

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 «Аутентификация в киберфизических системах»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль)
«Информационная безопасность киберфизических систем»

Ставрополь
2026

Содержание

ВВЕДЕНИЕ	3
Лабораторная работа №1	6
Лабораторная работа №2	21
Лабораторная работа №3	41
Лабораторная работа №4	55
Лабораторная работа №5	70
Лабораторная работа №6	83
Лабораторная работа №7	96
Лабораторная работа №8	108
Лабораторная работа №9	121

ВВЕДЕНИЕ

1. Цели и задачи освоения дисциплины:

Целью изучения дисциплины «Аутентификация в киберфизических системах» является развитие и формирование у студентов профессиональных компетенций, необходимых для решения теоретических и практических задач в области аутентификации и защиты доступа в киберфизических системах, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность».

Задачи освоения дисциплины «Аутентификация в киберфизических системах»:

- изучить теоретические основы аутентификации, включая модели, протоколы и алгоритмы;
- освоить методы и технологии аутентификации применительно к киберфизическим системам (КФС);
- сформировать навыки анализа уязвимостей механизмов аутентификации в КФС;
- овладеть практическими инструментами и средствами реализации аутентификации в распределённых и гетерогенных средах;
- научиться оценивать эффективность и надёжность механизмов аутентификации с учётом специфики КФС (ограниченные ресурсы устройств, жёсткие требования к задержкам и т.д.);
- совершенствовать умения и навыки с учётом специализации профессиональной деятельности;
- повысить профессиональный уровень в рамках имеющейся квалификации.

Дисциплина «Аутентификация в киберфизических системах» (Б1.В.08) относится к дисциплинам части, формируемой участниками образовательных отношений. Её освоение происходит в 3 семестре.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-2 Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	ИД-1 ПК-2 Осуществляет анализ особенностей проектирования и реализации политики безопасности вычислительных сетей в киберфизических системах	Перечисляет и кратко характеризует действующие нормативные акты, методические документы, регламентирующие проектирование политик безопасности для вычислительных сетей в составе киберфизических систем
	ИД-2 ПК-2 Проектирует и реализует политики безопасности вычислительных сетей в киберфизических системах	Разрабатывает концептуальную модель политики безопасности для заданной вычислительной сети киберфизической системы (определяет субъекты, объекты, правила разграничения доступа)
	ИД-4 К-2 формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизических системах	Разрабатывает комплект документов политики безопасности для заданной киберфизической системы (положение о политике безопасности, матрица доступа, правила разграничения доступа, инструкции для администраторов)
ПК-3. Способен	ИД-1 ПК-3 состав, порядок	Перечисляет и кратко

разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	характеризует основные нормативные документы, определяющие требования к системе управления информационной безопасностью киберфизических систем
	ИД-2 ПК-3 анализ уязвимости и построение модели угроз для киберфизических систем	Составляет проект документа с предложениями по совершенствованию системы управления информационной безопасностью в соответствии с принятыми в организации шаблонами
	ИД-6 ПК-3 Формализует методологию разработки предложений при совершенствовании системы управления информационной безопасностью киберфизических систем	Готовит развёрнутое заключение по итогам анализа системы управления информационной безопасностью, содержащее ранжированный перечень предложений с указанием ожидаемых результатов и сроков реализации

Тема 1: Методология аутентификации в киберфизических системах

Лабораторная работа №1

Реализация процедуры групповой подписи BBS на билинейных отображениях.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.

6. Операционная система специального назначения «Astra Linux Special Edition».

7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».

8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.

9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 XP».

10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».

11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».

12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».

13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».

14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».

15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.

16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».

17. Программное изделие «Kaspersky Endpoint Security for Aurora».

18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.

19. Программное комплекс Acronis Backup & Recovery.

20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.

21. Программное обеспечение Oracle Identity Access Management Suite.

22. Программное обеспечение SafeNet Authentication Service.

23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.

24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».

25. Программный комплекс «InfoWatch Traffic Monitor».

26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.

27. Программный комплекс защиты информации от НСД «Страж 1.1».

28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.

29. Программный комплекс обнаружения вторжений «Ребус-СОВ».

30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»
31. Специальное программное обеспечение «АС «ГРИФ».
32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».
2. Аппаратно-программный комплекс шифрования «Континент».
3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95.
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1.
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

1. Повторить теоретический материал лекций по темам «Особенности объектов цифровой индустрии как киберфизических объектов», «Организация безопасной эксплуатации объектов цифровой индустрии».
2. Изучить теоретический материал данного занятия.
3. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Какие новые области охватывают киберфизические системы?
2. Назовите технологии киберфизического преобразования.
3. В чем сущность трансформации технологического процесса?
4. Дайте характеристику этапам передового производства.
5. Что выступает в качестве среды взаимодействия в киберфизических системах?
6. Что такое киберфизический объект?
7. Что такое киберфизическая система?
8. Каковы признаки киберфизической системы?
9. Назовите элементы логической структуры киберфизической системы.
10. Свойства киберфизической системы.
11. Применение киберфизических систем.
12. Что является основной задачей при обеспечении кибербезопасности?
13. Назовите компоненты безопасности цифрового производства.
14. Какие функции контроля обеспечивает блок обеспечения безопасности?
15. Перечислите общий набор этапов функционирования блока безопасности.
16. Что входит в состав цифрового производства?
17. Сущность архитектуры цифрового производства.
18. В чем состоит метод представления производства?
19. Что такое модель умного оборудования?
20. Перечислите умные средства автоматизации когнитивной обработки.
21. Задачи магазина промышленных приложений.
22. Что входит в систему обеспечения кибербезопасности?
23. Что нужно для успешного функционирования системы обеспечения кибербезопасности?
24. Дайте характеристику доверенной среде на базе виртуализации.
25. Как реализуется безопасность внутренних и внешних коммуникаций?
26. Что такое программноконфигурируемые сети?
27. Преимущества программно-конфигурируемых сетей при построении систем управления кибербезопасностью?
28. Состав блок управления ПКС.
29. Перечислите возможные подходы к оценке безопасности киберфизических систем.
30. Какой должна быть оценка для всех типов систем и применима как для централизованных энергетических комплексов?
31. Какой подход может быть использован к оценке безопасности киберфизических систем?
32. В чем сущность показателя самоподобия?
33. Дайте характеристику понятию киберустойчивость.

34. От чего зависит оценка устойчивости системы в условиях деструктивных целенаправленных внешних атак?
35. Какие подходы могут быть применяться для оценки устойчивости КФС?
36. Дайте характеристику надежностного подхода для оценки устойчивости КФС.
37. Дайте характеристику подходу самоподобия для оценки устойчивости КФС.
38. Какая основная проблема реализации надежностного подхода?
39. Какие виды избыточности можно выделить в модели системы на основе функциональных графов и маршрутов?
40. В чем сущность параметрической избыточности?
41. В чем сущность функциональной избыточности?
42. В чем сущность структурной избыточности?
43. Как представляется оценка устойчивости КФС?
44. Каков механизм выработки компенсирующего воздействия в КФС?
45. В чем сущность гомеостатической концепции представления КФС?
46. Дайте характеристику архитектуры блока управления безопасностью КФС.
47. Что включает в себя блок управления безопасностью?
48. Что включает в себя блок мониторинга?
49. Какие функции выполняет блок генерации компенсирующего воздействия?
50. В чем сущность технология гомеостаза?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование схемы групповой подписи BBS	- 80 мин
2. Синтез групповой подписи BBS	- 80 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.
Всего	- 180 мин

Основные теоретические сведения

Схема групповой подписи BBS

Параметрами схемы BBS являются:

G_1, G_2 — мультипликативные циклические группы простого порядка p ;

G_2 — мультипликативная группа, имеющая подгруппу порядка p ;

ψ — гомоморфизм из группы G_2 в группу G_1 ;

$g_2 \in G_2$ — элемент порядка p ;

$\langle g_1 \rangle = G_1$ — образующая группы G_1 , такая что $\psi(g_2) = g_1$.

Элементы g_1 и g_2 выбирают случайным образом во время инициализации системы. Выбором элемента g_2 обычно ограничивают рассмотрение группы G_2 до ее циклической подгруппы $\langle g_2 \rangle$ порядка p . При этом имеет место изоморфизм $\langle g_2 \rangle \cong G_1$. Безопасность схемы BBS основана на следующих теоретико-числовых предположениях.

1. Задача q -SDH (strong Diffie–Hellman, сильное предположение Диффи–Хеллмана) заключается в том, чтобы по входному кортежу $(g_1, g_2, g_2^\gamma, g_2^{(\gamma^2)}, \dots, g_2^{(\gamma^q)})$, где $g_1 = \psi(g_2)$, найти пару $(g_1^{1/(\gamma+x)}, x)$, где $x \xleftarrow{R} \mathbb{Z}_p$.

Алгоритм A обладает эффектом ε при решении задачи q -SDH в (G_1, G_2) , если выполняется неравенство $\Pr\{A(g_1, g_2, g_2^\gamma, g_2^{(\gamma^2)}, \dots, g_2^{(\gamma^q)}) = (g_1^{1/(\gamma+x)}, x)\} \geq \varepsilon$. Здесь вероятность $\Pr$ определяется случайным выбором образующей $g_2 \in G_2$ (при этом $g_1 = \psi(g_2)$), элемента $\gamma \in \mathbb{Z}_p^*$ и случайных битов в алгоритме A .

Говорят, что в (G_1, G_2) действует предположение (q, t, ε) -SDH, если не существует алгоритма, время работы которого не больше t и который при этом обладает эффектом не менее ε при решении задачи q -SDH в (G_1, G_2) . При $q = 1$ говорят просто о предположении SDH).

2. Задача DL (decision linear, задача линейного распознавания) в группе G_1 заключается в том, чтобы по заданным $uv, h, u^a, v^b, h^c \in G_1$ выработать выходное значение «да», если $a + b = c$, и «нет» в противном случае. Здесь u, v, h — произвольные образующие группы G_1 , $a, b, c \xleftarrow{R} \mathbb{Z}_p$.

Эффект алгоритма A , решающего задачу DL в группе G_1 , задается как:

$$\begin{aligned} Adv_A^{linear} = & |\Pr\{A(u, v, h, u^a, v^b, h^{a+b}) = \text{"да"}: u, v, h \xleftarrow{R} G_1, a, b \xleftarrow{R} \mathbb{Z}_p\} - \\ & - \Pr\{A(u, v, h, u^a, v^b, \eta) = \text{"да"}: u, v, h, \eta \xleftarrow{R} G_1, a, b \xleftarrow{R} \mathbb{Z}_p\}|. \end{aligned}$$

Говорят, что алгоритм $A(t, \varepsilon)$ решает задачу DL в группе G_1 , если время его работы не превосходит t , а эффект Adv_A^{linear} составляет как минимум ε . В группе G_1 справедливо предположение (t, ε) -DL (или просто предположение DL), если не существует алгоритма, (t, ε) -решающего задачу DL в группе G_1 .

На сложности задачи DL основана безопасность схемы линейного шифрования (linear encryption, LE), которая естественным образом расширяет схему шифрования Эль-Гамала и в отличие от нее остается безопасной даже в тех группах, для которых существует эффективный алгоритм решения задачи распознавания DDH.

Доказывающий:

4) выбирает «маскирующие» значения: $r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \xleftarrow{R} \mathbb{Z}_p$;

5) вычисляет значения:

$$R_1 \leftarrow u^{r_\alpha}; R_2 \leftarrow v^{r_\beta}; R_3 \leftarrow e(T_3, g_2)^{r_x} e(h, w)^{-r_\alpha - r_\beta} e(h, g_2)^{-r_{\delta_1} - r_{\delta_2}};$$
$$R_4 \leftarrow T_1^{r_x} u^{-r_{\delta_1}}; R_5 \leftarrow T_2^{r_x} v^{-r_{\delta_2}};$$

6) отправляет проверяющему набор $(T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$.

Этап 2. *Проверяющий* отправляет в качестве запроса случайно выбранное число $c \xleftarrow{R} \mathbb{Z}_p$.

Этап 3. *Доказывающий* вычисляет и отправляет проверяющему значения. Параметрами схемы являются:

- ключ зашифрования: элементы $u, v, h \in G_1$;
- ключ расшифрования: экспоненты $x, y \in \mathbb{Z}_p$ такие что $u^x = v^y = h$;
- сообщение, которое нужно зашифровать: $M \in G_1$.

Зашифрование: выбрать случайные значения $a, b \xleftarrow{R} \mathbb{Z}_p$ и вычислить результат — тройку $(T_1, T_2, T_3) \leftarrow (u^a, v^b, Mh^{a+b})$.

Расшифрование: вычислить $M \leftarrow T_3 / (T_1^x T_2^y)$.

В предположении DL схема линейного шифрования является стойкой по отношению к атакам на основе подобранных открытых текстов

В схеме BBS используется следующий протокол, позволяющий провести аутентификацию субъекта, доказывающего знание пары $(A, x) \in G_1 \times \mathbb{Z}_p$, такой, что $A^{x+\gamma} = g_1$. Эта пара удовлетворяет условию $e(A, wg_2^x) = e(g_1, g_2)$, где $w = g_2^\gamma$.

Этап 1. *Доказывающий:*

1) выбирает случайные элементы $\alpha, \beta \xleftarrow{R} \mathbb{Z}_p$;

2) выполняет линейное зашифрование элемента A :

$$T_1 \leftarrow u^\alpha; T_2 \leftarrow v^\beta; T_3 \leftarrow A \cdot h^{\alpha+\beta};$$

3) вычисляет вспомогательные значения: $\delta_1 \leftarrow x\alpha \pmod{p}$; $\delta_2 \leftarrow x\beta \pmod{p}$.

Далее стороны предпринимают действия для доказательства знания значений $(\alpha, \beta, x, \delta_1, \delta_2)$, удовлетворяющих соотношениям:

$$u^\alpha = T_1; v^\beta = T_2; e(T_3, g_2)^x e(h, w)^{-\alpha-\beta} e(h, g_2)^{-\delta_1-\delta_2} =$$
$$= e(g_1, g_2) / e(T_3, w); T_1^x u^{-\delta_1} = 1; T_2^x v^{-\delta_2} = 1,$$

для чего:

Доказывающий:

4) выбирает «маскирующие» значения: $r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \xleftarrow{R} \mathbb{Z}_p$;

5) вычисляет значения:

$$R_1 \leftarrow u^{r_\alpha}; R_2 \leftarrow v^{r_\beta}; R_3 \leftarrow e(T_3, g_2)^{r_x} e(h, w)^{-r_\alpha - r_\beta} e(h, g_2)^{-r_{\delta_1} - r_{\delta_2}};$$
$$R_4 \leftarrow T_1^{r_x} u^{-r_{\delta_1}}; R_5 \leftarrow T_2^{r_x} v^{-r_{\delta_2}};$$

6) отправляет проверяющему набор $(T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$.

Этап 2. *Проверяющий* отправляет в качестве запроса случайно выбранное число $c \xleftarrow{R} \mathbb{Z}_p$.

Этап 3. *Доказывающий* вычисляет и отправляет проверяющему зна-

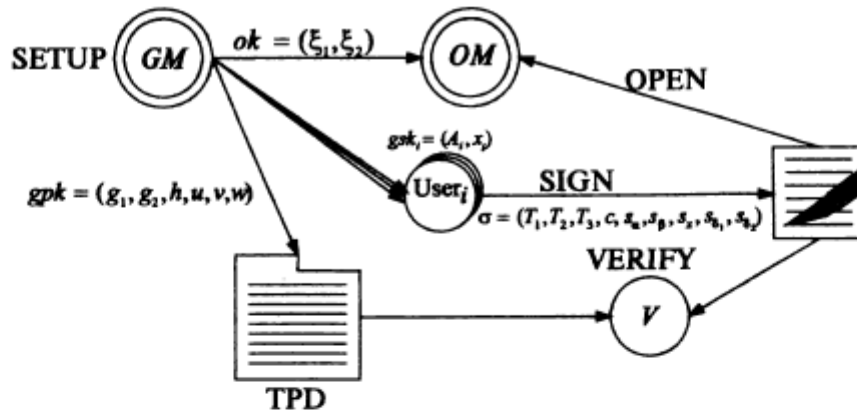


Рис. 1. Схема групповой подписи BBS

чения:

$$s_\alpha \leftarrow r_\alpha + c\alpha; \quad s_\beta \leftarrow r_\beta + c\beta; \quad s_x \leftarrow r_x + cx;$$

$$s_{\delta_1} \leftarrow r_{\delta_1} + c\delta_1; \quad s_{\delta_2} \leftarrow r_{\delta_2} + c\delta_2.$$

Этап 4. Проверяющий убеждается в выполнении равенств

$$u^{s_\alpha} \stackrel{?}{=} T_1^c R_1; \quad v^{s_\beta} \stackrel{?}{=} T_2^c R_2;$$

$$e(T_3, g_2)^{s_x} e(h, w)^{-s_\alpha - s_\beta} e(h, g_2)^{-s_{\delta_1} - s_{\delta_2}} \stackrel{?}{=} (e(g_1, g_2)/e(T_3, w))^c R_3;$$

$$T_1^{s_x} u^{-s_{\delta_1}} \stackrel{?}{=} R_4; \quad T_2^{s_x} v^{-s_{\delta_2}} \stackrel{?}{=} R_5$$

и принимает доказательство, если все эти условия выполнены.

В результате выполнения протокола субъект, проходящий аутентификацию, доказывает проверяющему знание пары SDH с нулевым разглашением в условиях предположения DL

На основе протокола доказательства с нулевым разглашением знания пары SDH можно построить схему групповой подписи. В ней используются:

- предположение q -SDH для групп (G_1, G_2) ;
- предположение DL для группы G_1 ;
- хеш-функция $H: \{0, 1\}^* \rightarrow \mathbb{Z}_p$.

