. Он включает в себя UDP, расширяет общую рамочную структуру, придавая ей возможность использования мощных обобщенных схем аутентификации, и расширяет систему адресации, включая в нее имя домена и адреса IP v6.

В настоящее время предлагается создать механизм управления входящими и исходящими многоадресными сообщениями IP, которые проходят через межсетевые экраны. Это достигается определением расширений для существующего протокола SOCKS V.5, что создает основу для аутентифицированного перехода межсетевых экранов одноадресным пользовательским трафиком TCP и UDP. Однако ввиду того, что поддержка UDP в текущей версии SOCKS V.5 имеет проблемы с масштабируемостью и другие недостатки (и их обязательно нужно разрешить, прежде чем переходить к многоадресной передаче), расширения определяются двояко: как базовые расширения UDP и как многоадресные расширения UDP.

Функционирование SOCKS заключается в замене стандартных сетевых системных вызовов в приложении их специальными версиями. Эти новые системные вызовы устанавливают связь с прокси-сервером SOCKS (который конфигурируется

самим пользователем в приложении или системным файлом конфигурации), подключаясь к хорошо известному порту (обычно это порт 1080/TCP). После установления связи с сервером SOCKS приложение отправляет серверу имя машины и номер порта, к которому хочет подключиться пользователь. Сервер SOCKS реально устанавливает связь с удаленным центральным компьютером, а затем прозрачно передает данные между приложением и удаленной машиной.

Трудность с использованием SOCKS состоит в том, что кто-то должен проводить работу по замене сетевых системных вызовов версиями SOCKS (этот процесс обычно называется «SOCKS-ификацией» приложения). Большинство обычных сетевых приложений (Telnet, FTP, finger, whois) уже SOCKS-ифицированы, и многие производители включают поддержку SOCKS в свои коммерческие приложения.

Задание на лабораторную работу

Студенты соответствующих вариантов объединяются в группу для исследования протоколов.

Вариант	Протокол	Приложение
1	SSL Протокол рукопожатия	Клиент
2		Сервер
3	SSL Протокол тревоги	Клиент
4		Сервер
5	SSL Протокол изменения шифра	Клиент
6		Сервер
7	SSL Протокол приложения	Клиент
8		Сервер
9	SOCKS 4	Клиент
10		Сервер
11	SOCKS 5	Клиент
12		Сервер

В работе необходимо исследовать устойчивость протоколов к известным атакам.

Содержание отчета

В отчете указать цель работы, представить результаты исследований.

Контрольные вопросы

1. Цель использования SSL/TLS.
2. Цель использования SOCKS.
3. Способы получения SSL-сертификата/
4. Механизмы образования ключа для текущего сессии в SSL/TLS.
5. Применение SSL/TLS.

Приложение 1

Простые числа для лабораторных работ

Вариант	Простые числа
1	170141183460469231731687303715884105757 170141183460469231731687303715884105773 170141183460469231731687303715884105793 170141183460469231731687303715884105829 170141183460469231731687303715884105851
2	170141183460469231731687303715884105979 170141183460469231731687303715884106001 170141183460469231731687303715884106031 170141183460469231731687303715884106123 170141183460469231731687303715884106207
3	170141183460469231731687303715884106213 170141183460469231731687303715884106231 170141183460469231731687303715884106273 170141183460469231731687303715884106303 170141183460469231731687303715884106309
4	170141183460469231731687303715884106319 170141183460469231731687303715884106409 170141183460469231731687303715884106439 170141183460469231731687303715884106721 170141183460469231731687303715884106723
5	170141183460469231731687303715884106787 170141183460469231731687303715884107009 170141183460469231731687303715884107029 170141183460469231731687303715884107149 170141183460469231731687303715884107237
6	170141183460469231731687303715884107339 170141183460469231731687303715884107467 170141183460469231731687303715884107477 170141183460469231731687303715884107579 170141183460469231731687303715884107587
7	170141183460469231731687303715884107621 170141183460469231731687303715884107639 170141183460469231731687303715884107717 170141183460469231731687303715884107923 170141183460469231731687303715884108073
8	170141183460469231731687303715884108077 170141183460469231731687303715884108227 170141183460469231731687303715884105727 170141183460469231731687303715884105703 170141183460469231731687303715884105689

9	170141183460469231731687303715884105433 170141183460469231731687303715884105419 170141183460469231731687303715884105221 170141183460469231731687303715884105217 170141183460469231731687303715884105151
10	170141183460469231731687303715884105031 170141183460469231731687303715884105031 170141183460469231731687303715884104993 170141183460469231731687303715884104927 170141183460469231731687303715884104771
11	170141183460469231731687303715884104647 170141183460469231731687303715884104623 170141183460469231731687303715884104587 170141183460469231731687303715884104527 170141183460469231731687303715884104497
12	170141183460469231731687303715884104281 170141183460469231731687303715884104243 170141183460469231731687303715884104233 170141183460469231731687303715884103987 170141183460469231731687303715884103981