Инициализация схемы производится координатором группы GM . Он генерирует все используемые в схеме ключи и раздает менеджеру OM и пользователям их закрытые ключи (рис. 1).

Генерация ключей:

Вход: n — число членов группы.

Выход: gpk — открытый ключ группы; ok — личный ключ раскрывающего менеджера группы; gsk_i , $1 \leq i \leq n$, — личные ключи членов группы.

1. Выбрать случайную образующую g_2 группы G_2 и вычислить $g_1 \leftarrow \psi(g_2)$.

2. Выбрать элементы $h \xleftarrow{R} G_1 \setminus \{1_{G_1}\}$, $\xi_1, \xi_2 \xleftarrow{R} \mathbb{Z}_p^*$ и вычислить $u, v \in G_1$, такие, что $u^{\xi_1} = v^{\xi_2} = h$.

3. Выбрать $ik = \gamma \xleftarrow{R} \mathbb{Z}_p^*$ и вычислить $w \leftarrow g_2^\gamma$.

4. Используя ключ γ , сгенерировать для каждого члена группы пару (A_i, x_i) : выбрать $x_i \xleftarrow{R} \mathbb{Z}_p^*$ и вычислить $A_i \leftarrow g_1^{1/(\gamma+x_i)} \in G_1$.

5. Результат: $gpk \leftarrow (g_1, g_2, h, u, v, w)$; $ok \leftarrow (\xi_1, \xi_2)$; $gsk_i \leftarrow (A_i, x_i)$, где $1 \leq i \leq n$.

Знать значение γ разрешается только координатору GM , выпускающему закрытые ключи.

Идея групповой подписи BBS состоит в доказательстве знания решения задачи q -SDH, т.е. знания такой пары (A, x) , что $\langle A^{x+\gamma} \rangle = G_1$.

Чтобы предоставить (другому) менеджеру OM возможность раскрывать подпись (идентифицировать подписавшего), доказательство должно быть только отчасти с нулевым разглашением: менеджер OM должен уметь восстанавливать значение A , используя специальную «лазейку».

Поэтому, чтобы подписать сообщение, член группы сначала зашифровывает сертификат A алгоритмом линейного шифрования LE на открытом ключе шифрования (u, v, h) менеджера OM , а затем предоставляет доказательство с нулевым разглашением того, что открытый текст на самом деле содержит сертификат A , для которого он знает соответствующее значение x . При этом пара значений (ξ_1, ξ_2) , которой обладает менеджер OM , является закрытым ключом расшифрования, что дает ему возможность раскрывать групповую подпись.

Формирование подписи:

Вход: $gpk = (g_1, g_2, h, u, v, w)$ — открытый ключ группы; $gsk_i = (A_i, x_i)$ — личный закрытый ключ члена группы, который хочет подписать сообщение; $M = \{0, 1\}^*$ — подписываемое сообщение.

Выход: σ — групповая подпись сообщения M .

1. Вычислить значения $T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5$, как определено на первом этапе протокола SDH (шаги 1–5).

2. Используя хэш-функцию, вычислить запрос

$$c \leftarrow H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in \mathbb{Z}_p.$$

3. Используя c , вычислить значения $s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2}$, как определено на третьем этапе протокола SDH.

4. Сформировать подпись: $\sigma \leftarrow (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$.

Проверка подписи:

Вход: $gpk = (g_1, g_2, h, u, v, w)$ — открытый ключ группы; $M = \{0, 1\}^*$ — подписанное сообщение; $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ — групповая подпись.

Выход: заключение о корректности подписи.

1. Вычислить значения:

$$\begin{aligned} \tilde{R}_1 &\leftarrow u^{s_\alpha} T_1^{-c}; & \tilde{R}_2 &\leftarrow v^{s_\beta} T_2^{-c}; \\ \tilde{R}_3 &\leftarrow e(T_3, g_2)^{s_x} e(h, w)^{-s_\alpha - s_\beta} e(h, g_2)^{-s_{\delta_1} - s_{\delta_2}} (e(T_3, w) / e(g_1, g_2))^c; \\ \tilde{R}_4 &\leftarrow T_1^{s_x} u^{-s_{\delta_1}}; & \tilde{R}_5 &\leftarrow T_2^{s_x} v^{-s_{\delta_2}}. \end{aligned}$$

2. Выполнить проверку: $c \stackrel{?}{=} H(M, T_1, T_2, T_3, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5)$.

3. Если условие на шаге 2 выполнено, то подпись принимается, иначе результат: подпись неверна.

Раскрытие подписи:

Вход: $gpk = (g_1, g_2, h, u, v, w)$ — открытый ключ группы; $ok = (\xi_1, \xi_2)$ — закрытый ключ раскрывающего менеджера OM ; $M = \{0, 1\}^*$ — подписанное сообщение; $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ — групповая подпись. Опционально: $\{A_i\}$ — элементы закрытых ключей членов группы.

Выход: i — индекс пользователя, подписавшего сообщение.

1. Выполнить проверку правильности подписи σ сообщения M .
2. Рассмотреть первые три элемента (T_1, T_2, T_3) подписи как шифртекст, полученный с помощью алгоритма линейного шифрования, и восстановить A , следуя алгоритму расшифрования схемы LE: $A \leftarrow T_3 / (T_1^{\xi_1} T_2^{\xi_2})$.
3. Если менеджер OM знает элементы $\{A_i\}$ — часть закрытого ключа каждого члена группы, то он может выяснить индекс i пользователя, соответствующий идентификатору A , восстановленному из подписи.

Схема BBS является безопасной в рамках модели со случайным оракулом, но не удовлетворяет требованию полной анонимности, так как для скрытия идентификатора участника в ней используется семантически безопасная схема линейного шифрования LE, стойкая только по отношению к атакам на основе подобранных открытых текстов. Свойство семантической безопасности подразумевает пассивного нарушителя, который самостоятельно выбирает открытые тексты, зашифровывает их на известном открытом ключе и анализирует получившиеся шифртексты, в то время как требование полной анонимности подразумевает доступ нарушителя к раскрывающему оракулу, то есть к расшифровывающему оракулу линейной схемы шифрования.

На практике для обеспечения безопасности схемы шифрования требования семантической безопасности обычно недостаточно, поскольку такие схемы не противостоят активным нарушителям, имеющим доступ к расшифровывающему оракулу. Таким образом, в схеме BBS используется теоретически потенциально слабое линейное шифрование, что не позволяет доказать ее безопасность по всем требованиям, предъявляемым моделью безопасности статической групповой подписи BMW.

Схема BBS не обеспечивает и невозможность ложного обвинения участника группы в формировании некоторой подписи, так как подразумевает, что личный закрытый ключ этого участника известен не только его владельцу, но и координатору GM , который может выпустить подпись на чужом закрытом ключе. Это также является серьезным недостатком, для преодоления которого требуются дополнительные организационные меры, к примеру, присвоение координатору группы статуса доверенного субъекта.

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.
2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.
3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

1. Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.
3. А.И. Астайкина. Саратов: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.А. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.: Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей: учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск: Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -
3. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/> -
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>
5. Интернет портал Защита-информации.SU <http://www.iso27000.ru/>
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>
7. Консорциум сетевых электронных библиотек ЭБС «Лань» <https://e.lanbook.com/>
8. ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/> -
9. ЭБС IPR SMART <https://www.iprbookshop.ru/>
10. ЭБС Znanium <https://znanium.com/>
11. ЭБС «Юрайт» <http://www.biblio-online.ru>
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

1. Используя теоретический материал, представленный в методических рекомендациях, изучить схему реализации групповой подписи BBS. Особое внимание обратить на параметры схемы и ее описание, на процедуры обеспечения безопасности схемы, содержание основных этапов реализации групповой подписи BBS (90 минут).

2. В соответствии с вариантами лабораторной работы №1 осуществить зашифровывание, описанных в теоретическом материале методических рекомендаций. На основе протокола доказательства с нулевым разглашением построить схему групповой подписи (90 минут.).

№ Варианта	Число членов группы
1.	2
2.	3
3.	4
4.	5
5.	6
6.	7
7.	8
8.	9
9.	10
10.	11
11.	12
12.	13
13.	14
14.	15
15.	16

Цель работы в реализации всей схемы состоит в доказательстве решения задачи q-SDH, **т.е. знания такой пары (A, x) , что $\langle A^{x+\gamma} \rangle = G_1$.**

Результаты лабораторной работы занести в отчет

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

- формулировку темы лабораторной работы;
- формулировку цели и решаемых в ходе лабораторной работы задач;
- порядок выполнения лабораторной работы с учетом достижения целевой установки;
- выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

Лабораторная работа №2

Реализация процедуры групповой подписи на базе динамической схемы ED-BBS.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».
8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.
9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 XP».

10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».

11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».

12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».

13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».

14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».

15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.

16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».

17. Программное изделие «Kaspersky Endpoint Security for Aurora».

18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.

19. Программное комплекс Acronis Backup & Recovery.

20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.

21. Программное обеспечение Oracle Identity Access Management Suite.

22. Программное обеспечение SafeNet Authentication Service.

23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.

24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».

25. Программный комплекс «InfoWatch Traffic Monitor».

26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.

27. Программный комплекс защиты информации от НСД «Страж 1.1».

28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.

29. Программный комплекс обнаружения вторжений «Ребус-СОВ».

30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»

31. Специальное программное обеспечение «АС «ГРИФ».

32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».

2. Аппаратно-программный комплекс шифрования «Континент».

3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95».
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1».
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

1. Повторить теоретический материал лекций по темам «Особенности объектов цифровой индустрии как киберфизических объектов», «Организация безопасной эксплуатации объектов цифровой индустрии».
2. Изучить теоретический материал данного занятия.
3. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Что нужно для успешного функционирования системы обеспечения кибербезопасности?
2. Дайте характеристику доверенной среде на базе виртуализации.
3. Как реализуется безопасность внутренних и внешних коммуникаций?
4. Что такое программноконфигурируемые сети?

5. Преимущества программно-конфигурируемых сетей при построении систем управления кибербезопасностью?
6. Состав блок управления ПКС.
7. Перечислите возможные подходы к оценке безопасности киберфизических систем.
8. Какой должна быть оценка для всех типов систем и применима как для централизованных энергетических комплексов?
9. Какой подход может быть использован к оценке безопасности киберфизических систем?
10. В чем сущность показателя самоподобия?
11. Дайте характеристику понятию киберустойчивость.
12. От чего зависит оценка устойчивости системы в условиях деструктивных целенаправленных внешних атак?
13. Какие подходы могут быть применяться для оценки устойчивости КФС?
14. Дайте характеристику надежностного подхода для оценки устойчивости КФС.
15. Дайте характеристику подходу самоподобия для оценки устойчивости КФС.
16. Какая основная проблема реализации надежностного подхода?
17. Какие виды избыточности можно выделить в модели системы на основе функциональных графов и маршрутов?
18. В чем сущность параметрической избыточности?
19. В чем сущность функциональной избыточности?
20. В чем сущность структурной избыточности?
21. Как представляется оценка устойчивости КФС?
22. Каков механизм выработки компенсирующего воздействия в КФС?
23. В чем сущность гомеостатической концепции представления КФС?
24. Дайте характеристику архитектуры блока управления безопасностью КФС.
25. Что включает в себя блок управления безопасностью?
26. Что включает в себя блок мониторинга?
27. Какие функции выполняет блок генерации компенсирующего воздействия?
28. В чем сущность технология гомеостаза?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование схемы групповой подписи на базе динамической схемы ED-BBS	- 80 мин
2. Синтез групповой подписи на базе динамической схемы ED-BBS.BBS	- 60 мин

3. Тестирование по теме 1	20 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.
Всего	- 180 мин

Основные теоретические сведения

Динамическая схема ED-BBS

Оригинальная схема групповой подписи BBS является статической, так как на вход алгоритму формирования начальных параметров и основных ключей подписи подается число участников формируемой группы. Это не позволяет добавлять в группу новых членов после того, как она сформирована, и ограничивает сферу применения подписи.

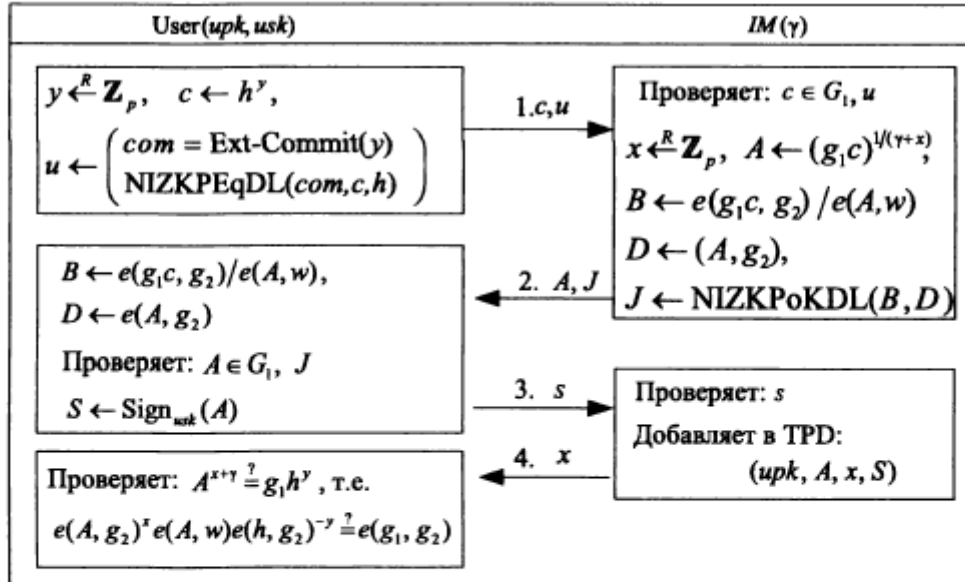


Рис. 1. Протокол добавления участника в группу

Для введения в схему BBS процедуры добавления участника необходимо дополнить членский сертификат (личный ключ) еще одним значением и модифицировать доказательство знания решения задачи q -SDH, с тем чтобы включить в него доказательство знания третьего значения личного ключа члена группы.

Протокол добавления участника в группу выполняется субъектом, желающим вступить в группу, и выпускающим менеджером этой группы (рис 1.). В результате успешного выполнения протокола субъект становится обладателем членского сертификата (A, x, y) , удовлетворяющего условию $A^{x+\gamma} = g_1 h^y$, а менеджер IM — части (A, x) этого сертификата, что позволяет ему в дальнейшем отслеживать подписи, генерируемые членом группы. Таким образом, значение y формируется на стороне субъекта и остается известным только ему.

Здесь Ext-Commit (extractable commitment) — обязательство относительно заданной информации, обладающее «лазейкой» для ее раскрытия.

Участник-кандидат связывает себя обязательством относительно выбранного им значения y . Это дает ему возможность доказать менеджеру IM , что он знает значение $y = d \log_h(c)$, а также не позволит в дальнейшем его изменить. Такое обязательство должно формироваться в соответствии с безусловно связывающей (perfectly binding) и вычислительно скрывающей (computationally hiding) схемой обязательств с «лазейкой».

«Лазейка» в протоколе добавления участника не должна быть известна ни одной стороне и используется только при доказательстве отслеживаемости и нефабрикуемости.

$\text{NIZKPEqDL}(com, c, h)$ — это неинтерактивное доказательство с нулевым разглашением (non-interactive zero knowledge proof of equality of discrete logarithms) того, что дискретный логарифм от c по основанию h равен связанному значением com значению y в модели со случайным оракулом. Сто-

ит заметить, что такое доказательство членства совместно с раскрываемым обязательством Ext-Commit является доказательством знания: субъект, сформировавший значение c , обязательно знает y .

$\text{NIZKPoKDL}(B, D)$ — это неинтерактивное доказательство с нулевым разглашением (non-interactive zero knowledge proof of knowledge of discrete logarithm) знания дискретного логарифма B по основанию D в модели со случайным оракулом.

В протоколе добавления участника все значения итогового сертификата (A, x, y) определяются на шагах 1 и 2.

На шаге 1:

- 1) участник-кандидат выбирает случайным образом y , вычисляет c и предоставляет доказательство знания выбранного значения;
- 2) менеджер IM использует значение c для формирования частей (A, x) сертификата.

На шаге 2 менеджер IM раскрывает кандидату первую часть A сгенерированного сертификата и предоставляет в значении $\text{NIZKPoKDL}(B, D)$ доказательство того, что он знает вторую его часть, так как $d \log_B D = x$.

На шаге 3 кандидат убеждается в том, что менеджер IM честен с ним, то есть передал верное значение A первой части сертификата, которая была получена с использованием значения c и для которой IM знает «ответную» часть x . Выполнение этой проверки гарантирует свойство нефабрикуемости. Далее кандидат подписывает полученное значение, после чего IM раскрывает вторую часть x сертификата.

На последнем шаге кандидат проверяет, удовлетворяет ли его новый сертификат основному условию $A^{x+y} = g_1 h^y$.

Подпись $\text{Sign}_{usk}(A)$ гарантирует, что кандидат владеет полным сертификатом, первой частью которого является значение A . Это позволит в дальнейшем при раскрытии подписи доказать, что вычисленное на ее основе значение A принадлежит данному участнику, от чего он, в свою очередь, не сможет отказаться. Для этого используется стандартное окружение инфраструктуры открытых ключей. Предполагается, что у каждого субъекта, желающего вступить в группу, есть личный ключ, который связан с открытым ключом, заверенным удостоверяющим центром. Окружение инфраструктуры открытых ключей отделено от окружения группы, благодаря чему в группу не нужно включать полностью доверенные субъекты, что обеспечивает свойства неотказуемости (члена группы от сертификата) и нефабрикуемости: даже если уполномоченные субъекты IM и OM будут скомпрометированы, они не смогут обвинить некоторого члена группы в том, что он сформировал подпись, которую на самом деле он не выпускал.

том, что он сформировал подпись, которую на самом деле он не выпускал.

Чтобы обеспечить полную анонимность получившейся динамической схемы групповой подписи, предлагается заменить используемую в базовой схеме BBS схему линейного шифрования части сертификата члена группы на схему, стойкую по отношению к атакам на основе адаптивно подобранных шифртекстов, что позволяет доказать безопасность предложенной схемы в соответствии с требованиями динамической модели BSZ.

Для этих целей предлагается использовать линейную схему LCS шифрования Крамера–Шоупа.

Линейная схема шифрования Крамера–Шоупа для схемы BBS KeyGen — генерация ключей:

- 1) выбрать случайные образующие: $u_1, u_2, u_3 \xleftarrow{R} G_1$;
- 2) выбрать случайные показатели степеней: $x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3 \xleftarrow{R} \mathbb{Z}_p$;
- 3) вычислить:

$$\begin{aligned} b_1 &\leftarrow u_1^{x_1} u_3^{x_3}, & c_1 &\leftarrow u_1^{y_1} u_3^{y_3}, & d_1 &\leftarrow u_1^{z_1} u_3^{z_3}, \\ b_2 &\leftarrow u_2^{x_2} u_3^{x_3}, & c_2 &\leftarrow u_1^{y_2} u_3^{y_3}, & d_2 &\leftarrow u_2^{z_2} u_3^{z_3}, \end{aligned}$$

- 4) выбрать случайную хэш-функцию: $H \xleftarrow{R} HF'$, где HF' — семейство универсальных односторонних хэш-функций, действующих из G^4 в $\mathbb{Z}_p$;

5) результат:

ключ зашифрования: $pk \leftarrow (u_1, u_2, u_3, b_1, b_2, c_1, c_2, d_1, d_2, H) \in G_1^9 \times HF'$;

ключ расшифрования: $sk \leftarrow (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3) \in \mathbb{Z}_p^9$.

$Encr_{pk}(M)$ — шифрование сообщения $M \in G_1$:

- 1) выбрать случайные показатели $r_1, r_2 \xleftarrow{R} \mathbb{Z}_p$;
- 2) вычислить шифртекст $CT = (T_1, T_2, T_3, T_4, T_5) \in G_1^5$, где $T_1 \leftarrow u_1^{r_1}$; $T_2 \leftarrow u_2^{r_2}$; $T_3 \leftarrow u_3^{r_1+r_2}$; $T_4 \leftarrow M d_1^{r_1} d_2^{r_2}$; $\alpha \leftarrow H(T_1, T_2, T_3, T_4)$; $T_5 \leftarrow (b_1 c_1^\alpha)^{r_1} (b_2 c_2^\alpha)^{r_2}$.

$Decr_{sk}(CT, pk)$ — расшифрование:

- 1) вычислить: $\alpha \leftarrow H(T_1, T_2, T_3, T_4)$;
- 2) проверить условие: $T_1^{x_1+y_1\alpha} T_2^{x_2+y_2\alpha} T_3^{x_3+y_3\alpha} \stackrel{?}{=} T_5$. Если оно не выполняется, то расшифрование отклоняется;

- 3) вычислить открытый текст: $M \leftarrow T_4 / (T_1^{z_1} T_2^{z_2} T_3^{z_3})$.

Корректность: если ключи и шифртекст сформированы в соответствии с приведенными алгоритмами, то проверка в алгоритме расшифрования будет успешна, так как

$$\begin{aligned} T_1^{x_1+y_1\alpha} T_2^{x_2+y_2\alpha} T_3^{x_3+y_3\alpha} &= (u_1^{r_1})^{x_1+y_1\alpha} (u_2^{r_2})^{x_2+y_2\alpha} (u_3^{r_1+r_2})^{x_3+y_3\alpha} = \\ &= (u_1^{x_1+y_1\alpha} u_3^{x_3+y_3\alpha})^{r_1} (u_2^{x_2+y_2\alpha} u_3^{x_3+y_3\alpha})^{r_2} = (b_1 c_1^\alpha)^{r_1} (b_2 c_2^\alpha)^{r_2} = T_5, \end{aligned}$$

что и требуется. В результате расшифрования получится правильное открытое сообщение M , так как

$$\begin{aligned} T_4 / (T_1^{z_1} T_2^{z_2} T_3^{z_3}) &= T_4 / (u_1^{r_1 z_1} u_2^{r_2 z_2} u_3^{(r_1+r_2)z_3}) = \\ &= T_4 / ((u_1^{z_1} u_3^{z_3})^{r_1} (u_2^{z_2} u_3^{z_3})^{r_2}) = (M d_1^{r_1} d_2^{r_2}) / (d_1^{r_1} d_2^{r_2}) = M. \end{aligned}$$

Схема LCS является безопасной по отношению к атакам на основе адаптивно подобранных шифртекстов, если HF' — семейство безопасных од-

носторонних хэш-функций и в группе G_1 выполняется линейное предположение DL.

В схеме LCS большая часть компонентов закрытого и открытого ключей, а также элемент T_5 шифртекста нужны, по сути, только для доказательства, что сформированный шифртекст является допустимым, то есть что первые три компонента шифртекста образуют линейный кортеж.

При включении схемы LCS в состав сложных протоколов групповой подписи вместо такого способа проверки шифртекста можно использовать бездиалоговое доказательство с нулевым разглашением NIZKPoLT(T_1, T_2, T_3, T_4) (non-interactive zero knowledge proof of linear tuple) того, что первые три элемента шифртекста (T_1, T_2, T_3) образуют линейный кортеж.

В такой модифицированной схеме LCS ключи зашифрования $pk \leftarrow (u_1, u_2, u_3, d_1, d_2, H) \in G_1^5 \times HF'$ и расшифрования $sk \leftarrow (z_1, z_2, z_3) \in \mathbb{Z}_p^3$ формируются аналогично этим же значениям в схеме LCS. Шифртекст в этом случае выглядит так: $CT = (T_1, T_2, T_3, T_4, \text{NIZKPoLT}(T_1, T_2, T_3, T_4))$, а расшифрование начинается с проверки доказательства NIZKPoLT(T_1, T_2, T_3, T_4). Такая модифицированная линейная схема LCS остается стойкой по отношению к атакам на основе адаптивно подобранных шифртекстов.

В представленной динамической схеме ED-BBS процедура формирования подписи — это доказательство знания такой тройки $(A, x, y) \in G_1 \times \mathbb{Z}_p^2$, что $A^{x+\gamma} = g_1 h^y$. При этом выполняется условие

$$e(A, g_2)^x e(A, w) e(h, g_2)^{-y} = e(g_1, g_2).$$

Открытый ключ группы в схеме ED-BBS имеет вид $gpk = (g_1, h, u_1, u_2, u_3, d_1, d_2, g_2, w)$, где $\langle g_1 \rangle = G_1$ — циклическая группа порядка p ; $g_2 \in G_2$ — элемент порядка p группы G_2 , $g_1 = \psi(g_2)$; $h, u_1, u_2, u_3 \stackrel{R}{\leftarrow} G_1$; $d_1, d_2 \in G_1$ — часть открытого ключа в линейной схеме шифрования Крамера–Шоупа, $d_1 \leftarrow u_1^{\xi_1} u_3^{\xi_3}$; $d_2 \leftarrow u_2^{\xi_2} u_3^{\xi_3}$ для некоторых $\xi_1, \xi_2, \xi_3 \stackrel{R}{\leftarrow} \mathbb{Z}_p$; $w = g_2^\gamma$, где $\gamma \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$ — личный закрытый ключ менеджера, выпускающего ключи.

Членский сертификат (личный ключ подписи) i -го пользователя имеет вид $gsk_i = (A_i, x_i, y_i) \in G_1 \times \mathbb{Z}_p^2$, где $A_i^{x_i+\gamma} = g_1 h^{y_i}$.

Динамическая схема ED-BBS [6]

Формирование подписи (выполняется членом группы).

1. Выбрать случайные элементы $r_1, r_2 \stackrel{R}{\leftarrow} \mathbb{Z}_p$.
2. Зашифровать элемент A_i по модифицированной схеме LCS: $T_1 \leftarrow u_1^{r_1}$; $T_2 \leftarrow u_2^{r_2}$; $T_3 \leftarrow u_3^{r_1+r_2}$; $T_4 \leftarrow A_i d_1^{r_1} d_2^{r_2}$.
3. Вычислить вспомогательные значения: $\delta_1 \leftarrow r_1 x_i$; $\delta_2 \leftarrow r_2 x_i$.
4. Выбрать случайные «маскирующие» значения $t_{r_1}, t_{r_2}, t_{\delta_1}, t_{\delta_2}, t_x, t_y$ из $\mathbb{Z}_p$.
5. Вычислить значения:

$$\begin{aligned} R_1 &\leftarrow u_1^{t_{r_1}}; & R_2 &\leftarrow u_2^{t_{r_2}}; & R_3 &\leftarrow u_3^{t_{r_1}+t_{r_2}}; & R_5 &\leftarrow T_1^{t_x} u_1^{-t_{\delta_1}}; \\ R_4 &\leftarrow \frac{e(T_4, g_2)^{t_x} e(h, g_2)^{-t_y}}{e(d_1, w)^{t_{r_1}} e(d_2, w)^{t_{r_2}} e(d_1, g_2)^{t_{\delta_1}} e(d_2, g_2)^{t_{\delta_2}}}; & R_6 &\leftarrow T_2^{t_x} u_2^{-t_{\delta_2}}. \end{aligned}$$

6. Используя хэш-функцию H , вычислить значение $c \leftarrow H(M, T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6) \in \mathbb{Z}_p$.

7. Вычислить значения

$$\begin{aligned} s_{r_1} &\leftarrow t_{r_1+cr_1}; & s_{r_2} &\leftarrow t_{r_2+cr_2}; & s_{\delta_1} &\leftarrow t_{\delta_1+c\delta_1}; & s_{\delta_2} &\leftarrow t_{\delta_2+c\delta_2}; \\ s_x &\leftarrow t_x + cx_i; & s_y &\leftarrow t_y + cy_i. \end{aligned}$$

Подпись $\sigma \leftarrow (T_1, T_2, T_3, T_4, c, s_{r_1}, s_{r_2}, s_{\delta_1}, s_{\delta_2}, s_x, s_y)$.

Проверка подписи.

1. Вычислить значения:

$$\begin{aligned} \tilde{R}_1 &\leftarrow u_1^{s_{r_1}} T_1^{-c}; & \tilde{R}_2 &\leftarrow u_2^{s_{r_2}} T_2^{-c}; & \tilde{R}_3 &\leftarrow u_3^{s_{r_1}+s_{r_2}} T_3^{-c}; \\ \tilde{R}_5 &\leftarrow T_1^{s_x} u_1^{-s_{\delta_1}}; & \tilde{R}_6 &\leftarrow T_2^{s_y} u_2^{-s_{\delta_2}}; \\ \tilde{R}_4 &\leftarrow \frac{e(T_4, g_2)^{s_x} e(h, g_2)^{-s_y}}{e(d_1, w)^{s_{r_1}} e(d_2, w)^{s_{r_2}} e(d_1, g_2)^{s_{\delta_1}} e(d_2, g_2)^{s_{\delta_2}}} \left(\frac{e(T_4, w)}{e(g_1, g_2)} \right)^c. \end{aligned}$$

2. Выполнить проверку: $c \stackrel{?}{=} H(M, T_1, T_2, T_3, T_4, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5, \tilde{R}_6)$.

3. Если проверяемое условие выполнено, то подпись принимается, в противном случае результат: подпись неверна.

Раскрытие подписи.

1. Выполнить проверку подписи σ .

2. Рассмотреть первые четыре элемента (T_1, T_2, T_3, T_4) подписи как первую часть шифртекста, полученного с помощью модифицированной схемы шифрования LCS, и восстановить A_i , следуя алгоритму расшифрования этой схемы: если проверка подписи прошла успешно, то вычислить $A_i \leftarrow T_4 / (T_1^{\xi_1} T_2^{\xi_2} T_3^{\xi_3})$, иначе признать подпись недействительной.

3. Если раскрывающий менеджер знает элементы $\{A_i\}$ закрытых ключей членов группы, то он может определить индекс i пользователя, соответствующий восстановленному из подписи идентификатору A_i .

4. Сформировать доказательство того, что раскрытие проведено верно.

Раскрывающий менеджер должен доказать, что знает представление значения T_4/A_i в виде $T_1^{\xi_1} T_2^{\xi_2} T_3^{\xi_3}$, т.е. знает все компоненты своего личного ключа, такого что $d_1 = u_1^{\xi_1} u_3^{\xi_3}$, $d_2 = u_2^{\xi_2} u_3^{\xi_3}$. Если он может предоставить такое бездиалоговое доказательство с нулевым разглашением, то он правильно раскрыл данную подпись.

5. Для доказательства того, что названный i -й пользователь связан со значением A_i , используется подпись $S = \text{Sign}_{usk_i}(A_i)$, хранящаяся в базе данных членов группы.

Проверка правильности раскрытия подписи.

1. Проверить доказательство, предоставленное раскрывающим менеджером.

2. С помощью открытого ключа upk_i , заверенного подписью удостоверяющего центра, проверить подпись S раскрытого значения A_i , принадлежащего указанному раскрывающим менеджером члену группы с идентификатором i .

Шаги 4–7 формирования подписи представляют собой доказательство

знания значений $(r_1, r_2, \delta_1, \delta_2, x_i, y_i)$, удовлетворяющих соотношениям:

$$\begin{aligned} u_1^{r_1} &= T_1; \quad u_2^{r_2} = T_2; \quad u_3^{r_1+r_2} = T_3; \\ \frac{e(g_1, g_2)}{e(T_4, w)} &= \frac{e(T_4, g_2)^{x_i} e(h, g_2)^{-y_i}}{e(d_1, w)^{r_1} e(d_2, w)^{r_2} (d_1, g_2)^{\delta_1} \times e(d_2, g_2)^{\delta_2}}; \\ T_1^x u_1^{-\delta_1} &= 1; \quad T_2^x u_2^{-\delta_2} = 1. \end{aligned}$$

Эти условия определяются следующими требованиями:

1) необходимо доказать правильность формирования шифртекста в соответствии с модифицированной схемой LCS, а именно то, что первые три компонента шифртекста образуют правильный линейный кортеж $(u_1, u_2, u_3, u_1^{r_1}, u_2^{r_2}, u_3^{r_1+r_2})$, т.е. сформировать новый элемент $\text{NIZKPoLT}(T_1, T_2, T_3, T_4)$ шифртекста. Отсюда возникают первые три условия;

2) каждому открытому значению должно соответствовать по меньшей мере одно обязательство в доказательстве с нулевым разглашением [81]. Для T_1, T_2, T_3 такие соотношения очевидны, так как неизвестные проверяющему значения располагаются в показателях степеней. Получим такое соотношение для T_4 . Известно, что $A_i^{x_i+\gamma} = g_1 h^{y_i}$, при этом $A_i = T_4 d_1^{-r_1} d_2^{-r_2}$ и $w = g_2^\gamma$. Таким образом:

$$\begin{aligned} e(g_1, g_2) &= e(A_i^{x_i+\gamma} h^{-y_i}, g_2) = e(T_4^{x_i+\gamma} d_1^{-r_1(x_i+\gamma)} d_2^{-r_2(x_i+\gamma)}, g_2) e(h, g_2)^{-y_i} = \\ &= \frac{e(T_4, g_2)^{x_i+\gamma} e(h, g_2)^{-y_i}}{e(d_1, g_2)^{\delta_1} e(d_2, g_2)^{\delta_2} e(d_1, w)^{r_1} e(d_2, w)^{r_2}}, \end{aligned}$$

откуда и следует ограничение, накладываемое на T_4 . Если оно не выполняется, то при правильно сгенерированных параметрах это означает, что либо шифртекст по схеме LCS некорректен, либо пользователь, сформировавший этот шифртекст, не знает значение A_i подлинного сертификата. Дополнительное «связывание» T_4 с доказательством осуществляется при формировании запроса с помощью случайного оракула — на вход ему подается в том числе значение T_4 , чего требует модифицированная схема LCS;

3) необходимо доказать внутреннюю связь между значениями, знание которых доказывается. В данном случае взаимосвязаны только значения r_1, r_2, x_i и δ_1, δ_2 . Отсюда возникают последние два условия: $T_1^{x_i} u_1^{-\delta_1} = 1$, $T_2^{x_i} u_2^{-\delta_2} = 1$. Если какое-то из них не выполняется, то либо некорректно сформирован шифртекст, либо неправильно вычислены значения δ_1, δ_2 .

Таким образом, показав выполнение этих шести условий, доказывающий предоставит гарантии того, что он знает сертификат, верно сформировал каждое из четырех значений шифртекста, а также правильно вычислил вспомогательные значения, используемые в протоколе доказательства.