Приложение 2

Параметры эллиптической кривой для лабораторных работ

Вариант	Параметры эллиптической кривой
1	<p>p = DB7C 2ABF62E3 5E668076 BEAD208B a = DB7C 2ABF62E3 5E668076 BEAD2088 b = 659E F8BA0439 16EED89 11702B22 G = 04 09487239 995A5EE7 6B55F9C2 F098A89C E5AF8724 C0A23E0E 0FF77500 n = DB7C 2ABF62E3 5E7628DF AC6561C5</p>
2	<p>p = DB7C 2ABF62E3 5E668076 BEAD208B a = 6127 C24C05F3 8A0AAAF6 5C0EF02C b = 51DE F1815DB5 ED74FCC3 4C85D709 G = 04 4BA30AB5 E892B4E1 649DD092 8643ADCD 46F5882E 3747DEF3 6E956E97 n = 36DF 0AAFD8B8 D7597CA1 0520D04B</p>
3	<p>p = FFFFFFFD FFFFFFFF FFFFFFFF FFFFFFFF a = FFFFFFFD FFFFFFFF FFFFFFFF FFFFFFFC b = E87579C1 1079F43D D824993C 2CEE5ED3 G = 04 161FF752 8B899B2D 0C28607C A52C5B86 CF5AC839 5BAFEB13 C02DA292 DDED7A83 n = FFFFFFFE 00000000 75A30D1B 9038A115</p>
4	<p>p = FFFFFFFD FFFFFFFF FFFFFFFF FFFFFFFF a = D6031998 D1B3BBFE BF59CC9B BFF9AEE1 b = 5EEEFCA3 80D02919 DC2C6558 BB6D8A5D G = 04 7B6AA5D8 5E572983 E6FB32A7 CDEBC140 27B6916A 894D3AEE 7106FE80 5FC34B44 n = 3FFFFFFF 7FFFFFFF BE002472 0613B5A3</p>
5	<p>p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFAC73 a = 00000000 00000000 00000000 00000000 00000000 b = 00000000 00000000 00000000 00000000 00000007 G = 04 3B4C382C E37AA192 A4019E76 3036F4F5 DD4D7EBB 938CF935 318FDCED 6BC28286 531733C3 F03C4FEE n = 01 00000000 00000000 0001B8FA 16DFAB9A CA16B6B3</p>
6	<p>p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFF a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFC b = 1C97BEFC 54BD7A8B 65ACF89F 81D4D4AD C565FA45 G = 04 4A96B568 8EF57328 46646989 68C38BB9 13CBFC82 23A62855 3168947D 59DCC912 04235137 7AC5FB32 n = 01 00000000 00000000 0001F4C8 F927AED3 CA752257</p>
7	<p>p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFAC73 a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFAC70 b = B4E134D3 FB59EB8B AB572749 04664D5A F50388BA G = 04 52DCB034 293A117E 1F4FF11B 30F7199D 3144CE6D FEAFEF2 E331F296 E071FA0D F9982CFE A7D43F2E n = 01 00000000 00000000 0000351E E786A818 F3A1A16B</p>
8	<p>p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFEE37 a = 00000000 00000000 00000000 00000000 00000000 00000000 b = 00000000 00000000 00000000 00000000 00000000 00000003</p>

	<p>G = 04 DB4FF10E C057E9AE 26B07D02 80B7F434 1DA5D1B1 EAE06C7D 9B2F2F6D 9C5628A7 844163D0 15BE8634 4082AA88 D95E2F9D n = FFFFFFFF FFFFFFFF FFFFFFFE 26F2FC17 0F69466A 74DEFD8D</p>
9	<p>p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFC b = 64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1 G = 04 188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012 07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811 n = FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831</p>
10	<p>p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFE56D a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 b = 00000000 00000000 00000000 00000000 00000000 00000000 00000005 G = 04 A1455B33 4DF099DF 30FC28A1 69A467E9 E47075A9 0F7E650E B6B7A45C 7E089FED 7FBA3442 82CAFBD6 F7E319F7 C0B0BD59 E2CA4BDB 556D61A5 n = 01 00000000 00000000 00000000 0001DCE8 D2EC6184 CAF0A971 769FB1F7</p>
11	<p>p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 00000000 00000001 a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFE b = B4050A85 0C04B3AB F5413256 5044B0B7 D7BFD8BA 270B3943 2355FFB4 G = 04 B70E0CBD 6BB4BF7F 321390B9 4A03C1D3 56C21122 343280D6 115C1D21 BD376388 B5F723FB 4C22DFE6 CD4375A0 5A074764 44D58199 85007E34 n = FFFFFFFF FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D</p>
12	<p>p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFC2F a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007 G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8 n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141</p>

Приложение 3

Варианты открытого текста для лабораторных работ

Вариант	Текст
1	They met me in the day of success: and I have learned by the perfectest report, they have more in them than mortal knowledge.
2	When I burned in desire to question them further, they made themselves air, into which they vanished.
3	Whiles I stood rapt in the wonder of it, came missives from the king, who all-hailed me 'Thane of Cawdor;
4	by which title, before, these weird sisters saluted me, and referred me to the coming on of time, with 'Hail, king that shalt be!'
5	This have I thought good to deliver thee, my dearest partner of greatness, that thou mightst not lose the dues of rejoicing, by being ignorant of what greatness is promised thee.
6	Lay it to thy heart, and farewell.' Glamis thou art, and Cawdor; and shalt be What thou art promised: yet do I fear thy nature;
7	It is too full o' the milk of human kindness To catch the nearest way: thou wouldst be great;
8	Art not without ambition, but without The illness should attend it: what thou wouldst highly, That wouldst thou holily;
9	wouldst not play false, And yet wouldst wrongly win: thou'ldst have, great Glamis, That which cries 'Thus thou must do, if thou have it;
10	And that which rather thou dost fear to do Than wishest should be undone.' Hie thee hither, That I may pour my spirits in thine ear;
11	And chastise with the valour of my tongue All that impedes thee from the golden round, Which fate and metaphysical aid doth seem To have thee crown'd withal.
12	Thou'rt mad to say it: Is not thy master with him? who, were't so, Would have inform'd for preparation.