Корректность протокола обосновывается следующей цепочкой равенств:

$$\begin{aligned} u_1^{sr_1} &= u_1^{tr_1+cr_1} = u_1^{tr_1} (u_1^{r_1})^c = R_1 T_1^c; \\ u_2^{sr_2} &= u_2^{tr_2+cr_2} = u_2^{tr_2} (u_2^{r_2})^c = R_2 T_2^c; \\ u_3^{sr_1+sr_2} &= u_3^{tr_1+cr_1+tr_2+cr_2} = u_3^{tr_1+tr_2} (u_3^{r_1+r_2})^c = R_3 T_3^c; \end{aligned}$$

$$\begin{aligned}
& \frac{e(T_4, g_2)^{s_x} e(h, g_2)^{-s_y}}{e(d_1, w)^{s_{r_1}} e(d_2, w)^{s_{r_2}} e(d_1, g_2)^{s_{\delta_1}} e(d_2, g_2)^{s_{\delta_2}}} = \\
& = \frac{e(T_4, g_2)^{t_x} e(h, g_2)^{-t_y}}{e(d_1, w)^{t_{r_1}} e(d_2, w)^{t_{r_2}} e(d_1, g_2)^{t_{\delta_1}} e(d_2, g_2)^{t_{\delta_2}}}; \\
& \left(\frac{e(T_4, g_2)^{x_i} e(h, g_2)^{-y_i}}{e(d_1, w)^{r_1} e(d_2, w)^{r_2} e(d_1, g_2)^{\delta_1} e(d_2, g_2)^{\delta_2}} \right)^c = R_4 \left(\frac{e(g_1, g_2)}{e(T_4, w)} \right)^c; \\
& T_1^{s_x} u_1^{-s_{\delta_1}} = T_1^{t_x} u_1^{-t_{\delta_1}} T_1^x u_1^{-\delta_1} = R_6; \\
& T_2^{s_x} u_2^{-s_{\delta_2}} = T_2^{t_x} u_2^{-t_{\delta_2}} T_2^x u_2^{-\delta_2} = R_7.
\end{aligned}$$

Расширенная схема ED-BBS (extended dynamic BBS) обладает следующими свойствами : невозможность фальсификации, «строгая» невозможность ложного обвинения, устойчивость к сговору, несопоставимость подписей .

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.

Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.

E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.

Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред. А.И. Астайкина. Саратов: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.

Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.

Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.а. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.

Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.

Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.:Лаборатория знаний, 2020. — 482 с.

Ли, П. Архитектура интернета вещей / П. Ли ; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

Дубков, И. С. Решение практических задач на базе технологии интернета вещей : учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск : Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»

Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>

Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -

Официальный сайт Федеральной службы безопасности Российской

Федерации <http://www.fsb.ru/> -

Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>

Интернет портал Защита-информации.SU <http://www.iso27000.ru/>

Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>

Консорциум сетевых электронных библиотек ЭБС «Лань»
<https://e.lanbook.com/>

ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/>

ЭБС IPR SMART <https://www.iprbookshop.ru/>

ЭБС Znanium <https://znanium.com/>

ЭБС «Юрайт» <http://www.biblio-online.ru>

Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

Используя теоретический материал, представленный в методических рекомендациях, изучить процедуру реализации групповой подписи на базе динамической схемы ED-BBS. Особое внимание обратить на то, что оригинальная схема групповой подписи BBS является статической, так как на вход алгоритму формирования начальных параметров и основных ключей подписи подается число участников формируемой группы. Это не позволяет добавлять в группу новых членов после того, как она сформирована, и ограничивает сферу применения подписи. (90 минут).

В соответствии с вариантами лабораторной работы №1 осуществить добавление протоколе участника коммуникационного взаимодействия в соответствии с описанными в теоретическом материале. Для этих целей предлагается использовать линейную схему LCS шифрования Крамера-Шоупа. Синтез подписи реализовать с учетом описания процедур проверки и раскрытия подписи, а также проверки ее правильности (90 минут.).

№ Варианта	Число членов группы и число
------------	--------------------------------

	добавления участников
1.	2+1
2.	3+2
3.	4+3
4.	5+2
5.	6+4
6.	7+1
7.	8+2
8.	9+3
9.	10+4
10.	11+5
11.	12+1
12.	13+4
13.	14+2
14.	15+5
15.	16+3

Цель работы состоит в подтверждение выполнения всех шести условий, доказывающих гарантии того, что студент знает сертификат, верно сформировал каждое из четырех значений шифртекста, а также правильно вычислил вспомогательные значения, используемые в протоколе доказательства.

Результаты лабораторной работы занести в отчет

1. За 20 минут до окончания занятий проводится тестирование по теме №1. Вопросы тестирования охватывают теоретический материал, выданный на лекционных занятиях.

Перечень вопросов выносимый на процедуру тестирования.

1. Дайте характеристику понятию «Индустрия 4.0».
2. В чем особенность применения программно-аппаратного управления в современных условиях?
3. Что отличает «второй машинный век»?
4. Что такое Интернет вещей?
5. Какие новые области охватывают киберфизические системы?
6. Назовите технологии киберфизического преобразования.
7. В чем сущность трансформации технологического процесса?
8. Дайте характеристику этапам передового производства.
9. Что выступает в качестве среды взаимодействия в киберфизических системах?

10. Что такое киберфизический объект?
11. Что такое киберфизическая система?
12. Каковы признаки киберфизической системы?
13. Назовите элементы логической структуры киберфизической системы.
14. Свойства киберфизической системы.
15. Применение киберфизических систем.
16. Что является основной задачей при обеспечении кибербезопасности?
17. Назовите компоненты безопасности цифрового производства.
18. Какие функции контроля обеспечивает блок обеспечения безопасности?
19. Перечислите общий набор этапов функционирования блока безопасности.
20. Что входит в состав цифрового производства?
21. Сущность архитектуры цифрового производства.
22. В чем состоит метод представления производства?
23. Что такое модель умного оборудования?
24. Перечислите умные средства автоматизации когнитивной обработки.
25. Задачи магазина промышленных приложений.
26. Что входит в систему обеспечения кибербезопасности?
27. Что нужно для успешного функционирования системы обеспечения кибербезопасности?
28. Дайте характеристику доверенной среде на базе виртуализации.
29. Как реализуется безопасность внутренних и внешних коммуникаций?
30. Что такое программноконфигурируемые сети?
31. Преимущества программно-конфигурируемых сетей при построении систем управления кибербезопасностью?
32. Состав блок управления ПКС.
33. Перечислите возможные подходы к оценке безопасности киберфизических систем.
34. Какой должна быть оценка для всех типов систем и применима как для централизованных энергетических комплексов?
35. Какой подход может быть использован к оценке безопасности киберфизических систем?
36. В чем сущность показателя самоподобия?
37. Дайте характеристику понятию киберустойчивость.
38. От чего зависит оценка устойчивости системы в условиях деструктивных целенаправленных внешних атак?
39. Какие подходы могут быть применяться для оценки устойчивости КФС?
40. Дайте характеристику надежностного подхода для оценки устойчивости КФС.

41. Дайте характеристику подходу самоподобия для оценки устойчивости КФС.
42. Какая основная проблема реализации надежного подхода?
43. Какие виды избыточности можно выделить в модели системы на основе функциональных графов и маршрутов?
44. В чем сущность параметрической избыточности?
45. В чем сущность функциональной избыточности?
46. В чем сущность структурной избыточности?
47. Как представляется оценка устойчивости КФС?
48. Каков механизм выработки компенсирующего воздействия в КФС?
49. В чем сущность гомеостатической концепции представления КФС?
50. Дайте характеристику архитектуры блока управления безопасностью КФС.
51. Что включает в себя блок управления безопасностью?
52. Что включает в себя блок мониторинга?
53. Какие функции выполняет блок генерации компенсирующего воздействия?
54. В чем сущность технология гомеостаза?

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

- формулировку темы лабораторной работы;
- формулировку цели и решаемых в ходе лабораторной работы задач;
- порядок выполнения лабораторной работы с учетом достижения целевой установки;
- выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

Тема 2: Особенности аутентификации в киберфизических системах

Лабораторная работа №3

Реализация процедуры групповой подписи BBS с отзывом права подписи.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».
8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.

9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 ХР».
10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».
13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».
14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».
15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.
16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».
17. Программное изделие «Kaspersky Endpoint Security for Aurora».
18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.
19. Программное комплекс Acronis Backup & Recovery.
20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.
21. Программное обеспечение Oracle Identity Access Management Suite.
22. Программное обеспечение SafeNet Authentication Service.
23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.
24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».
25. Программный комплекс «InfoWatch Traffic Monitor».
26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.
27. Программный комплекс защиты информации от НСД «Страж 1.1».
28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.
29. Программный комплекс обнаружения вторжений «Ребус-СОВ».
30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»
31. Специальное программное обеспечение «АС «ГРИФ».
32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

23. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».
24. Аппаратно-программный комплекс шифрования «Континент».
25. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
26. Коммутатор Cisco 2XXX/38XX.
27. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95».
28. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
29. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
30. Маршрутизатор Cisco 3825/3845.
31. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
32. Межсетевой экран Cisco ASA 5580-20.
33. Межсетевой экран Cisco PIX Firewall 515E.
34. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
35. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
36. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
37. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
38. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
39. Программный комплекс защиты информации от НСД «Страж 1.1».
40. Система защиты информации «Secret Net».
41. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
42. Система защиты информации от несанкционированного доступа «Страж NT».
43. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
44. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

5. Повторить теоретический материал лекций по темам «Особенности объектов цифровой индустрии как киберфизических объектов», «Организация безопасной эксплуатации объектов цифровой индустрии».
6. Изучить теоретический материал данного занятия.
7. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
8. Ответить на контрольные вопросы.

Контрольные вопросы

1. Какие новые области охватывают киберфизические системы?
2. Какие условия должны быть соблюдены для аутентификации данных?
3. Чем должен быть снабжен ключ проверки электронной подписи?
4. Какое количество ключей электронной подписи может быть в киберфизических системах?
5. Что из себя представляет аутентификация по Типу 1?
6. Что из себя представляет аутентификация по Типу 2?

7. Какими недостатками обладает решение по проведению процедуры аутентификации по Типу 2?
8. Что из себя представляет аутентификация по Типу 3?
9. В чем заключается принцип кластеризации при проведении процедур аутентификации?
10. Что такое пороговая подпись?
11. Что такое групповая подпись?
12. Что такое кольцевая подпись?
13. Что такое коллективная подпись?
14. Какие проблемы порождает глобальная доступность киберфизических объектов?
15. Назовите свойства киберсреды.
16. В чем состоит специфика защиты КФС от информационных угроз?
17. Какие новые цели появляются у киберпреступников?
18. Какие факторы способствуют деятельности киберпреступников?
19. Какие новые вызовы имеют место в связи с переходом от информационной экономики к цифровой?
20. Какие проблемы возникают по защите элементов АСУ?
21. Какие цели злоумышленников ожидаются в условиях цифровой экономики?
22. Назовите мотивы злоумышленников в условиях цифровой экономики.
23. Какие уязвимые элементы характерны для технологии виртуализации?
24. Какие уязвимые элементы характерны для облачных технологий?
25. Какие уязвимые элементы характерны для технологий умного дома?
26. Какие уязвимые элементы характерны для мобильных систем?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование схемы групповой подписи BBS с отзывом права подписи	- 80 мин
2. Синтез групповой подписи BBS с отзывом права подписи	- 80 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.
Всего	- 180 мин

Основные теоретические сведения

Схема BBS с отзывом права подписи

Различают три естественные модели взаимодействия субъектов с целью отзыва права подписи у пользователя без влияния на возможность других членов группы подписывать сообщения:

- *формирование новой группы при каждом отзыве* (необходимо генерировать заново основные ключи группы) и включение в нее всех членов старой группы, кроме лишенных права подписи. Это способ предполагает повторное проведение протокола Join с каждым пользователем, а также отправку открытого широковещательного сообщения всем проверяющим, может быть применен к любой схеме групповой подписи, но в силу своей универсальности является наиболее накладным, так как требует формирования и повторного распределения всех ключей, а также одновременного оповещения об этих изменениях всех проверяющих;
- *отзыв с динамическим накоплением* (dynamic accumulators) требует рассылки единственного открытого широковещательного сообщения всем подписывающим и проверяющим;
- *отзыв, локальный для проверяющего* (verifier local revocation, VLR), требует отправки открытого сообщения только всем проверяющим.

Здесь не нужно взаимодействие с членами группы.

Таким образом, требование возможности отзыва права подписи может быть уточнено применяемой для отзыва моделью.

При отзыве с динамическим накоплением, если нужно отозвать право подписи у i -го члена группы, менеджер IM , выпускающий ключи, создает новую запись списка отзыва. При формировании записи используются: действующий открытый ключ группы, часть личного ключа отзываемого пользователя и личный ключ ik менеджера IM . Сформированная запись отзыва рассылается всем членам группы и всем проверяющим.

Все участники группы и проверяющие используют эту запись, чтобы вычислить новый открытый ключ группы. Все действующие члены группы на основе этой записи отзыва и своего старого личного ключа могут обновить свой личный ключ для соответствия новому открытому ключу группы gpk .

Несмотря на то что менеджер IM может не знать полный личный ключ каждого члена, оставшегося в группе, он может, используя свой ключ ik и старые значения ключей участников группы, вычислить новые значения ключей из сертификатов пользователей. Эти сертификаты требуются ему для поддержания базы данных членов группы в актуальном состоянии. Следовательно, менеджер IM может обновить базу данных членов группы, используемую менеджером OM для раскрытия подписей.

Таким образом, после проведения этих операций у группы обновляется открытый ключ, а у всех действующих пользователей — личные ключи.

Этот подход обладает следующими недостатками:

- объем вычислений достаточно велик (если число отозванных пользователей велико). В частности, менеджер IM должен обновить все записи в базе данных членов группы;

- из-за изменения ключей группы невозможно проверить подписи, сформированные на старых ключах;
- всем заинтересованным субъектам необходимо разослать сообщение, содержащее запись отзыва; в противном случае возможна рассинхронизация данных подписывающих и проверяющих. К тому же в некоторых схемах запись отзыва содержит все данные, позволяющие любой стороне легко вычислить личный ключ отозванного пользователя. Если требование одновременной рассылки не будет выполнено, то пользователь, получивший сообщение раньше, может воспользоваться личным ключом отозванного члена группы и сформировать от его имени подпись, которая будет принята проверяющим, не обновившим ключи вовремя. Следовательно, одна из задач, которую нужно решить для построения системы групповой аутентификации на основе схемы подписи ED-BBS, — добавление такой возможности отзыва с определенного момента времени, чтобы все подписи, сформированные до того, как была выпущена очередная запись списка отзыва, остались корректными, проверяемыми и отслеживаемыми; необходимо также обеспечить строгую синхронизацию субъектов.

Покажем, как адаптировать отзыв права подписи с динамическим накоплением для работы в расширенной версии схемы BBS. Иерархическая структура рассматриваемых систем позволяет разослать одно открытое шифрованное сообщение всем подписывающим и проверяющим.

Чтобы отозвать право подписи у i -го пользователя, выпускающий менеджер публикует элемент $RL_i = (A_i^*, x_i, h_i^*)$ списка отзыва, где $A_i^* = g_2^{1/(\gamma+x_i)} \in G_2$ и $h_i^* = h^{1/(\gamma+x_i)}$. Заметим, что $A_i = \psi(A_i^*)$ и для вычисления значения A_i^* , h_i^* нужно знать ключ $ik = \gamma$. Если группы G_1 и G_2 совпадают, то гомоморфизм ψ тождественный и $A_i = A_i^*$.

Для r отзываеваемых участников список отзыва $RL = \{RL_1, \dots, RL_r\}$ рассылается всем членам группы и проверяющим в системе, которые используют его для обновления ключей gpk и gsk . Пусть $u = \prod_{i=1}^r (\gamma + x_i) \in \mathbb{Z}_p^*$. Тогда новый открытый ключ группы $(\hat{g}_1, \hat{h}, u_1, u_2, u_3, d_1, d_2, \hat{g}_2, \hat{w})$ получается из старого следующим образом: $\hat{g}_1 = g_1^{1/u}$, $\hat{h} = h^{1/u}$, $\hat{g}_2 = g_2^{1/u}$, $\hat{w} = \hat{g}_2^\gamma$.

Имея открытый ключ группы $gpk = (g_1, h, u_1, u_2, u_3, d_1, d_2, g_2, w)$ и один отозванный личный ключ, например $(A_1^*, x_1, h_1^*) \in RL$, каждый участник взаимодействия может создать новый открытый ключ группы $(\hat{g}_1, \hat{h}, u_1, u_2, u_3, d_1, d_2, \hat{g}_2, \hat{w})$, такой что $\hat{g}_1 = g_1^{1/(\gamma+x_1)}$; $\hat{h} = h^{1/(\gamma+x_1)}$; $\hat{g}_2 = g_2^{1/(\gamma+x_1)}$; $\hat{w} = \hat{g}_2^\gamma$, следующим образом:

$$\hat{g}_1 \leftarrow \psi(A_1^*); \quad \hat{g}_2 \leftarrow A_1^*; \quad \hat{w} \leftarrow g_2(A_1^*)^{-x_1}; \quad \hat{h} \leftarrow h_1^*.$$

Тогда

$$\begin{aligned} \hat{g}_1 &= \psi(A_1^*) = g_1^{1/(\gamma+x_1)}; \quad \hat{h} = h^{1/(\gamma+x_1)}; \quad \hat{g}_2 = A_1^* = g_2^{1/(\gamma+x_1)}; \\ \hat{w} &= g_2(A_1^*)^{-x_1} = g_2 g_2^{-x_1/(\gamma+x_1)} = g_2^{\gamma/(\gamma+x_1)} = \hat{g}_2^\gamma, \end{aligned}$$

как и требуется.

Все действующие пользователи также могут обновить свои личные закрытые ключи. Действительно, пользователь с личным ключом $gsk = (A, x, y)$, получив элемент $RL_1 = (A_1^*, x_1, h_1^*)$ списка отзыва, вычисляет $\hat{A} \leftarrow (\psi(A_1^*)(h_1^*)^y / A)^{1/(x-x_1)}$ и меняет свой личный ключ на $(\hat{A}, x, y)$. Тогда

$$\begin{aligned}\hat{A}^{x+\gamma} &= \frac{(g_1^{1/(\gamma+x_1)} h^{y/(\gamma+x_1)})^{(\gamma+x_1+x-x_1)/(x-x_1)}}{A^{(\gamma+x)/(x-x_1)}} = \\ &= \frac{(g_1 h^y)^{1/(x-x_1)} (g_1^{1/(\gamma+x_1)} h^{y/(\gamma+x_1)})}{(g_1 h^y)^{1/(x-x_1)}} = \hat{g}_1 \hat{h}^y.\end{aligned}$$

Таким образом, $(\hat{A}, x, y)$ — корректный закрытый ключ, соответствующий новому открытому ключу группы $(\hat{g}_1, \hat{h}, u_1, u_2, u_3, d_1, d_2, \hat{g}_2, \hat{w})$.

Повторив такой процесс r раз, можно отозвать право подписи у всех пользователей, попавших в список отзыва.

Пользователь, чей сертификат отозван, не может вычислить новый закрытый ключ в соответствии с приведенными выше правилами.

Смена ключей требует коррекции базы данных членов группы. Записи в этой базе имеют вид (upk, A, x, h^y, S) , где upk — личный сертифицированный ключ пользователя, S — подпись значения A на закрытом ключе владельца сертификата. При смене ключей все записи становятся неактуальными, однако выпускающий менеджер может вычислить новое значение $\hat{A}$ для каждой такой записи, так как знает ключ ik : $\hat{A} \leftarrow ((g_1 h^y)^{1/(\gamma+x_1)} / A)^{1/(x-x_1)}$, но не может скорректировать подпись S . Тем не менее это не повлияет на возможность проверки корректности раскрытия групповой подписи, так как из новых открытого и закрытого ключей, а также из элемента списка отзыва можно выразить старое значение A , подпись для которого действительна: $A \leftarrow \hat{g}_1 \hat{h}^y \hat{A}^{x_1-x}$.

Таким образом, достоверно зная все факты отзыва членских сертификатов, всегда можно модифицировать алгоритм проверки правильности раскрытия подписи для работы со значением A , выраженным через новые значения ключей и записей списка отзыва. Если когда-либо производились операции отзыва, то при проверке правильности раскрытия придется отслеживать всю историю изменения части A закрытого ключа пользователя, оставшегося в группе.

Благодаря тому, что в списке отзыва публикуется только часть сертификата отзываемого участника, ни один из участников не может воспользоваться этой информацией, чтобы сформировать подпись с помощью раскрытого менеджером группы сертификата и обмануть тех проверяющих, которые еще не успели обновить локальную копию открытого ключа группы.

Данный протокол отзыва права подписи в схеме ED-BBS не решает некоторых прикладных проблем:

- нет возможности отозвать право подписи с определенного момента времени. Нужно, чтобы подписи, сформированные членом группы до того, как его сертификат попал в список отзыва, сохраняли полный набор свойств, обеспечиваемых базовой схемой, — корректность, анонимность и отслеживаемость;

- не ясно, как запретить членам группы использовать свои старые сертификаты для формирования групповой подписи;
- не ясно, как обеспечить корректность, анонимность и отслеживаемость всех подписей, сформированных членами группы до изменения открытого ключа группы.

Таким образом, все возникающие трудности имеют временной характер, поскольку запись отзыва не привязана ко времени ее формирования. Кроме того, ко времени не привязаны открытый ключ группы, закрытые ключи членов группы и записи в базе данных членов группы. Для преодоления этих недостатков можно добавить временные метки:

- к открытому ключу группы gpk — время его создания t_{gpk} ;
- к каждой записи $(upk_{ji}, A_{ji}, x_{ji}, h^{y_{ji}}, S_{ji})$ в базе данных членов группы — время t_{RL_i} прекращения действия записи j -го пользователя ввиду отзыва у него права подписи либо ввиду ее изменения в связи с отзывом права подписи у другого члена группы. Действительная в настоящий момент времени запись имеет нулевую временную метку;
- к каждой групповой подписи σ — время t_σ ее формирования. Таким образом, каждая групповая подпись привязывается к определенному i -му моменту времени t_σ , в который был действителен определенный открытый ключ группы gpk_i , и сама групповая подпись была сформирована членом группы с действующим на тот момент сертификатом gsk_{ji} , то есть с любой групповой подписью σ ассоциирована связка $(gpk_i, t_{gpk_i}) - (\sigma, t_\sigma) - (gsk_{ji}, t_{RL_i})$, при этом:
- в подписи σ зашифровано значение A_{ji} , то есть ее сформировал j -й пользователь, обладающий членским сертификатом $gsk_{ji} = (A_{ji}, x_{ji}, y_{ji})$, действующим в i -й период, с которым связано время прекращения его действия t_{RL_i} ;
- выполняются неравенства $t_{gpk_i} \neq t_\sigma, t_\sigma \neq t_{RL_i}$. Это означает, что формирование группы (либо исключение какого-либо члена из группы, сопровождающееся изменением открытого ключа группы), добавление члена в группу и формирование им подписи сообщения — не могли произойти одновременно;
- $t_{gpk_i} < t_\sigma$ — группа должна быть сформирована раньше, чем могут быть созданы подписи от ее имени;
- не существует другой пары (gpk_k, t_{gpk_k}) , относящейся к этой группе и такой, что $t_{gpk_i} < t_{gpk_k} < t_\sigma$, то есть gpk_i — актуальный открытый ключ группы на момент формирования подписи σ ;
- $t_\sigma < t_{RL_i}$ и не существует другой пары (gsk_{jk}, t_{RL_k}) , относящейся к j -му члену группы и такой, что $t_\sigma < t_{RL_k} < t_{RL_i}$, то есть gsk_{ji} — актуальный закрытый ключ j -го члена группы на момент формирования подписи σ .

Такую связку можно назвать окружением подписи σ . Для выполнения проверки подписи, ее раскрытия и доказательства корректности раскрытия нужно использовать ключи из окружения этой подписи.

Если за поддержание временных меток открытых ключей и записей базы данных членов отвечает выпускающий менеджер, то за установку временной метки в подписи отвечает член группы. Таким образом, требуется ввести нового доверенного участника — временного менеджера *ТМ*, ставящего временную метку и удостоверяющего ее своей личной подписью. На этого участника возлагается и обязанность удостоверения временных меток, проставляемых на открытом ключе группы и записях базы данных членов группы.

В рассмотренной схеме EDR-BBS (extended dynamic revocable BBS) временной менеджер фиксирует время создания группы, а также время и факт включения пользователя в группу, заверяет время создания групповой подписи, удостоверяет запись отзыва, поддерживает базы данных в актуальном состоянии, обеспечивает атомарность операции отзыва.

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.

Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.

E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.

Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред. А.И. Астайкина. Саратов: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.

Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.

Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.А. Мельников. — 3-е изд., стер. — М.: Флинта, 2019. — 444 с.

Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.

Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.: Лаборатория знаний, 2020. — 482 с.

Ли, П. Архитектура интернета вещей / П. Ли; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

Дубков, И. С. Решение практических задач на базе технологии интернета вещей: учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск: Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»

Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>

Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -

Официальный сайт Федеральной службы безопасности Российской

Федерации <http://www.fsb.ru/> -

Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>

Интернет портал Защита-информации.SU <http://www.iso27000.ru/>

Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>

Консорциум сетевых электронных библиотек ЭБС «Лань»
<https://e.lanbook.com/>

ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/>

ЭБС IPR SMART <https://www.iprbookshop.ru/>

ЭБС Znanium <https://znanium.com/>

ЭБС «Юрайт» <http://www.biblio-online.ru>

Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

Используя теоретический материал, представленный в методических рекомендациях, исследовать схему групповой подписи BBS с отзывом права подписи. Особое внимание обратить на то, что при отзыве с динамическим накоплением, если нужно отозвать право подписи у i -го члена группы, менеджер, выпускающий ключи, создает новую запись списка отзыва. При формировании записи используются: действующий открытый ключ группы, часть личного ключа отзываемого пользователя и личный ключ *ik* менеджера *IM*. Сформированная запись отзыва рассылается всем членам группы и всем проверяющим. (90 минут).

В соответствии с вариантами лабораторной работы №1 осуществить синтез групповой подписи BBS с отзывом права подписи, описанных в теоретическом материале методических рекомендаций. (90 минут.).

№ Варианта	Число членов группы	Количество отзываемых подписей
16.	2	1
17.	3	2
18.	4	3

19.	5	2
20.	6	3
21.	7	2
22.	8	3
23.	9	2
24.	10	3
25.	11	2
26.	12	3
27.	13	3
28.	14	4
29.	15	5
30.	16	10

Цель работы - модифицировать алгоритм проверки правильности раскрытия подписи с учетом исходных данных Результаты лабораторной работы занести в отчет

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

формулировку темы лабораторной работы;

формулировку цели и решаемых в ходе лабораторной работы задач;

порядок выполнения лабораторной работы с учетом достижения целевой установки;

выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

Лабораторная работа №4

Построение схемы групповой подписи на решетках по протоколу DKV.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».
8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.
9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 XP».

10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».

11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».

12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».

13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».

14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».

15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.

16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».

17. Программное изделие «Kaspersky Endpoint Security for Aurora».

18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.

19. Программное комплекс Acronis Backup & Recovery.

20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.

21. Программное обеспечение Oracle Identity Access Management Suite.

22. Программное обеспечение SafeNet Authentication Service.

23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.

24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».

25. Программный комплекс «InfoWatch Traffic Monitor».

26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.

27. Программный комплекс защиты информации от НСД «Страж 1.1».

28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.

29. Программный комплекс обнаружения вторжений «Ребус-СОВ».

30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»

31. Специальное программное обеспечение «АС «ГРИФ».

32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».

2. Аппаратно-программный комплекс шифрования «Континент».

3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95».
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1».
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

1. Повторить теоретический материал лекций по темам «Особенности объектов цифровой индустрии как киберфизических объектов», «Организация безопасной эксплуатации объектов цифровой индустрии».
2. Изучить теоретический материал данного занятия.
3. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Какие новые области охватывают киберфизические системы?
2. Какие условия должны быть соблюдены для аутентификации данных?
3. Чем должен быть снабжен ключ проверки электронной подписи?
4. Какое количество ключей электронной подписи может быть в киберфизических системах?
5. Что из себя представляет аутентификация по Типу 1?
6. Что из себя представляет аутентификация по Типу 2?

7. Какими недостатками обладает решение по проведению процедуры аутентификации по Типу 2?
8. Что из себя представляет аутентификация по Типу 3?
9. В чем заключается принцип кластеризации при проведении процедур аутентификации?
10. Что такое пороговая подпись?
11. Что такое групповая подпись?
12. Что такое кольцевая подпись?
13. Что такое коллективная подпись?
14. Какие проблемы порождает глобальная доступность киберфизических объектов?
15. Назовите свойства киберсреды.
16. В чем состоит специфика защиты КФС от информационных угроз?
17. Какие новые цели появляются у киберпреступников?
18. Какие факторы способствуют деятельности киберпреступников?
19. Какие новые вызовы имеют место в связи с переходом от информационной экономики к цифровой?
20. Какие проблемы возникают по защите элементов АСУ?
21. Какие цели злоумышленников ожидаются в условиях цифровой экономики?
22. Назовите мотивы злоумышленников в условиях цифровой экономики.
23. Какие уязвимые элементы характерны для технологии виртуализации?
24. Какие уязвимые элементы характерны для облачных технологий?
25. Какие уязвимые элементы характерны для технологий умного дома?
26. Какие уязвимые элементы характерны для мобильных систем?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование схемы групповой подписи на решетках по протоколу DKV	- 80 мин
2. Синтез схемы групповой подписи на решетках по протоколу DKV	- 60 мин
3. Тестирование по теме 2	20 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.
Всего	- 180 мин

Основные теоретические сведения

Групповая подпись на решетках по протоколу DKV

Первой попыткой построения схем групповой подписи на решетках стал протокол DKV . Модель представляет собой сочетание уже опубликованных ранее идей, но в основном следует шаблонам, описанным в схеме BMW . В 2013 году был разработан протокол LLS , который является логичным продолжением протокола DKV . Его авторы сделали упор на оптимизацию, и основной особенностью протокола стал малый размер цифровой подписи. Сравним эти схемы групповой подписи.

Пусть:

- $L(A^T) = \{y \in \mathbb{Z}^m \mid y \equiv A^T s \pmod{q}, s \in \mathbb{Z}_q^n\}$ — решетка размерности m для фиксированного q и матрицы $A \in \mathbb{Z}_q^{n \times m}$;
- $L^\perp(A) = q(\Lambda(A^T))^* = \{w \in \mathbb{Z}^m \mid A^* w \equiv 0 \pmod{q}\}$ — решетка, ортогональная решетке L , т. е., если $x \in L(A^T)$, $y \in L^\perp(A)$, то $x^T y \equiv 0 \pmod{q}$;
- $\text{dist}(L(A^T), z) = \min_{s \in \mathbb{Z}_q^n} \|(A^T s - z) \pmod{q}\|$, $z \in \mathbb{Z}_q^m$ — функция, вычисляющая расстояние между вектором z и ближайшим к нему узлом решетки $L(A^T)$;
- $D_{L,s,c}(x) = \frac{D_{s,c}(x)}{\sum_{y \in L} D_{s,c}(y)}$, $\forall x \in L$ — функция плотности нормального распределения. Если $c = 0$, то соответствующую функцию обозначают $D_{L,s}(x)$;
- $\text{TrapSamp}(1^n, 1^m, q)$ — процедура, формирующая однородную матрицу $B \in \mathbb{Z}_q^{n \times m}$ и матрицу-лазейку $T' \in \mathbb{Z}^{m \times m}$. Можно показать, что матрица T' является базисом для некоторой решетки $L^\perp(A)$, причем $A^* T' \equiv 0 \pmod{q}$;
- $\text{SuperSamp}(1^n, 1^m, q, B)$, $q \geq 2$, $m \geq 8n \log q$, $B \in \mathbb{Z}_q^{n \times m}$ — процедура вычисления матриц $A \in \mathbb{Z}_q^{n \times m}$ и $T \in \mathbb{Z}^{m \times m}$ таких, что $A^* T \equiv 0 \pmod{q}$;
- $\text{GPVInvert}(A, T, s, h)$ — функция, которая генерирует минимальный вектор $e \leftarrow D_{L^\perp(A)+t,s}$, где значение $t \in \mathbb{Z}^m$ таково, что $At = h$. Без использования лазейки задача нахождения такого вектора e является сложной;
- $\text{RandBasis}(S)$ — процедура, которая принимает на вход базис S некоторой решетки и возвращает новый базис той же решетки;
- $\text{GPVSample}(A, r)$ — процедура, которая принимает на вход базис A некоторой решетки и параметр r и возвращает некоторый вектор из данной решетки;
- $\text{ExtBasis}(B, T_A)$ — процедура, которая принимает на вход матрицу $B \in \mathbb{Z}_q^{m' \times n}$, $m < m'$, и базис T_A решетки $L_q^\perp(A)$, где $A \in \mathbb{Z}_q^{m \times n}$ — верхняя подматрица матрицы B . Возвращает базис T_B решетки $L_q^\perp(B)$;
- $\text{Decrypt}(c, S)$ — процедура, которая восстанавливает значение вектора из шифртекста c с использованием лазейки S .

В этом протоколе открытый мастер-ключ состоит из ключа pk_e , используемого в системе шифрования с открытым ключом, а также n ключей проверки подписей $pk_1, pk_2, \dots, pk_n$. При этом i -му пользователю выдается персональный секретный ключ sk_i , соответствующий ключу pk_i . Чтобы подписать сообщение M , пользователь с номером i использует ключ sk_i , а затем шифрует полученное значение при помощи ключа pk_e . Свойства анонимности и отслеживаемости обеспечиваются за счет того, что менеджер группы — единственный участник, знающий ключ расшифрования sk_e .

В протоколе DKV используются следующие параметры:

- $n \in \mathbb{Z}$ — параметр безопасности;
- $N \in \mathbb{Z}$ — предполагаемое число участников группы;
- $q = \text{poly}(n)$, $q \in \mathbb{Z}$;
- $m \geq 8n \log q$, $m \in \mathbb{Z}$;
- $s \in \mathbb{Z}$ — случайное число в интервале от 1 до $\sqrt{n \log q \log n}$;
- γ — целое число из интервала от 1 до $\sqrt{m}/\log m$.

Мастер-ключ (открытый ключ, доступный любому участнику в системе, в том числе и нарушителю) включает в себя:

- B — открытый ключ шифрования (используется схема групповой подписи GPV) — базис в $\mathbb{Z}_q^{m \times n}$;
- $A_1, A_2, \dots, A_N \in \mathbb{Z}_q^{n \times m}$ — набор ключей для проверки подписей;
- $H: \{0, 1\}^* \rightarrow \mathbb{Z}_q^n$ — хэш-функция, используемая случайным оракулом.

У каждого пользователя есть закрытый ключ gsk_i , с помощью которого он подписывает сообщение.

Чтобы подготовить сообщение M , i -й пользователь должен:

1. Подписать его ключом gsk_i . Для формирования подписи пользователь использует лазейку $T_i = gsk_i$, чтобы найти минимальный вектор $e_i \in \mathbb{Z}^m$: $A_i e_i = H(M)$:

$$e_i \leftarrow GPV\text{Invert}(A_i, T_i, s, h_i),$$

где $h_i = H(M \| r \| i)$, $r \leftarrow \{0, 1\}^n$, — случайная двоичная строка.

2. Зашифровать вектор e_i с помощью алгоритма Реева: $z = B^T s + e_i$, где $s \in \mathbb{Z}_q^n$ — случайный вектор.

3. Предоставить доказательство с нулевым разглашением того, что сообщение сформировано корректно.