Литература

1. Алексеев, А.П.; Многоуровневая защита информации Электронный ресурс : монография / А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2017. - 128 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-904029-72-2
2. Бурькова, Е. В; Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова ; Министерство образования и науки Российской Федерации ; Оренбургский государственный университет ; Кафедра вычислительной техники и защиты информации. - Оренбург : Оренбургский государственный университет, 2017. - 158 с. : табл., схем. - <http://biblioclub.ru/>. - Библиогр. в кн. - ISBN 978-5-7410-1697-8
3. Горев, А.И.; Обработка и защита информации в компьютерных системах Электронный ресурс : практическое пособие / А.А. Симачков / А.И. Горев. - Омск : Омская академия МВД России, 2016. - 88 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-88651-642-5
4. Шаньгин, В. Ф; Информационная безопасность и защита информации Электронный ресурс / В. Ф. Шаньгин. - Информационная безопасность и защита информации, 2019-04-19. - Саратов : Профобразование, 2017. - 702 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-4488-0070-2

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
**Федеральное государственное автономное образовательное учреждение
высшего образования**
**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
НЕВИННОМЫССКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ
(ФИЛИАЛ)**

Методические указания к самостоятельной работе
для студентов направления
15.04.04 «Автоматизация технологических процессов и производств»
по дисциплине
**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА
ДАННЫХ»**

Невинномысск, 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	43
ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ	
1. ОБЩАЯ ХАРАКТЕРИСТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ	
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ»	45
1.1. Подготовка к лекциям.....	47
1.2. Подготовка к практическим занятиям	48
1.3. Самостоятельное изучение материала тем	50
1.4. Подготовка к экзамену	53
2. СРЕДСТВА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ОБУЧАЮЩИХСЯ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ	
«ПРОЕКТИРОВАНИЕ СИСТЕМ АВТОМАТИЗАЦИИ»	54
3. ОТЧЕТНОСТЬ ПО ДИСЦИПЛИНЕ	66
РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА	67

ВВЕДЕНИЕ

Дисциплина «Информационная безопасность и защита данных» ставит своей целью формирование следующих компетенций будущего магистра по направлению подготовки 15.04.04 — Автоматизация технологических процессов и производств.

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-3. Способен собирать и анализировать исходные данные для проектирования средств и систем автоматизации	ИД-1 ПК-3. Собирает и анализирует исходные данные для проектирования средств и систем автоматизации	Производит сбор и анализ исходных данных для проектирования средств и систем автоматизации с встроенными механизмами обеспечения информационной безопасности и защиты данных.
	ИД-2 ПК-3. Оформляет техническое задание и обосновывает его для заказчика	Производит оформление технического задания для проектирования средств и систем автоматизации с встроенными механизмами обеспечения информационной безопасности и защиты данных
	ИД-3 ПК-3. Использует современные информационные технологии для сбора и анализа исходных данных для проектирования средств и систем автоматизации	Имеет практический опыт использования современных информационных технологий для сбора и анализа исходных данных для проектирования средств и систем автоматизации

Задачи изучения дисциплины заключаются:

- приобретении студентами знаний и практических навыков в области, определяемой основной целью дисциплины;
- приобретение практических навыков работы с алгоритмами защиты информации.

Студент после изучения дисциплины «Информационная безопасность и защита данных» должен

- производить сбор и анализ исходных данных для проектирования средств и систем автоматизации с встроенными механизмами обеспечения информационной безопасности и защиты данных.

- производить оформление технического задания для проектирования средств и систем автоматизации с встроенными механизмами обеспечения информационной безопасности и защиты данных

- иметь практический опыт использования современных информационных технологий для сбора и анализа исходных данных для проектирования средств и систем автоматизации

Методические указания предназначены для выполнения самостоятельной работы по дисциплине «Информационная безопасность и защита данных» с учетом требований ФГОС ВО для направления подготовки 15.04.04 — Автоматизация технологических процессов и производств. Они способствуют лучшему усвоению студентами теоретических положений и обеспечивает приобретение практических навыков по исследованию элементов и систем автоматического регулирования и управления.

ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1	Пороговое разделение секрета. Постановка задачи: разделение секрета между n участниками с возможностью восстановления при наличии не менее t участников (схемы (t, n)). Схема Шамира на основе интерполяции полиномов и схема Блэкли на основе пересечения гиперплоскостей. Применение пороговых схем в системах распределенного хранения ключей, протоколах аутентификации и многосторонних вычислениях.
2	Криптография на базе эллиптических кривых. Алгебраическая структура эллиптических кривых над конечными полями, операция сложения точек. Задача дискретного логарифмирования на эллиптической кривой (ECDLP) и ее стойкость. Алгоритмы формирования и проверки электронной подписи (ECDSA, ГОСТ Р 34.10), протоколы выработки общего ключа (ECDH).
3	Электронная цифровая подпись ГОСТ Р 34.10-2018. Математическая основа: использование эллиптических кривых, параметры кривых, простое поле или поле характеристики два. Процедуры генерации ключевой пары, формирования подписи (вычисление хеша, определение точки кривой, вычисление компонент подписи) и проверки подписи. Отличия от предыдущей версии ГОСТ Р 34.10-2012, области применения в системах отечественной криптографии.
4	Парольная защита.

	Методы хранения паролей: хеширование (с солью, с адаптивной сложностью, PBKDF2, bcrypt, Argon2). Атаки на парольную защиту (перебор, словарные атаки, радужные таблицы) и способы противодействия. Политики генерации и управления паролями, двухфакторная аутентификация, использование менеджеров паролей.
5	Криптографические методы аутентификации. Протоколы аутентификации с нулевым разглашением, на основе симметричных и асимметричных криптосистем. Аутентификация по времени (TOTP), одноразовые пароли (HOTP), сертификаты открытых ключей. Обеспечение целостности и взаимной аутентификации в сетевых протоколах (CHAP, EAP, Kerberos).
6	Защита на канальном уровне. Протоколы шифрования канального уровня: MACsec (IEEE 802.1AE), технологии защиты в беспроводных сетях (WPA3, WEP). Управление ключами сеанса, обеспечение конфиденциальности и целостности на уровне кадра. Интеграция с протоколами более высоких уровней, аппаратная реализация и влияние на производительность.
7	Защита на сетевом уровне. Протокол IPsec: архитектура (AH, ESP), режимы работы (транспортный, туннельный), управление ключами (IKE, IKEv2). Виртуальные частные сети (VPN) на основе IPsec, использование сертификатов и предварительно разделенных ключей. Сравнение с альтернативными решениями (WireGuard, OpenVPN), обеспечение защиты от атак на сетевом уровне.
8	Защита на сеансовом уровне. Протокол TLS/SSL: версии, алгоритмы шифрования и аутентификации, процедуры установления сеанса (handshake). Управление сессионными ключами, обеспечение прямой секретности (Perfect Forward Secrecy) с использованием ephemeral Diffie-Hellman. Применение в защищенных каналах передачи данных (HTTPS, FTPS, WebSocket Secure), уязвимости и современные требования к конфигурации.