Для более эффективного формирования доказательства вместо одного ключа шифрования B можно использовать набор $\{B_1, B_2, \dots, B_N\}$. Тогда, чтобы подписать сообщение, i -й пользователь вычисляет «настоящую» подпись e_i и набор псевдоподписей e_j , $i \neq j$ (подписи e_j не будут минимальными, а значит, будут неверными). Эти подписи шифруются по тому же принципу, что и вектор e_i . При необходимости пользователь сможет доказать, что в каждом шифртексте z_j содержится псевдоподпись и что одна из этих подписей минимальна.

Неинтерактивное доказательство NIWI. Для доказательства с нулевым разглашением используется протокол NIWI (noninteractive witness-indistinguishable [65]). Пусть $B_1, B_2, \dots, B_N \in \mathbb{Z}_q^{n \times m}$ и $z_1, z_2, \dots, z_N \in \mathbb{Z}_q^{n \times m}$, $\gamma = \gamma(n)$; $L_{s,\gamma} = (L_{YES}, L_{NO})$ — некоторый промежуточный язык, определенный следующим образом:

$$L_{YES} = \left\{ \begin{pmatrix} B_1, B_2, \dots, B_N \\ z_1, z_2, \dots, z_N \end{pmatrix} \mid \exists s \in \mathbb{Z}_q^n, 1 \leq i \leq N: \|z_i - B_i^T s\| \leq s\sqrt{m} \right\};$$

$$L_{NO} = \left\{ \begin{pmatrix} B_1, B_2, \dots, B_N \\ z_1, z_2, \dots, z_N \end{pmatrix} \mid \exists s \in \mathbb{Z}_q^n, 1 \leq i \leq N: \|z_i - B_i^T s\| > s\sqrt{m} \right\}.$$

Здесь L_{YES} — набор точек, по крайней мере одна из которых близка к соответствующей решетке; L_{NO} — набор точек, ни одна из которых не лежит достаточно близко к узлам данной решетки. Рассмотрим модификацию задачи CVP, т.е. язык $L'_{s,\gamma} = (L'_{YES}, L'_{NO})$:

$$L'_{YES} = \{(B, z, t) \mid \exists s: \|z - B^T s\| \leq t\};$$

$$L'_{NO} = \{(B, z, t) \mid \forall s: \|z - B^T s\| > \gamma t\}.$$

Для языка L'_γ при $1 \leq \gamma \leq \sqrt{m}/\log m$ существует система доказательств NIWI [75, 106]. Следует отметить, что язык $L_{s,\gamma}$ может быть переопределен как дизъюнкция нескольких экземпляров L'_γ :

$$\begin{pmatrix} B_1, B_2, \dots, B_N \\ z_1, z_2, \dots, z_N \end{pmatrix} \in L_{YES} \Leftrightarrow \bigvee_i ((B_i, s_i, s\sqrt{m}) \in L'_{YES});$$

$$\begin{pmatrix} B_1, B_2, \dots, B_N \\ z_1, z_2, \dots, z_N \end{pmatrix} \in L_{NO} \Leftrightarrow \bigwedge_i ((B_i, s_i, s\sqrt{m}) \in L'_{NO}).$$

Неинтерактивное доказательство NIWI. Для доказательства с нулевым разглашением используется протокол NIWI (noninteractive witness-indistinguishable). Пусть $B_1, B_2, \dots, B_N \in \mathbb{Z}_q^{n \times m}$ и $z_1, z_2, \dots, z_N \in \mathbb{Z}_q^{n \times m}$, $\gamma = \gamma(n)$; $L_{s,\gamma} = (L_{YES}, L_{NO})$ — некоторый промежуточный язык, определенный следующим образом:

$$L_{YES} = \left\{ \begin{pmatrix} B_1, B_2, \dots, B_N \\ z_1, z_2, \dots, z_N \end{pmatrix} \mid \exists s \in \mathbb{Z}_q^n, 1 \leq i \leq N: \|z_i - B_i^T s\| \leq s\sqrt{m} \right\};$$

$$L_{NO} = \left\{ \begin{pmatrix} B_1, B_2, \dots, B_N \\ z_1, z_2, \dots, z_N \end{pmatrix} \mid \exists s \in \mathbb{Z}_q^n, 1 \leq i \leq N: \|z_i - B_i^T s\| > s\sqrt{m} \right\}.$$

Здесь L_{YES} — набор точек, по крайней мере одна из которых близка к соответствующей решетке; L_{NO} — набор точек, ни одна из которых не лежит достаточно близко к узлам данной решетки. Рассмотрим модификацию задачи CVP, т.е. язык $L'_{s,\gamma} = (L'_{YES}, L'_{NO})$:

$$L'_{YES} = \{(B, z, t) \mid \exists s: \|z - B^T s\| \leq t\};$$

$$L'_{NO} = \{(B, z, t) \mid \forall s: \|z - B^T s\| > \gamma t\}.$$

Для языка L'_γ при $1 \leq \gamma \leq \sqrt{m}/\log m$ существует система доказательств NIWI. Следует отметить, что язык $L_{s,\gamma}$ может быть переопределен как дизъюнкция нескольких экземпляров L'_γ :

$$\begin{aligned} \left(\begin{matrix} B_1, B_2, \dots, B_N \\ z_1, z_2, \dots, z_N \end{matrix} \right) \in L_{YES} &\Leftrightarrow \bigvee_i ((B_i, s_i, s\sqrt{m}) \in L'_{YES}); \\ \left(\begin{matrix} B_1, B_2, \dots, B_N \\ z_1, z_2, \dots, z_N \end{matrix} \right) \in L_{NO} &\Leftrightarrow \bigwedge_i ((B_i, s_i, s\sqrt{m}) \in L'_{NO}). \end{aligned}$$

Основные алгоритмы протокола DKV

Setup:

Вход: $1^n, 1^N$.

Выход: PK — открытый ключ группы; TK — ключ менеджера группы для отслеживания подписей; $\vec{gsk}$ — вектор ключей для подписи сообщений.

1. Для $1 \leq i \leq N$ вычислить: $(B_i S'_i) \leftarrow \text{TrapSamp}(1^n 1^m q)$; $(A_i, T_i) \leftarrow \text{SuperSamp}(1^n, 1^m, q, B_i)$; $S_i \leftarrow \text{RandBasis}(S'_i)$.

2. $PK \leftarrow ((A_i, B_i)_{i=1}^N)$; $TK \leftarrow (S_i)_{i=1}^N$; $\vec{gsk} \leftarrow (T_i)_{i=1}^N$.

Sign:

Вход: $gsk[j]$ — персональный закрытый ключ j -го пользователя, M — сообщение.

Выход: Подпись σ .

1. Сгенерировать случайную строку $r \leftarrow \{0, 1\}^n$.

2. Для $1 \leq i \leq N$ вычислить $h_i \leftarrow H(M \| r \| i)$.

3. Положить $e_j \leftarrow \text{GPVInvert}(A_j, T_j, s, h_j)$.

4. Для $1 \leq i \leq N$, $i \neq j$, найти e_i , решив систему $A_i e_i = h_i \pmod{q}$.

5. Для $1 \leq i \leq N$ выбрать произвольный вектор $s_i \in \mathbb{Z}_q^n$ и вычислить $z_i = B_i^T s_i + e_i \pmod{q} \in \mathbb{Z}_q^m$.

6. Сформировать доказательство π по протоколу NIWI с помощью параметра γ .

7. Подписью является кортеж $\sigma = (r, z_1, \dots, z_N, \pi)$.

Verify:

Вход: PK, M, σ .

Выход: 0 или 1.

1. Преобразовать подпись в форму $\sigma \rightarrow (r, z_1, \dots, z_N, \pi)$.

2. Вернуть 1, если доказательство π корректно и $A_i z_i = H(M \| r \| i)$ для всех $1 \leq i \leq N$. Иначе вернуть 0.

Open:

Вход: TK, M, σ .

Выход: i — идентификатор пользователя.

Для $1 \leq i \leq N$:

1. Преобразовать подпись в форму $\sigma \rightarrow (r, z_1, \dots, z_N, \pi)$.

2. Восстановить значение e_i при помощи лазейки T_i из равенства $A_i e_i = H(M)$.

3. Восстановить значение s_i из равенства $z_i = B_i^T s_i + e_i$.

4. Вернуть i , если $\text{dist}(L(B_i^T, z_i)) \leq s\sqrt{m}$.

Протокол DKV обладает свойствами корректности, анонимности и отслеживаемости. К недостаткам можно отнести следующие:

- по построению размер подписи линейно зависит от числа пользователей, что делает его менее эффективным, чем обычные схемы групповой подписи, основанные, например, на билинейных отображениях;
- отсутствует возможность отзыва права подписи, добавления нового пользователя и проверки правильности раскрытия подписи (без знания какого-либо секрета).

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.
2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л.Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю.С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.
3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

1. Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.
3. А.И. Астайкина. Саратов: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.А. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.: Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей: учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск: Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -
3. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/> -
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>
5. Интернет портал Защита-информации.SU <http://www.iso27000.ru/>
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>
7. Консорциум сетевых электронных библиотек ЭБС «Лань» <https://e.lanbook.com/>
8. ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/> -
9. ЭБС IPR SMART <https://www.iprbookshop.ru/>
10. ЭБС Znanium <https://znanium.com/>
11. ЭБС «Юрайт» <http://www.biblio-online.ru>
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

2. Используя теоретический материал, представленный в методических рекомендациях, исследовать схему групповой подписи на решетках по протоколу DKV. Особое внимание при этом обратить на то, что в этом протоколе открытый мастер-ключ состоит из ключа pk_e , используемого в системе шифрования с открытым ключом, а также n ключей проверки подписей $pk_1, pk_2, \dots, pk_n$. При этом i -му пользователю выдается персональный секретный ключ ski , соответствующий ключу pk_i . Чтобы подписать сообщение M , пользователь с номером i использует ключ ski , а затем шифрует полученное значение при помощи ключа pk_e . (90 минут).

3. В соответствии с вариантами лабораторной работы №1 осуществить разработку основных алгоритмов по протоколу DKV. (90 минут.).

№ Варианта	Число членов группы	Параметр безопасности
31.	2	2
32.	3	3
33.	4	4
34.	5	5
35.	6	6
36.	7	3
37.	8	7
38.	9	6
39.	10	5
40.	11	3
41.	12	6
42.	13	7
43.	14	6
44.	15	5
45.	16	1

Цель работы состоит в реализации алгоритмов по протоколу DKV с доказательствами корректности, анонимности подписи.

Результаты лабораторной работы занести в отчет

4. За 20 минут до окончания занятий проводится тестирование по теме №1. Вопросы тестирования охватывают теоретический материал, выданный на лекционных занятиях.

Перечень вопросов, выносимый на процедуру тестирования.

1. Какие новые области охватывают киберфизические системы?

2. Какие условия должны быть соблюдены для аутентификации данных?
3. Чем должен быть снабжен ключ проверки электронной подписи?
4. Какое количество ключей электронной подписи может быть в киберфизических системах?
5. Что из себя представляет аутентификация по Типу 1?
6. Что из себя представляет аутентификация по Типу 2?
7. Какими недостатками обладает решение по проведению процедуры аутентификации по Типу 2?
8. Что из себя представляет аутентификация по Типу 3?
9. В чем заключается принцип кластеризации при проведении процедур аутентификации?
10. Что такое пороговая подпись?
11. Что такое групповая подпись?
12. Что такое кольцевая подпись?
13. Что такое коллективная подпись?
14. Какие проблемы порождает глобальная доступность киберфизических объектов?
15. Назовите свойства киберсреды.
16. В чем состоит специфика защиты КФС от информационных угроз?
17. Какие новые цели появляются у киберпреступников?
18. Какие факторы способствуют деятельности киберпреступников?
19. Какие новые вызовы имеют место в связи с переходом от информационной экономики к цифровой?
20. Какие проблемы возникают по защите элементов АСУ?
21. Какие цели злоумышленников ожидаются в условиях цифровой экономики?
22. Назовите мотивы злоумышленников в условиях цифровой экономики.
23. Какие уязвимые элементы характерны для технологии виртуализации?
24. Какие уязвимые элементы характерны для облачных технологий?
25. Какие уязвимые элементы характерны для технологий умного дома?
26. Какие уязвимые элементы характерны для мобильных систем?

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

- формулировку темы лабораторной работы;
- формулировку цели и решаемых в ходе лабораторной работы задач;
- порядок выполнения лабораторной работы с учетом достижения целевой установки;
- выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

Тема 3: Процедуры реализации подписи в киберфизических системах

Лабораторная работа №5

Построение схемы групповой подписи на решетках по протоколу LLLS.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».
8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.

9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 ХР».
10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».
13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».
14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».
15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.
16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».
17. Программное изделие «Kaspersky Endpoint Security for Aurora».
18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.
19. Программное комплекс Acronis Backup & Recovery.
20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.
21. Программное обеспечение Oracle Identity Access Management Suite.
22. Программное обеспечение SafeNet Authentication Service.
23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.
24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».
25. Программный комплекс «InfoWatch Traffic Monitor».
26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.
27. Программный комплекс защиты информации от НСД «Страж 1.1».
28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.
29. Программный комплекс обнаружения вторжений «Ребус-СОВ».
30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»
31. Специальное программное обеспечение «АС «ГРИФ».
32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».
2. Аппаратно-программный комплекс шифрования «Континент».
3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95».
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1».
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

1. Повторить теоретический материал лекций по темам «Реализация групповой подписи в киберфизической системе», «Криптографические протоколы в условиях ограниченных вычислительных ресурсов».
2. Изучить теоретический материал данного занятия.
3. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Что нужно для успешного функционирования системы обеспечения кибербезопасности?
2. Кем и когда была предложена схема групповой подписи?
3. Какими свойствами обладает групповая подпись?
4. Для чего могут быть использованы групповые подписи?
5. Перечислите участников схемы групповой подписи?

6. Какие функции в схеме реализации групповой подписи выполняет менеджер (координатор) группы?
7. Какие функции в схеме реализации групповой подписи выполняет выпускающий менеджер?
8. Какие функции в схеме реализации групповой подписи выполняет раскрывающий менеджер?
9. Какие функции в схеме реализации групповой подписи выполняют члены группы?
10. Из каких процедур обычно состоит схема групповой подписи?
11. Какие схемы групповой подписи могут реализовываться в КФС?
12. Какие требования предъявляются к протоколам групповых подписей?
13. Поясните что из себя представляет свойство полной анонимности при реализации групповой подписи?
14. Какими дополнительными свойствами может обладать групповая подпись в КФС в зависимости от решаемой прикладной задачи?
15. Чем определяется эффективность схемы групповой подписи?
16. Что из себя представляет классификационная схема групповых подписей?
17. По каким признакам можно классифицировать схемы групповой подписи?
18. Перечислите участников процедуры выдачи/получения сертификатов при реализации одной из схем групповой подписи.
19. Что подразумевает использование в схеме групповой подписи временного токена?
20. Рост числа разнородных интеллектуальных устройств, имеющих доступ в Интернет, накладывает ряд ограничений на используемые технологии и технологические решения, применяемые для обеспечения защитных функций, назовите эти ограничения.
21. Приведите примеры малоресурсных систем.
22. Основные особенности малоресурсных систем.
23. Чем осложнена криптографическая защита малоресурсных систем?
24. Дайте характеристику понятию - личностная криптография.
25. В чем особенности личностных криптосистем?
26. Какова процедура выработки ключа в личностной криптосистеме?
27. Для реализации в FANET- сети может быть использована личностная схема шифрования с подписью, чем определяется такая возможность?
28. Что включает в себя личностная схема шифрования с подписью?
29. Поясните состав модели связи для интеграции беспроводных датчиков в Интернете вещей.
30. По каким причинам возникает необходимость аутсорсинга вычислений?

31. Что необходимо для создания аутсорс-версии криптографического алгоритма ALG?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование схемы групповой подписи на решетках по протоколу LLLS	- 80 мин
2. Синтез схемы групповой подписи на решетках по протоколу LLLS	- 80 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.
Всего	- 180 мин

Основные теоретические сведения

Групповая подпись на решетках по протоколу LLS

Основной особенностью протокола LLS является малый размер цифровой подписи. Так, для параметра безопасности t и размера группы N открытый ключ и цифровая подпись имеют длину $O(t^2 \log N)$. Следует отметить, что ни одна схема с размером подписи $O(\log N)$ не является корректной, поскольку полученная подпись нескрываемая, поэтому основная задача состоит в минимизации значения $O(t^2)$. Данный протокол стал первым шагом в решении данной задачи. Так же как и протокол DKV, он представляет собой модель со случайным оракулом, а безопасность основана на задачах LWE и ISIS.

В основе протокола LLS лежит парадигма шифрования сертификата участника группы на открытом ключе. Тем самым участник может предоставить неинтерактивное доказательство того, что зашифрованный текст содержит его действительный сертификат. Идея модели состоит в том, чтобы шифровать не долговременный сертификат участника, а разовый сертификат, который генерируется при каждом формировании подписи, наследуется от исходного и шифруется вместе с доказательством.

Авторы протокола LLS руководствовались опытом авторов DKV, но различия прослеживаются уже на самом нижнем уровне архитектуры протокола. В частности, изменению подверглось доказательство того, что шифротекст сформирован легитимным членом группы. В DKV «настоящая» подпись скрывается за $N - 1$ фиктивными подписями, которые также удовлетворяют проверочному уравнению, при этом не будучи короткими векторами. Во избежание линейной зависимости размера подписи от числа членов группы предлагается следующий подход.

Каждому члену группы присваивается уникальный l -битный идентификатор $id \leftarrow id[0] \dots id[l] \in \{0, 1\}^l$, где $l = \lceil \log_2 N \rceil$. Опираясь на схему подписи, использующую короткий базис некоторой решетки вместо одиночного вектора, можно предоставить подписывающему возможность генерировать разовые сертификаты — пары $x_1, x_2 \in Z^m$ дискретных гауссовых векторов, удовлетворяющие соотношению

$$x_1^T A + x_2^T \left(A_0 + \sum_{i=1}^l id[i] A_i \right) = 0 \pmod{q},$$

где q — малое простое число; $A, A_0, \dots, A_l$ — части открытого ключа группы.

На основе параметров безопасности системы — числа n и ожидаемого максимального числа пользователей $N = 2^l$ — генерируются:

- целое число $m \approx n \log q$;
- целое число $r \approx m^{3/2} \sqrt{\ln \log q \log m}$;
- число $\alpha \in \mathbb{R}$: $\alpha^{-1} \geq \tilde{O}(pm^3 \log m)$;
- $p \approx (\alpha q + r)m^{3/2}n$;
- простое число $q \approx l + \alpha^{-1} \sqrt{nl}$.

- $H: \{0, 1\}^* \rightarrow \{0, 1\}^t$, $t = \Theta(n)$, — хэш-функция, моделирующая случайный оракул.

Для данного протокола переопределим процедуру *RandBasis* следующим образом: *RandBasis*(Ss) — принимает на вход базис некоторой решетки и параметр s , возвращает новый базис той же решетки.

Основные алгоритмы протокола LLS

Setup:

Вход: $n, N = 2^l$.

Выход: $gpk, gsk, gmsk$.

1. $(A, T_A) \leftarrow \text{TrapSamp}(1^n, 1^m, q)$, где T_A — короткий базис.
2. Для $i = 0, \dots, l$:
 - 2.1. Выбрать $A_i \in \mathbb{Z}_q^{m \times n}$.
 - 2.2. $(B_i, S'_i) \leftarrow \text{SuperSamp}(1^n, 1^m, q, A_i)$.
 - 2.3. Выбрать $\beta \approx \sqrt{mn \log q \log m}$.
 - 2.4. $S_i \leftarrow \text{RandBasis}(S'_i, \beta)$.
3. Для $j = 0, \dots, N - 1$:
 - 3.1. $id_j = id_j[0] \dots id_j[l] \in \{0, 1\}^l$.
 - 3.2. $A_{id_j} \leftarrow \frac{A}{A_0 + \sum_{i=1}^l id_j[i] A_i} \in \mathbb{Z}_q^{2^m \times n}$.
 - 3.3. $T'_{id_j} \leftarrow \text{ExtBasis}(A_{id_j}, T_A)$.
 - 3.4. Выбрать $\beta \approx \sqrt{mn \log q \log m}$.
 - 3.5. $T_{id_j} \leftarrow \text{RandBasis}(T'_{id_j}, \beta)$.
 - 3.6. $gsk[j] \leftarrow T_{id_j}$.
4. $gmsk \leftarrow \{S_i\}_{i=0}^l$ — закрытый ключ менеджера группы, $gpk \leftarrow (A, \{A_i, B_i\}_{i=0}^l)$.

Sign:

Вход: $gsk[j], gpk, M$.

Выход: подпись Σ .

1. $(x_1^r \mid x_2^r)^r \leftarrow \text{GPVSample}(gsk[j], r)$.
2. Выбрать $s_0 \in \mathbb{Z}_q^n$ и вычислить шифртекст $c_0 = B_0 s_0 + x_2 \in \mathbb{Z}_q^m$.
3. Выбрать $s \in \mathbb{Z}_q^n$.
4. Для $i = 0, \dots, l$ вычислить $e_i \leftarrow D_{\mathbb{Z}^m, \alpha q}$, $c_i \leftarrow B_i s + p e_i + id_j[i] x_2$.
5. Сформировать доказательство с нулевым разглашением:

$$\pi_0 \leftarrow \{(B_0, c_0, \sqrt{2}\sigma/q, s_0) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^n \times \mathbb{Q} \times \mathbb{Z}^m: \\ (s_0^r B_0 = c_0^r) \wedge (\|x\| \leq \beta)\}.$$

6. Для $i = 1, \dots, l$ сформировать доказательство с нулевым разглашением $\pi_{OR,i}$ аналогично п. 5 с параметрами

$$((B_i \mid B_0), p^{-1}(c_i - c_0), \sqrt{2}\alpha, (s^r \mid (-s_0^r))^r).$$

7. Для $i = 0, \dots, l$ вычислить $y_i \leftarrow id_j[i]x_2 \in \mathbb{Z}^m$ и сформировать доказательство с нулевым разглашением π_K для e_i, y_i, x_1 :

$$x_1^T A + \sum_{i=0}^l c_i^T A_i = \sum_{i=1}^l e_i^T (pA_i); \quad e_i^T (pA_i) + y_i^T A_i = c_i^T A_i.$$

8. Положить $\Sigma = ((c_i)_{0 \leq i \leq l}, \pi_0, (\pi_{OR,i})_{1 \leq i \leq l}, \pi_K)$.

Verify:

Вход: gpk, M, Σ .

Выход: Заключение о правильности подписи.

1. Преобразовать подпись в форму

$$\Sigma \rightarrow ((c_i)_{0 \leq i \leq l}, \pi_0, (\pi_{OR,i})_{1 \leq i \leq l}, \pi_K).$$

2. Если доказательства $\pi_0, (\pi_{OR,i})_{1 \leq i \leq l}, \pi_K$ корректны, то подпись верна. Иначе — подпись неверна.

Open:

Вход: $gmsk, gpk, M, \Sigma$.

Выход: Идентификатор id пользователя.

1. Преобразовать подпись в форму

$$\Sigma \rightarrow ((c_i)_{0 \leq i \leq l}, \pi_0, (\pi_{OR,i})_{1 \leq i \leq l}, \pi_K).$$

2. Восстановить $x_2 \leftarrow Decrypt(c_0, S_0)$.

3. Для $i = 1, \dots, l$, используя S_i , определить, какой из двух векторов — $p^{-1}c_i$ или $p^{-1}(c_i - x_2)$ — близок к линейной оболочке B_i над $\mathbb{Z}_q$. В первом случае положить $id[i] \leftarrow 0$, иначе $id[i] \leftarrow 1$;

4. Положить $id \leftarrow id[0] \dots id[l]$.

Данная схема является корректной, отслеживаемой, обеспечивает анонимность, малый размер подписи и более высокую скорость по сравнению с протоколом DKV.

К недостаткам протокола можно отнести:

- отсутствие возможности отзыва права подписи и проверки правильности раскрытия подписи (без знания какого-либо секрета);
- отсутствие механизма добавления нового пользователя и невозможность его организации (по построению).

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

4. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.
5. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.
6. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

1. Коршунов, Г. И. K70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.
3. А.И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.а. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.:Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли ; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей : учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск : Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -
3. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/> -
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>
5. Интернет портал Защита-информации.SU <http://www.iso27000.ru/>
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>
7. Консорциум сетевых электронных библиотек ЭБС «Лань» <https://e.lanbook.com/>
8. ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/> -
9. ЭБС IPR SMART <https://www.iprbookshop.ru/>
10. ЭБС Znanium <https://znanium.com/>
11. ЭБС «Юрайт» <http://www.biblio-online.ru>
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

1. Используя теоретический материал, представленный в методических рекомендациях, исследовать схемы групповой подписи на решетках по протоколу LLLS. Особое внимание обратить на то, что в основе протокола LLLS лежит парадигма шифрования сертификата участника группы на открытом ключе. Тем самым участник может предоставить не интерактивное доказательство того, что зашифрованный текст содержит его действительный сертификат. Идея модели состоит в том, чтобы шифровать не долговременный сертификат участника, а разовый сертификат, который генерируется при каждом формировании подписи, наследуется от исходного и шифруется вместе с доказательством. (90 минут).

2. В соответствии с вариантами лабораторной работы №1 осуществить синтез основных алгоритмов протокола LLLS в соответствии с порядком, представленным в методических рекомендациях (90 минут).

№ Варианта	Размер группы	Параметр безопасности
46.	2	4
47.	3	5
48.	4	6
49.	5	7
50.	6	3
51.	7	4
52.	8	5
53.	9	7
54.	10	5
55.	11	4
56.	12	3
57.	13	5
58.	14	7
59.	15	8
60.	16	5

Цель работы состоит в реализации основных алгоритмов протокола LLLS в соответствии с порядком, представленным в методических рекомендациях с последующим заключением о правильности подписи.

Результаты лабораторной работы занести в отчет

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

- формулировку темы лабораторной работы;

- формулировку цели и решаемых в ходе лабораторной работы задач;
- порядок выполнения лабораторной работы с учетом достижения целевой установки;
- выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

Лабораторная работа №6

Построение схемы групповой подписи на решетках с процедурой отзыва по протоколу DKV-DVLR.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».
8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.

9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 ХР».
10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».
13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».
14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».
15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.
16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».
17. Программное изделие «Kaspersky Endpoint Security for Aurora».
18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.
19. Программное комплекс Acronis Backup & Recovery.
20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.
21. Программное обеспечение Oracle Identity Access Management Suite.
22. Программное обеспечение SafeNet Authentication Service.
23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.
24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».
25. Программный комплекс «InfoWatch Traffic Monitor».
26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.
27. Программный комплекс защиты информации от НСД «Страж 1.1».
28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.
29. Программный комплекс обнаружения вторжений «Ребус-СОВ».
30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»
31. Специальное программное обеспечение «АС «ГРИФ».
32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».
2. Аппаратно-программный комплекс шифрования «Континент».
3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95».
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1».
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- **ЗАПРЕЩАЕТСЯ:** переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

1. Повторить теоретический материал лекций по темам «Реализация групповой подписи в киберфизической системе», «Криптографические протоколы в условиях ограниченных вычислительных ресурсов».
2. Изучить теоретический материал данного занятия.
3. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Что нужно для успешного функционирования системы обеспечения кибербезопасности?
2. Кем и когда была предложена схема групповой подписи?
3. Какими свойствами обладает групповая подпись?
4. Для чего могут быть использованы групповые подписи?
5. Перечислите участников схемы групповой подписи?

6. Какие функции в схеме реализации групповой подписи выполняет менеджер (координатор) группы?

7. Какие функции в схеме реализации групповой подписи выполняет выпускающий менеджер?

8. Какие функции в схеме реализации групповой подписи выполняет раскрывающий менеджер?

9. Какие функции в схеме реализации групповой подписи выполняют члены группы?

10. Из каких процедур обычно состоит схема групповой подписи?

11. Какие схемы групповой подписи могут реализовываться в КФС?

12. Какие требования предъявляются к протоколам групповых подписей?

13. Поясните что из себя представляет свойство полной анонимности при реализации групповой подписи?

14. Какими дополнительными свойствами может обладать групповая подпись в КФС в зависимости от решаемой прикладной задачи?

15. Чем определяется эффективность схемы групповой подписи?

16. Что из себя представляет классификационная схема групповых подписей?

17. По каким признакам можно классифицировать схемы групповой подписи?

18. Перечислите участников процедуры выдачи/получения сертификатов при реализации одной из схем групповой подписи.

19. Что подразумевает использование в схеме групповой подписи временного токена?

20. Рост числа разнородных интеллектуальных устройств, имеющих доступ в Интернет, накладывает ряд ограничений на используемые технологии и технологические решения, применяемые для обеспечения защитных функций, назовите эти ограничения.

21. Приведите примеры малоресурсных систем.

22. Основные особенности малоресурсных систем.

23. Чем осложнена криптографическая защита малоресурсных систем?

24. Дайте характеристику понятию - личностная криптография.

25. В чем особенности личностных криптосистем?

26. Какова процедура выработки ключа в личностной криптосистеме?

27. Для реализации в FANET- сети может быть использована личностная схема шифрования с подписью, чем определяется такая возможность?

28. Что включает в себя личностная схема шифрования с подписью?

29. Поясните состав модели связи для интеграции беспроводных датчиков в Интернете вещей.

30. По каким причинам возникает необходимость аутсорсинга вычислений?

31. Что необходимо для создания аутсорс-версии криптографического алгоритма ALG?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование схемы групповой подписи на решетках с процедурой отзыва по протоколу DKV-DVLR	- 80 мин
2. Синтез схемы групповой подписи на решетках с процедурой отзыва по протоколу DKV-DVLR	- 60 мин
3. Тестирование по теме 3	20 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.
Всего	- 180 мин

Основные теоретические сведения

Групповая подпись на решетках с процедурой отзыва по протоколу DKV-DVLR

Дополним схему DKV процедурой VLR-отзыва. При этом потребуем, чтобы схема сохранила свойства анонимности и отслеживаемости; кроме того, можно обеспечить полную ССА-анонимность.

Для вышеописанной модели механизм VLR-отзыва будет выглядеть следующим образом. В списке отзыва RL , доступном только раскрывающему менеджеру, находятся мастер-ключи S_i , соответствующие отозванным пользователям. Для проверки подписи менеджер будет выполнять действия согласно протоколу $Is_Revoked$.

Кроме того, во время формирования подписи необходимо добавлять временную метку для того, чтобы сформированные пользователем до отзыва сообщения считались неотозванными, что в данном случае обеспечит выполнение свойства несопоставимости.

Для добавления в схему DKV нового члена в группу с N участниками необходимо выполнить дополнительное вычисление параметров для нового члена по алгоритму $Join$.

Процедуры $Setup$ и $Open$ выполняются так же, как в базовом протоколе.

Sign:

Вход: $gsk[j]$ — персональный закрытый ключ j -го пользователя, M — сообщение.

Выход: Подпись σ .

1. Сгенерировать случайную строку $r \leftarrow \{0, 1\}^n$.
2. Для $1 \leq i \leq N$ вычислить $h_i \leftarrow H(M || r || i)$.
3. Положить $e_j \leftarrow GPVInvert(A_j, T_j, s, h_j)$.
4. Для $1 \leq i \leq N, i \neq j$, найти e_i , решив систему $A_i e_i = h_i \pmod{q}$.
5. Для $1 \leq i \leq N$ выбрать произвольный вектор $s_i \in \mathbb{Z}_q^n$ и вычислить $z_i = B_i^T s_i + e_i \pmod{q} \in \mathbb{Z}_q^m$.
6. Сформировать доказательство π по протоколу NIWI (noninteractive witness-indistinguishable [65]) с помощью параметра γ .
7. Положить $t \leftarrow timestamp()$, где $timestamp$ — функция, возвращающая временную метку, содержащую текущую дату и время.
8. Подписью является кортеж $\sigma = (r, z_1, \dots, z_N, \pi, t)$.

Verify:

Вход: PK, M, σ .

Выход: 0 или 1.

1. Преобразовать подпись в форму $\sigma \leftarrow (r, z_1, \dots, z_N, \pi, t)$;
2. Вернуть 0, если $IS_REVOKED(M, \sigma) = 1$;
3. Вернуть 1, если доказательство π корректно и $A_i z_i = H(M || r || i)$ для всех $1 \leq i \leq N$. Иначе вернуть 0.

Is_Revoked:

Вход: $TK = RL, M, \sigma$.

Выход: право подписи отозвано/не отозвано.

1. Преобразовать подпись σ в форму $(r, z_1, \dots, z_N, \pi, t)$
2. Для каждого $\{S_i, t_i\} \in RL$ вернуть «сертификат отозван», если

$$\begin{cases} \text{dist}(L(B_i^T, z_i)) \leq s\sqrt{m}; \\ t \geq t_i. \end{cases}$$

3. Вернуть «сертификат не отозван».

Join:

Вход: $1^n, 1^{N+1}$.

Выход: $TK, PK, \overrightarrow{gsk}$.

1. $(B_{N+1}, S'_{N+1}) \leftarrow \text{TrapSamp}(1^n, 1^m, q)$.
2. $(A_{N+1}, T_{N+1}) \leftarrow \text{SuperSamp}(1^n, 1^m, q, B_{N+1})$.
3. $S_{N+1} \leftarrow \text{RandBasis}(S'_{N+1})$.
4. Добавить (A_{N+1}, B_{N+1}) в PK , T_{N+1} — в $\overrightarrow{gsk}$, S_{N+1} — в TK .

Для доказательства корректности схемы DKV-DVLR достаточно показать, что открытый ключ группы PK , набор секретных ключей пользователей $\overrightarrow{gsk}$ и набор маркеров отзыва $\{S_i, t_i\}$ сформированы таким образом, что алгоритм *Verify* выдает значение «подпись верна» тогда и только тогда, когда маркер (S_j, t_j) , соответствующий сформировавшему данную подпись

j -му пользователю, не содержится в списке отозванных, т. е.

$$\text{Verify}(PK, M, \sigma) = \text{True} \Leftrightarrow \begin{cases} (S_j, t_j) \notin RL, \\ t < t_j. \end{cases}$$

Кроме того, схема обладает свойствами анонимности и отслеживаемости.

В данной расширенной схеме:

- выполняются основные требования, предъявляемые к групповым подписям;
- расширен функционал за счет процедур отзыва и добавления новых членов;
- размер подписи напрямую зависит от числа пользователей.

Таким образом, данная схема рекомендуется к использованию в активно расширяющихся системах, не имеющих жестких ограничений по использованию ресурсов.

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.
2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.
3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

1. Коршунов, Г. И. K70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.
3. А.И. Астайкина. Саратов: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.а. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.:Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли ; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей : учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск : Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -
3. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/> -
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>
5. Интернет портал Защита-информации.SU <http://www.iso27000.ru/>
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>
7. Консорциум сетевых электронных библиотек ЭБС «Лань» <https://e.lanbook.com/>
8. ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/> -
9. ЭБС IPR SMART <https://www.iprbookshop.ru/>
10. ЭБС Znanium <https://znanium.com/>
11. ЭБС «Юрайт» <http://www.biblio-online.ru>
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

1. Используя теоретический материал, представленный в методических рекомендациях к лабораторной работе, исследовать схему групповой подписи на решетках с процедурой отзыва по протоколу DKV-DVLR. Особое внимание обратить на то, что во время формирования подписи по протоколу DKV-DVLR необходимо добавлять временную метку для того, чтобы сформированные пользователем до отзыва сообщения считались неотозванными, что в данном случае обеспечит выполнение свойства несопоставимости, а для добавления в схему DKV нового члена в группу с участниками необходимо выполнить дополнительное вычисление параметров для нового члена по алгоритму Join (90 минут).