1. ОБЩАЯ ХАРАКТЕРИСТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ»

Самостоятельная работа студентов (далее — СРС) является неотъемлемой составляющей образовательного процесса в Университете и является обязательной для каждого студента. Основная цель СРС — освоение в полном объеме образовательной программы и последовательное формирование компетенций эффективной самостоятельной профессиональной (практической и научно-теоретической) деятельности.

Самостоятельная работа конкретна по своей предметной направленности и сопровождается непрерывным контролем и оценкой ее результатов.

Количество часов, отводимое на самостоятельную работу, определяется учебным планом направления подготовки 15.04.04.

Содержательно самостоятельная работа студентов определяется ФГОС ВО направления подготовки 15.04.04, программой и учебно-методическим комплексом дисциплины «Информационная безопасность и защита данных».

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей дисциплины «Информационная безопасность и защита данных», объема часов на ее изучение, вида заданий для СРС, индивидуальных возможностей студентов и условий учебной деятельности.

Формы самостоятельной работы студентов определяются содержанием дисциплины «Информационная безопасность и защита данных», степенью подготовленности студентов. Они могут быть тесно связаны с теоретическим курсом и иметь учебный или учебно-исследовательский характер. Форму самостоятельной работы студентов определяют кафедра ИСЭА при разработке программы дисциплины «Информационная безопасность и защита данных».

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

СРС, не предусмотренная образовательной программой, учебным планом и учебно-методическими материалами, раскрывающими и конкретизирующими их содержание, осуществляется студентами инициативно, с целью реализации собственных учебных и научных интересов.

В учебном процессе выделяют аудиторную и внеаудиторную самостоятельную работу.

Аудиторная самостоятельная работа по дисциплине «Информационная безопасность и защита данных» выполняется на учебных занятиях (лекциях, практических, лабораторных занятиях и консультациях) под руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов выполняется во внеаудиторное время по заданию и при методическом руководстве и контроле преподавателя, но без его непосредственного участия. СРС включает в себя:

- подготовку к аудиторным занятиям (лекционным и практическим) и выполнение соответствующих заданий;
- работу над отдельными темами учебных дисциплин (модулей) в соответствии с учебно-тематическими планами;
- выполнение контрольных работ;
- подготовку ко всем видам промежуточных и итоговых контрольных испытаний.

1.1. Подготовка к лекциям

Главное в период подготовки к лекционным занятиям — научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Слушание и запись лекций — сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, их конспектирование

помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим студентом. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях.

Конспект лекций лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

1.2. Подготовка к практическим занятиям

Подготовку к каждому практическому занятию студент должен начать с ознакомления с методическими указаниями, которые включают содержание работы. Тщательное продумывание и изучение вопросов основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений студенту необходимо самостоятельно выбрать тему доклада по проблеме и по возможности подготовить по нему презентацию.

Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или

письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы семинара, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

В зависимости от содержания и количества отведенного времени на изучение каждой темы практическое занятие может состоять из четырех-пяти частей:

1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/или выступление с презентациями по выбранной проблеме.
3. Обсуждение выступлений по теме — дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания.
5. Подведение итогов занятия.

Первая часть — обсуждение теоретических вопросов — проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний студентов. Примерная продолжительность — до 15 минут. Вторая часть — выступление студентов с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов практического занятия. Обязательный элемент доклада — представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность — 20-25 минут. После докладов следует их обсуждение — дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность — до 15-20 минут. Если программой предусмотрено выполнение практического задания в рамках конкретной темы, то преподавателями определяется его содержание и дается время на его выполнение, а затем идет обсуждение результатов. Подведением итогов заканчивается практическое занятие.

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-

методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

1.3. Самостоятельное изучение материала тем

Конспект — наиболее совершенная и наиболее сложная форма записи. Слово «конспект» происходит от латинского «conspectus», что означает «обзор, изложение». В правильно составленном конспекте обычно выделено самое основное в изучаемом тексте, сосредоточено внимание на наиболее существенном, в кратких и четких формулировках обобщены важные теоретические положения.

Конспект представляет собой относительно подробное, последовательное изложение содержания прочитанного. На первых порах целесообразно в записях ближе держаться тексту, прибегая зачастую к прямому цитированию автора. В дальнейшем, по мере выработки навыков конспектирования, записи будут носить более свободный и сжатый характер.

Конспект книги обычно ведется в тетради. В самом начале конспекта указывается фамилия автора, полное название произведения, издательство, год и место издания. При цитировании обязательная ссылка на страницу книги. Если цитата взята из собрания сочинений, то необходимо указать соответствующий том. Следует помнить, что четкая ссылка на источник — непереносимое правило конспектирования. Если конспектируется статья, то указывается, где и когда она была напечатана.

Конспект подразделяется на части в соответствии с заранее продуманным планом. Пункты плана записываются в тексте или на полях конспекта. Писать его рекомендуется четко и разборчиво, так как небрежная запись с течением времени становится малопонятной для ее автора. Существует правило: конспект, составленный для себя, должен быть по возможности написан так, чтобы его легко прочитал и кто-либо другой.

Формы конспекта могут быть разными и зависят от его целевого назначения (изучение материала в целом или под определенным углом зрения, подготовка к докладу, выступлению на занятии и т.д.), а также от характера произведения (монография, статья, документ и т.п.). Если речь идет просто об изложении содержания работы, текст конспекта может быть сплошным, с выделением особо важных положений подчеркиванием или различными значками.

В случае, когда не ограничиваются переложением содержания, а фиксируют в конспекте и свои собственные суждения по данному вопросу или дополняют конспект соответствующими материалами их других источников, следует отводить место для такого рода записей. Рекомендуется разделить страницы тетради пополам по вертикали и в левой части вести конспект произведения, а в правой свои дополнительные записи, совмещая их по содержанию.

Конспектирование в большей мере, чем другие виды записей, помогает вырабатывать навыки правильного изложения в письменной форме важные теоретических и практических вопросов, умение четко их формулировать и ясно излагать своими словами.

Таким образом, составление конспекта требует вдумчивой работы, затраты времени и труда. Зато во время конспектирования приобретаются знания, создается фонд записей.

Конспект может быть текстуальным или тематическим. В текстуальном конспекте сохраняется логика и структура изучаемого произведения, а запись ведется в соответствии с расположением материала в книге. За основу тематического конспекта берется не план произведения, а содержание какой-либо темы или проблемы.

Текстуальный конспект желательно начинать после того, как вся книга прочитана и продумана, но это, к сожалению, не всегда возможно. В первую очередь

необходимо составить план произведения письменно или мысленно, поскольку в соответствии с этим планом строится дальнейшая работа. Конспект включает в себя тезисы, которые составляют его основу. Но, в отличие от тезисов, конспект содержит краткую запись не только выводов, но и доказательств, вплоть до фактического материала. Иначе говоря, конспект — это расширенные тезисы, дополненные рассуждениями и доказательствами, мыслями и соображениями составителя записи.

Как правило, конспект включает в себя и выписки, но в него могут войти отдельные места, цитируемые дословно, а также факты, примеры, цифры, таблицы и схемы, взятые из книги. Следует помнить, что работа над конспектом только тогда будет творческой, когда она не ограничена текстом изучаемого произведения. Нужно дополнять конспект данными из других источников.

В конспекте необходимо выделять отдельные места текста в зависимости от их значимости. Можно пользоваться различными способами: подчеркиваниями, вопросительными и восклицательными знаками, репликами, краткими оценками, писать на полях своих конспектов слова: «важно», «очень важно», «верно», «характерно».

В конспект могут помещаться диаграммы, схемы, таблицы, которые придадут ему наглядность.

Составлению тематического конспекта предшествует тщательное изучение всей литературы, подобранной для раскрытия данной темы. Бывает, что какая-либо тема рассматривается в нескольких главах или в разных местах книги. А в конспекте весь материал, относящийся к теме, будет сосредоточен в одном месте. В плане конспекта рекомендуется делать пометки, к каким источникам (вплоть до страницы) придется обратиться для раскрытия вопросов. Тематический конспект составляется обычно для того, чтобы глубже изучить определенный вопрос, подготовиться к докладу, лекции или выступлению на семинарском занятии. Такой конспект по содержанию приближается к реферату, докладу по избранной теме, особенно если включает и собственный вклад в изучение проблемы.

1.4. Подготовка к экзамену

Экзаменационная сессия — очень тяжелый период работы для студентов и ответственный труд для преподавателей. Главная задача экзаменов — проверка качества усвоения содержания дисциплины.

На основе такой проверки оценивается учебная работа не только студентов, но и преподавателей: по результатам экзаменов можно судить и о качестве всего учебного процесса. При подготовке к экзамену студенты повторяют материал курсов, которые они слушали и изучали в течение семестра, обобщают полученные знания, выделяют главное в предмете, воспроизводят общую картину для того, чтобы яснее понять связь между отдельными элементами дисциплины.

При подготовке к экзаменам основное направление дают программы курса и конспект, которые указывают, что в курсе наиболее важно. Основной материал должен прорабатываться по учебнику, поскольку конспекта недостаточно для изучения дисциплины. Учебник должен быть проработан в течение семестра, а перед экзаменом важно сосредоточить внимание на основных, наиболее сложных разделах. Подготовку по каждому разделу следует заканчивать восстановлением в памяти его краткого содержания в логической последовательности.

До экзамена обычно проводится консультация, но она не может возместить отсутствия систематической работы в течение семестра и помочь за несколько часов освоить материал, требующийся к экзамену. На консультации студент получает лишь ответы на трудные или оставшиеся неясными вопросы. Польза от консультации будет только в том случае, если студент до нее проработает весь материал. Надо учиться задавать вопросы, выработать привычку пользоваться справочниками, энциклопедиями, а не быть на иждивении у преподавателей, который не всегда может тут же, «с ходу» назвать какой-либо факт, имя, событие. На экзамене нужно показать не только знание предмета, но и умение логически связно построить устный ответ.

Получив билет, надо вдуматься в поставленные вопросы для того, чтобы правильно понять их. Нередко студент отвечает не на тот вопрос, который поставлен, или в простом вопросе ищет скрытого смысла. Не поняв вопроса и не обдумав план ответа, не следует начинать писать. Конспект своего ответа надо рассматривать как

план краткого сообщения на данную тему и составлять ответ нужно кратко. При этом необходимо показать умение выражать мысль четко и доходчиво.

Отвечать нужно спокойно, четко, продуманно, без торопливости, придерживаясь записи своего ответа. На экзаменах студент показывает не только свои знания, но и учится владеть собой. После ответа на билет могут следовать вопросы, которые имеют целью выяснить понимание других разделов курса, не вошедших в билет. Как правило, на них можно ответить кратко, достаточно показать знание сути вопроса. Часто студенты при ответе на дополнительные вопросы проявляют поспешность: не поняв смысла того, что у них спрашивают, начинают отвечать и нередко говорят не по сути.

Следует помнить, что необходимым условием правильного режима работы в период экзаменационной сессии является нормальный сон, поэтому подготовка к экзаменам не должна быть в ущерб сну. Установлено, что сильное эмоциональное напряжение во время экзаменов неблагоприятно отражается на нервной системе и многие студенты из-за волнений не спят ночи перед экзаменами. Обычно в сессию студенту не до болезни, так как весь организм озабочен одним — сдать экзамены. Но это еще не значит, что последствия неправильно организованного труда и чрезмерной занятости не скажутся потом. Поэтому каждый студент помнить о важности рационального распорядка рабочего дня и о своевременности снятия или уменьшения умственного напряжения.

2. СРЕДСТВА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ОБУЧАЮЩИХСЯ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ»

Вопросы для собеседования

Тема 1. Криптографические методы защиты данных

1. Что такое криптография и какие цели она преследует?
2. Какие виды криптографических методов существуют?
3. Что такое симметричное шифрование и как оно работает?

4. Какие алгоритмы симметричного шифрования существуют?
5. Что такое асимметричное шифрование и как оно работает?
6. Какие алгоритмы асимметричного шифрования существуют?
7. Что такое хэширование и для чего оно используется?
8. Какие алгоритмы хэширования существуют?
9. Что такое цифровая подпись и для чего она используется?
10. Какие алгоритмы цифровой подписи существуют?
11. Что такое электронная подпись и как она работает?
12. Какие алгоритмы электронной подписи существуют?
13. Что такое PKI и как оно помогает защитить данные?
14. Какие проблемы могут возникнуть при использовании криптографических методов защиты данных?
15. Что такое квантовая криптография и как она отличается от классической криптографии?
16. Какие алгоритмы квантовой криптографии существуют?
17. Какие преимущества и недостатки имеет квантовая криптография?
18. Какие тенденции развития криптографических методов защиты данных можно выделить?
19. Какие новые угрозы могут появиться в связи с развитием криптографических методов защиты данных?
20. Какие рекомендации можно дать для обеспечения безопасности при использовании криптографических методов защиты данных?

Тема 2. Защита аппаратных средств АСУ ТП

1. Что такое АСУ ТП и какие аппаратные средства используются в ней?
2. Какие угрозы могут возникнуть для аппаратных средств АСУ ТП?
3. Какие методы защиты аппаратных средств АСУ ТП существуют?
4. Что такое защита от электромагнитных помех и как она реализуется в АСУ ТП?
5. Как обеспечивается защита от перегрузок и коротких замыканий в аппаратных средствах АСУ ТП?

6. Что такое защита от несанкционированного доступа и как она реализуется в АСУ ТП?
7. Какие методы криптографической защиты используются для аппаратных средств АСУ ТП?
8. Какие протоколы безопасности используются для защиты аппаратных средств АСУ ТП?
9. Что такое физическая защита аппаратных средств АСУ ТП и как она реализуется?
10. Какие методы мониторинга и контроля используются для защиты аппаратных средств АСУ ТП?
11. Как обеспечить защиту аппаратных средств АСУ ТП от вирусов и злонамеренных программ?
12. Как обеспечить защиту аппаратных средств АСУ ТП от физических воздействий, таких как пожары или наводки?
13. Какие методы резервирования и восстановления используются для обеспечения надежности аппаратных средств АСУ ТП?
14. Какие меры безопасности следует принимать при установке и настройке аппаратных средств АСУ ТП?
15. Как обеспечить защиту аппаратных средств АСУ ТП при удаленном доступе?
16. Какие методы защиты используются для защиты каналов связи между аппаратными средствами АСУ ТП?
17. Какие проблемы могут возникнуть при использовании сторонних устройств и оборудования в АСУ ТП?
18. Какие требования к безопасности должны быть учтены при разработке аппаратных средств АСУ ТП?
19. Какие новые угрозы могут появиться в связи с развитием технологий и оборудования для АСУ ТП?
20. Какие рекомендации можно дать для обеспечения безопасности при использовании аппаратных средств АСУ ТП?

Тема 3. Защита программного обеспечения АСУ ТП

1. Что такое программное обеспечение АСУ ТП и как оно используется?
2. Какие угрозы могут возникнуть для программного обеспечения АСУ ТП?
3. Какие методы защиты программного обеспечения АСУ ТП существуют?
4. Что такое защита от вредоносных программ и как она реализуется в программном обеспечении АСУ ТП?
5. Как обеспечивается защита от несанкционированного доступа к программному обеспечению АСУ ТП?
6. Какие методы криптографической защиты используются для программного обеспечения АСУ ТП?
7. Какие протоколы безопасности используются для защиты программного обеспечения АСУ ТП?
8. Что такое физическая защита программного обеспечения АСУ ТП и как она реализуется?
9. Какие методы мониторинга и контроля используются для защиты программного обеспечения АСУ ТП?
10. Как обеспечить защиту программного обеспечения АСУ ТП при удаленном доступе?
11. Какие методы защиты используются для защиты каналов связи между программным обеспечением АСУ ТП?
12. Какие проблемы могут возникнуть при использовании стороннего программного обеспечения в АСУ ТП?
13. Какие требования к безопасности должны быть учтены при разработке программного обеспечения АСУ ТП?
14. Какие новые угрозы могут появиться в связи с развитием технологий и программного обеспечения для АСУ ТП?
15. Какие рекомендации можно дать для обеспечения безопасности при использовании программного обеспечения АСУ ТП?

Тема 4. Защита сетевых ресурсов АСУ ТП

1. Что такое сетевые ресурсы АСУ ТП и как они используются?

2. Какие угрозы могут возникнуть для сетевых ресурсов АСУ ТП?
3. Какие методы защиты сетевых ресурсов АСУ ТП существуют?
4. Как обеспечивается защита от взлома сетевых ресурсов АСУ ТП?
5. Как обеспечивается защита от несанкционированного доступа к сетевым ресурсам АСУ ТП?
6. Какие методы криптографической защиты используются для сетевых ресурсов АСУ ТП?
7. Какие протоколы безопасности используются для защиты сетевых ресурсов АСУ ТП?
8. Что такое физическая защита сетевых ресурсов АСУ ТП и как она реализуется?
9. Какие методы мониторинга и контроля используются для защиты сетевых ресурсов АСУ ТП?
10. Как обеспечить защиту сетевых ресурсов АСУ ТП при удаленном доступе?
11. Какие методы защиты используются для защиты каналов связи между сетевыми ресурсами АСУ ТП?
12. Какие проблемы могут возникнуть при использовании сторонних сетевых ресурсов в АСУ ТП?
13. Какие требования к безопасности должны быть учтены при разработке сетевых ресурсов АСУ ТП?
14. Какие новые угрозы могут появиться в связи с развитием технологий и сетевых ресурсов для АСУ ТП?
15. Какие рекомендации можно дать для обеспечения безопасности при использовании сетевых ресурсов АСУ ТП?

Тема 5. Организационные основы защиты информации в автоматизированных системах на предприятии

1. Какие организационные меры по защите информации существуют в автоматизированных системах на предприятии?
2. Какова роль руководства предприятия в обеспечении безопасности информации в АС?

3. Какие процедуры должны быть введены на предприятии для обеспечения безопасности информации в АС?
4. Как обучение персонала влияет на защиту информации в АС?
5. Какие политики и правила должны быть установлены для обеспечения безопасности информации в АС?
6. Какие меры предосторожности должны быть приняты для защиты информации от утечки?
7. Какие методы аутентификации и авторизации используются для защиты информации в АС?
8. Какова роль службы безопасности информации в автоматизированных системах на предприятии?
9. Какие инструменты используются для обнаружения и предотвращения угроз безопасности информации в АС?
10. Какие меры должны быть приняты для обеспечения защиты от внешних угроз, таких как хакерские атаки?
11. Какие меры должны быть приняты для обеспечения защиты от внутренних угроз, таких как неправомерные действия сотрудников?
12. Какие методы шифрования используются для защиты информации в АС?
13. Какова роль системы контроля доступа в обеспечении безопасности информации в АС?
14. Какие меры должны быть приняты для обеспечения защиты от утечки информации через социальную инженерию?
15. Какие меры должны быть приняты для обеспечения безопасности информации при использовании облачных технологий в АС?

Тема 6. Сопровождение комплексной системы защиты информации в автоматизированной системе

1. Какие шаги необходимо предпринять для сопровождения комплексной системы защиты информации в АС?
2. Какие изменения могут возникнуть в комплексной системе защиты информации в процессе ее сопровождения?

3. Какова роль сотрудников службы поддержки в сопровождении комплексной системы защиты информации в АС?
4. Какие инструменты и технологии используются для сопровождения комплексной системы защиты информации в АС?
5. Какие меры предосторожности должны быть приняты при сопровождении комплексной системы защиты информации в АС?
6. Какова роль аудиторов в сопровождении комплексной системы защиты информации в АС?
7. Какие процессы и процедуры должны быть введены для эффективного сопровождения комплексной системы защиты информации в АС?
8. Какие проблемы могут возникнуть при сопровождении комплексной системы защиты информации в АС и как их можно решить?
9. Какие меры должны быть приняты для обеспечения надежности и стабильности комплексной системы защиты информации в АС?
10. Какие изменения в законодательстве могут повлиять на сопровождение комплексной системы защиты информации в АС?
11. Как оценить эффективность сопровождения комплексной системы защиты информации в АС?
12. Какова роль технических специалистов в сопровождении комплексной системы защиты информации в АС?
13. Какие меры должны быть приняты для обеспечения безопасности при обновлении и модернизации комплексной системы защиты информации в АС?
14. Какие преимущества может дать эффективное сопровождение комплексной системы защиты информации в АС для предприятия?
15. Какие меры должны быть приняты для обеспечения безопасности при эксплуатации комплексной системы защиты информации в АС?

Тема 7. Анализ угроз сохранности информации

1. Какие методы используются для анализа угроз сохранности информации?
2. Какие виды угроз могут возникнуть при хранении и передаче конфиденциальной информации?

3. Каковы последствия нарушения сохранности информации для организации?
4. Какие меры безопасности должны быть приняты для защиты от угроз сохранности информации?
5. Какие технологии и программные средства могут помочь в анализе угроз сохранности информации?
6. Какие методы используются для оценки рисков сохранности информации?
7. Каковы основные принципы организации системы защиты информации от угроз сохранности?
8. Какие уязвимости могут быть обнаружены в системе защиты информации?
9. Какие методы используются для мониторинга и обнаружения угроз сохранности информации?
10. Какие меры должны быть приняты для защиты от внутренних угроз сохранности информации?
11. Какие меры должны быть приняты для защиты от внешних угроз сохранности информации?
12. Какие меры должны быть приняты для защиты от угроз, связанных с техническими отказами?
13. Какие меры должны быть приняты для защиты от угроз, связанных с человеческим фактором?
14. Какие меры должны быть приняты для защиты от угроз, связанных с социальной инженерией?
15. Какова роль аудиторов в анализе угроз сохранности информации?

Тема 8. Аттестация объектов информатизации по требованиям безопасности информации

1. Что такое аттестация объектов информатизации по требованиям безопасности информации?
2. Какие объекты информатизации могут быть аттестованы?
3. Какие документы необходимо предоставить для проведения аттестации объектов информатизации?

4. Какие требования безопасности информации обычно проверяются при аттестации объектов информатизации?
5. Кто проводит аттестацию объектов информатизации по требованиям безопасности информации?
6. Какие этапы включает процесс аттестации объектов информатизации по требованиям безопасности информации?
7. Какова стоимость проведения аттестации объектов информатизации по требованиям безопасности информации?
8. Какие меры должны быть приняты, если объект информатизации не прошел аттестацию по требованиям безопасности информации?
9. Какие преимущества получает организация после аттестации объекта информатизации по требованиям безопасности информации?
10. Какие сроки действия имеет аттестация объекта информатизации по требованиям безопасности информации?
11. Какие изменения могут повлиять на результаты аттестации объекта информатизации по требованиям безопасности информации?
12. Какие рекомендации могут быть даны организации после проведения аттестации объекта информатизации по требованиям безопасности информации?
13. Какие дополнительные меры безопасности могут быть предложены организации после проведения аттестации объекта информатизации по требованиям безопасности информации?
14. Какие последствия могут возникнуть, если организация не проводит аттестацию своих объектов информатизации по требованиям безопасности информации?
15. Какие требования безопасности информации могут быть изменены в процессе аттестации объекта информатизации?

Критерии оценивания компетенций

Оценка «зачтено» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и

приемами их выполнения. Допускаются некоторые неточности, недостаточно правильные формулировки в изложении программного материала, затруднения при выполнении практических работ.

Оценка «не зачтено» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические задания.

Вопросы к экзамену

Вопросы (задача, задание) для проверки уровня обученности

1. Что такое информационная безопасность и зачем она необходима?
2. Какие виды угроз существуют для информационной безопасности?
3. Какие основные принципы безопасности следует учитывать при работе с информацией?
4. Какие методы шифрования существуют и как они помогают защитить данные?
5. Что такое вирус и какие виды вирусов существуют?
6. Какие меры безопасности следует принимать при работе с электронной почтой?
7. Что такое фишинг и как его предотвратить?
8. Какие меры безопасности следует принимать при работе с социальными сетями?
9. Что такое бэкдор и как он может быть использован злоумышленниками?
10. Какие меры безопасности следует принимать при работе с Wi-Fi сетями?
11. Что такое скимминг и как его предотвратить?
12. Какие меры безопасности следует принимать при работе с общественными компьютерами?
13. Что такое многократная аутентификация и как она помогает защитить данные?

14. Какие меры безопасности следует принимать при работе с облачными сервисами?
15. Что такое ботнет и как он может быть использован злоумышленниками?
16. Какие меры безопасности следует принимать при работе с онлайн-магазинами?
17. Что такое кейлоггер и как его предотвратить?
18. Какие меры безопасности следует принимать при работе с онлайн-играми?
19. Что такое скам и как его предотвратить?
20. Какие меры безопасности следует принимать при работе с удаленным доступом к компьютеру?
21. Что такое VPN и как он помогает защитить данные?
22. Какие меры безопасности следует принимать при работе с веб-камерой?
23. Что такое хакер и какой виды хакеров существуют?
24. Какие меры безопасности следует принимать при работе с социальными инженерами?
25. Что такое защита периметра и как она помогает защитить данные?
26. Какие меры безопасности следует принимать при работе с общественными Wi-Fi сетями?
27. Что такое троянский конь и как его предотвратить?
28. Какие меры безопасности следует принимать при работе с онлайн-финансами?
29. Что такое фаервол и как он помогает защитить данные?
30. Какие меры безопасности следует принимать при работе с онлайн-сервисами?
31. Что такое вредоносное ПО и как его предотвратить?
32. Какие меры безопасности следует принимать при работе с общественными USB-портами?
33. Что такое аутентификация и как она помогает защитить данные?
34. Какие меры безопасности следует принимать при работе с онлайн-кассами?
35. Что такое сканеры уязвимостей и как они помогают защитить данные?

36. Какие меры безопасности следует принимать при работе с онлайн-оплатой?
37. Что такое атака типа "человек посередине" и как ее предотвратить?
38. Какие меры безопасности следует принимать при работе с облачными вычислениями?
39. Что такое биометрическая аутентификация и как она помогает защитить данные?
40. Какие меры безопасности следует принимать при работе с онлайн-голосованием?
41. Что такое защита от внутренних угроз и как ее обеспечить?
42. Какие меры безопасности следует принимать при работе с онлайн-конференциями?
43. Что такое DLP и как он помогает защитить данные?
44. Какие меры безопасности следует принимать при работе с онлайн-сервисами хранения паролей?
45. Что такое защита от DDoS-атак и как ее обеспечить?

Критерии оценивания компетенций

Оценка **«отлично»** выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

Оценка **«хорошо»** выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

Оценка **«удовлетворительно»** выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности,

недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

Оценка «**неудовлетворительно**» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

3. ОТЧЕТНОСТЬ ПО ДИСЦИПЛИНЕ

Успеваемость студентов по дисциплине оценивается в ходе текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация в форме экзамена предусматривает проведение обязательной экзаменационной процедуры.

Для студентов очно-заочной формы обучения рейтинговая оценка знаний не предусмотрена

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Перечень основной литературы:

1. Алексеев, А.П.; Многоуровневая защита информации Электронный ресурс : монография / А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2017. - 128 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-904029-72-2

2. Бурькова, Е. В; Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова ; Министерство образования и науки Российской Федерации ; Оренбургский государственный университет ; Кафедра вычислительной техники и защиты информации. - Оренбург : Оренбургский государственный университет, 2017. - 158 с. : табл., схем. - <http://biblioclub.ru/>. - Библиогр. в кн. - ISBN 978-5-7410-1697-8

Перечень дополнительной литературы:

1. Горев, А.И.; Обработка и защита информации в компьютерных системах Электронный ресурс : практическое пособие / А.А. Симаков / А.И. Горев. - Омск : Омская академия МВД России, 2016. - 88 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-88651-642-5

2. Шаньгин, В. Ф; Информационная безопасность и защита информации Электронный ресурс / В. Ф. Шаньгин. - Информационная безопасность и защита информации, 2019-04-19. - Саратов : Профобразование, 2017. - 702 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-4488-0070-2