2. В соответствии с вариантами лабораторной работы осуществить синтез схемы групповой подписи на решетках с процедурой отзыва по протоколу DKV-DVLR. Реализовать все этапы алгоритма протокола по описанной в методической разработке методике (90 минут.).

№ Варианта	Число членов группы и число добавления участников
61.	2+1
62.	3+2
63.	4+3
64.	5+2
65.	6+4
66.	7+1
67.	8+2
68.	9+3
69.	10+4
70.	11+5
71.	12+1
72.	13+4
73.	14+2
74.	15+5
75.	16+3

Цель работы состоит в обосновании корректности схемы DKV-DVLR, а именно доказательстве того, что открытый ключ группы, набор секретных ключей пользователей и набор маркеров отзыва сформированы таким

образом, что алгоритм Verify выдает значение «подпись верна».

Результаты лабораторной работы занести в отчет

3. За 20 минут до окончания занятий проводится тестирование по теме №3. Вопросы тестирования охватывают теоретический материал, выданный на лекционных занятиях.

Перечень вопросов выносимый на процедуру тестирования.

1. Что нужно для успешного функционирования системы обеспечения кибербезопасности?
2. Кем и когда была предложена схема групповой подписи?
3. Какими свойствами обладает групповая подпись?
4. Для чего могут быть использованы групповые подписи?
5. Перечислите участников схемы групповой подписи?
6. Какие функции в схеме реализации групповой подписи выполняет менеджер (координатор) группы?
7. Какие функции в схеме реализации групповой подписи выполняет выпускающий менеджер?
8. Какие функции в схеме реализации групповой подписи выполняет раскрывающий менеджер?
9. Какие функции в схеме реализации групповой подписи выполняют члены группы?
10. Из каких процедур обычно состоит схема групповой подписи?
11. Какие схемы групповой подписи могут реализовываться в КФС?
12. Какие требования предъявляются к протоколам групповых подписей?
13. Поясните что из себя представляет свойство полной анонимности при реализации групповой подписи?
14. Какими дополнительными свойствами может обладать групповая подпись в КФС в зависимости от решаемой прикладной задачи?
15. Чем определяется эффективность схемы групповой подписи?
16. Что из себя представляет классификационная схема групповых подписей?
17. По каким признакам можно классифицировать схемы групповой подписи?
18. Перечислите участников процедуры выдачи/получения сертификатов при реализации одной из схем групповой подписи.
19. Что подразумевает использование в схеме групповой подписи временного токена?
20. Рост числа разнородных интеллектуальных устройств, имеющих доступ в Интернет, накладывает ряд ограничений на используемые технологии и технологические решения, применяемые для обеспечения защитных функций, назовите эти ограничения.
21. Приведите примеры малоресурсных системы.
22. Основные особенности малоресурсных систем.

23. Чем осложнена криптографическая защита малоресурсных систем?
24. Дайте характеристику понятию - личностная криптография.
25. В чем особенности личностных криптосистем?
26. Какова процедура выработки ключа в личностной криптосистеме?
27. Для реализации в FANET- сети может быть использована личностная схема шифрования с подписью, чем определяется такая возможность?
28. Что включает в себя личностная схема шифрования с подписью?
29. Поясните состав модели связи для интеграции беспроводных датчиков в Интернете вещей.
30. По каким причинам возникает необходимость аутсорсинга вычислений?
31. Что необходимо для создания аутсорс-версии криптографического алгоритма ALG?

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

- формулировку темы лабораторной работы;
- формулировку цели и решаемых в ходе лабораторной работы задач;
- порядок выполнения лабораторной работы с учетом достижения целевой установки;
- выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

Лабораторная работа №7

Построение схемы групповой подписи на решетках с процедурой отзыва по протоколу LLLS-VLR.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».
8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.

9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 ХР».
10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».
13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».
14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».
15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.
16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».
17. Программное изделие «Kaspersky Endpoint Security for Aurora».
18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.
19. Программное комплекс Acronis Backup & Recovery.
20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.
21. Программное обеспечение Oracle Identity Access Management Suite.
22. Программное обеспечение SafeNet Authentication Service.
23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.
24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».
25. Программный комплекс «InfoWatch Traffic Monitor».
26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.
27. Программный комплекс защиты информации от НСД «Страж 1.1».
28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.
29. Программный комплекс обнаружения вторжений «Ребус-СОВ».
30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»
31. Специальное программное обеспечение «АС «ГРИФ».
32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».
2. Аппаратно-программный комплекс шифрования «Континент».
3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95».
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1».
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

1. Повторить теоретический материал лекций по темам «Криптографические протоколы в условиях ограниченных вычислительных ресурсов», «Реализация коллективной упорядоченной подписи в киберфизических системах», «Реализация направленной подписи с делегированием полномочий в киберфизических системах».
2. Изучить теоретический материал данного занятия.
3. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Как ассоциируется при реализации групповой аутентификации каждый участник группы?
2. Что не позволяют сделать пороговые подписи?

3. Какую разновидность представляет собой упорядоченная цифровая?
4. Почему использование единой коллективной подписи фиксированной длины, реализованной при участии нескольких пользователей актуально?
5. Какую подпись необходимо использовать если нужна верификация не только самой подписи, но и порядка ее создания?
6. Что такое композиционный подход?
7. Каким требованиям должны удовлетворять оптимальные схемы упорядоченных подписей?
8. С помощью чего осуществляется формирование упорядоченной подписи?
9. Какую проблему позволяет решить применение упорядоченной цифровой подписи?
10. На какой задаче основаны многие протоколы коллективной, в том числе и упорядоченной, цифровой подписи?
11. Что является особенностью большинства схем цифровой подписи?
12. Что является проблемой неоспоримой подписи?
13. Как реализуется интерактивность при реализации неоспоримой электронной подписи?
14. Что из себя представляет направленная подпись, в чем ее специфика?
15. Какими свойствами обладает направленная подпись?
16. Поясните работу общей схемы направленной подписи.
17. Кто и когда предложил одну из первых частично гомоморфных схем шифрования?
18. Кто предложили криптосистему на основе билинейных отображений на эллиптических кривых?
19. Кто впервые построил теоретическую модель полностью гомоморфной криптосистемы?
20. Что из себя представляет гомоморфная криптосистема, дайте ей характеристику?
21. Какие алгоритмы включает в себя гомоморфная криптосистема?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование схемы групповой подписи на решетках с процедурой отзыва по расширенному протоколу LLLS-VLR	- 80 мин
2. Синтез схемы групповой подписи на решетках с процедурой отзыва по расширенному протоколу	- 80 мин

LLLS-VLR

Заключение

- 3 мин.

Задание студентам для самостоятельной работы

- 2 мин.

Всего

- 180 мин

Основные теоретические сведения

Групповая подпись на решетках с процедурой отзыва по расширенному протоколу LLLS-VLR

В протоколе LLLS предлагается организовать VLR-отзыв следующим образом. В списке отзыва, доступном только раскрывающему менеджеру, находятся идентификаторы пользователей $id \in \{0, 1\}^l$. Для проверки подписи менеджер выполняет действия согласно процедуре *Is_Revoked*. Кроме того, как и при расширении протокола DKV, во время формирования подписи необходимо добавлять временную метку, что обеспечит выполнение свойства несопоставимости.

Процедуры *Setup* и *Open* выполняются так же, как в базовом протоколе.

Sign:

Вход: $gsk[j], gpk, M$.

Выход: подпись Σ .

1. $(x_1^T \mid x_2^T)^T \leftarrow GPVSample(gsk[j], r)$.
2. Выбрать $s_0 \in \mathbb{Z}_q^n$ и вычислить шифртекст $c_0 = B_0 s_0 + x_2 \in \mathbb{Z}_q^m$.
3. Выбрать $s \in \mathbb{Z}_q^n$.
4. Для $i = 0, \dots, l$ вычислить $e_i \leftarrow D_{\mathbb{Z}^m, \alpha q}$, $c_i \leftarrow B_i s + p e_i + id_j[i] x_2$.
5. Сформировать доказательство с нулевым разглашением:

$$\pi_0 \leftarrow \{(B_0, c_0, \sqrt{2}\sigma/q, s_0) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^n \times Q \times \mathbb{Z}^m: \\ (s_0^T B_0 = c_0^T) \wedge (\|x\| \leq \beta)\}.$$

6. Для $i = 1, \dots, l$ сформировать доказательство с нулевым разглашением $\pi_{OR,i}$ аналогично п. 5 с параметрами

$$((B_i \mid B_0), p^{-1}(c_i - c_0), \sqrt{2}\alpha, (s^T \mid (-s_0^T))^T).$$

7. Для $i = 0, \dots, l$ вычислить $y_i \leftarrow id_j[i] x_2 \in \mathbb{Z}^m$ и сформировать доказательство с нулевым разглашением π_K для e_i, y_i, x_1 :

$$x_1^T A + \sum_{i=0}^l c_i^T A_i = \sum_{i=0}^l e_i^T (p A_i); \quad e_i^T (p A_i) + y_i^T A_i = c_i^T A_i.$$

8. Положить $t \leftarrow timestamp()$, где *timestamp* — функция, возвращающая временную метку, содержащую текущую дату и время.

9. Положить $\Sigma = ((c_i)_{0 \leq i \leq l}, \pi_0, (\pi_{OR,i})_{1 \leq i \leq l}, \pi_K, t)$.

Verify:

Вход: gpk, M, Σ .

Выход: Заключение о правильности подписи.

1. Преобразовать подпись в форму

$$\Sigma \rightarrow ((c_i)_{0 \leq i \leq l}, \pi_0, (\pi_{OR,i})_{1 \leq i \leq l}, \pi_K, t).$$

2. Если $Is_Revoked(M, \Sigma) = 1$, то подпись неверна.
3. Если доказательства $\pi_0, (\pi_{OR,i})_{1 \leq i \leq l}, \pi_K$ корректны, то подпись верна.

Иначе — подпись неверна.

Is_Revoked:

Вход: $gmsk, gpk, M, \Sigma$.

Выход: Вывод о том, отозвано ли право подписи у пользователя, сформировавшего подпись.

1. Преобразовать подпись в форму

$$\Sigma \rightarrow ((c_i)_{0 \leq i \leq l}, \pi_0, (\pi_{OR,i})_{1 \leq i \leq l}, \pi_K, t);$$

2. Восстановить $x_2 \leftarrow Decrypt(c_0, S_0)$;
3. Для $1 \leq i \leq l$ по известному значению c_i восстановить значение e_i .
4. Для каждого $(id, t_{id}) \in RL$:

Для $1 \leq i \leq l$:

- 4.1. Восстановить $y_i \leftarrow id[i]x_2$.
- 4.2. Вернуть «сертификат отозван», если:

$$\begin{cases} e_i^T(pA_i) + y_i^T A_i = c_i^T A_i; \\ t > t_{id}. \end{cases}$$

5. Вернуть «сертификат не отозван».

Аналогично предыдущему случаю для доказательства корректности схемы LLL-VLR достаточно показать, все структуры данных сформированы таким образом, что алгоритм *Verify* выдает значение «подпись верна» тогда и только тогда, когда маркер (id, t_{id}) , соответствующий пользователю id , не содержится в списке отозванных, т.е.

$$Verify(gpk, M, \sigma) = True \Leftrightarrow \begin{cases} (id, t_{id}) \notin RL \\ t < t_{id}. \end{cases}$$

Схема LLL-VLR обладает свойствами анонимности и отслеживаемости, удовлетворяет основным требованиям, предъявляемым к групповым подписям, обеспечивает малый размер подписи, имеет возможность отзыва подписи, не может быть расширена до динамической схемы, поскольку выбираемые на этапе инициализации системы параметры безопасности напрямую зависят от предполагаемого числа участников в группе.

Таким образом, данная схема рекомендуется к использованию в организациях, где структура со временем не претерпевает значительных изменений, а также в силу своего малого размера подойдет для систем с ограниченными ресурсами.

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.
2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.
3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

1. Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.
3. А.И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.а. Мельников. — 3-е изд., стер. — М.: Флинта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М: Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли ; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей: учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск: Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -
3. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/> -
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>
5. Интернет портал Защита-информации.SU <http://www.iso27000.ru/>
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>
7. Консорциум сетевых электронных библиотек ЭБС «Лань» <https://e.lanbook.com/>
8. ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/> -
9. ЭБС IPR SMART <https://www.iprbookshop.ru/>
10. ЭБС Znanium <https://znanium.com/>
11. ЭБС «Юрайт» <http://www.biblio-online.ru>
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

1. Используя теоретический материал, представленный в методических рекомендациях к лабораторной работе, исследовать схемы групповой подписи на решетках с процедурой отзыва по расширенному протоколу LLLS-VLR. Особое внимание обратить на то, что в протоколе LLLS предлагается организовать VLR-отзыв специальным образом. В списке отзыва, доступном только раскрывающему менеджеру, находятся идентификаторы пользователей. Для проверки подписи менеджер выполняет действия исключительно согласно процедуре *Is_Revoked*. Кроме того, как и при расширении протокола DKV, во время формирования подписи необходимо добавлять временную метку, что обеспечит выполнение свойства несопоставимости (90 минут).

2. В соответствии с вариантами лабораторной работы осуществить синтез схемы групповой подписи на решетках с процедурой отзыва по расширенному протоколу LLLS-VLR. При этом в соответствии с последовательностью этапов разработки протокола сформировать алгоритмы с фиксацией элементов входа и выхода (90 минут).

№ Варианта	Число членов группы	Количество отозванных пользователей
76.	2	2
77.	3	4
78.	4	6
79.	5	5
80.	6	4
81.	7	3
82.	8	2
83.	9	5
84.	10	6
85.	11	4
86.	12	6
87.	13	7
88.	14	5
89.	15	4
90.	16	3

Цель работы состоит в подтверждении корректности схемы LLL-VLR в ходе которой достаточно показать, что все структуры данных сформированы таким образом, что алгоритм *Verify* выдает значение «подпись верна» только

тогда, когда маркер (*id*, *t_{id}*), соответствующий пользователю *id*, не содержится в списке отозванных.

Результаты лабораторной работы занести в отчет

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

- формулировку темы лабораторной работы;
- формулировку цели и решаемых в ходе лабораторной работы задач;
- порядок выполнения лабораторной работы с учетом достижения целевой установки;
- выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

Тема 4: Криптографические протоколы аутентификации в киберфизических системах

Лабораторная работа №8

Построение криптографического протокола на основе аутсорс-алгоритмов
вычисления билинейного отображения.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».

8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.
9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 XP».
10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».
13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».
14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».
15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.
16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».
17. Программное изделие «Kaspersky Endpoint Security for Aurora».
18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.
19. Программное комплекс Acronis Backup & Recovery.
20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.
21. Программное обеспечение Oracle Identity Access Management Suite.
22. Программное обеспечение SafeNet Authentication Service.
23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.
24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».
25. Программный комплекс «InfoWatch Traffic Monitor».
26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.
27. Программный комплекс защиты информации от НСД «Страж 1.1».
28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.
29. Программный комплекс обнаружения вторжений «Ребус-СОВ».
30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»
31. Специальное программное обеспечение «АС «ГРИФ».

32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».
2. Аппаратно-программный комплекс шифрования «Континент».
3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95.
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1.
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

1. Повторить теоретический материал лекций по темам «Криптографические протоколы в условиях ограниченных вычислительных ресурсов», «Реализация коллективной упорядоченной подписи в киберфизических системах», «Реализация направленной подписи с делегированием полномочий в киберфизических системах».
2. Изучить теоретический материал данного занятия.
3. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Как ассоциируется при реализации групповой аутентификации каждый участник группы?
2. Что не позволяют сделать пороговые подписи?
3. Какую разновидность представляет собой упорядоченная цифровая?
4. Почему использование единой коллективной подписи фиксированной длины, реализованной при участии нескольких пользователей актуально?
5. Какую подпись необходимо использовать если нужна верификация не только самой подписи, но и порядка ее создания?
6. Что такое композиционный подход?
7. Каким требованиям должны удовлетворять оптимальные схемы упорядоченных подписей?
8. С помощью чего осуществляется формирование упорядоченной подписи?
9. Какую проблему позволяет решить применение упорядоченной цифровой подписи?
10. На какой задаче основаны многие протоколы коллективной, в том числе и упорядоченной, цифровой подписи?
11. Что является особенностью большинства схем цифровой подписи?
12. Что является проблемой неоспоримой подписи?
13. Как реализуется интерактивность при реализации неоспоримой электронной подписи?
14. Что из себя представляет направленная подпись, в чем ее специфика?
15. Какими свойствами обладает направленная подпись?
16. Поясните работу общей схемы направленной подписи.
17. Кто и когда предложил одну из первых частично гомоморфных схем шифрования?
18. Кто предложили криптосистему на основе билинейных отображений на эллиптических кривых?
19. Кто впервые построил теоретическую модель полностью гомоморфной криптосистемы?
20. Что из себя представляет гомоморфная криптосистема, дайте ей характеристику?
21. Какие алгоритмы включает в себя гомоморфная криптосистема?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование алгоритма BilinearMap1 и BilinearMap2	- 80 мин

2. Синтез протокола на базе алгоритма BilinearMap1	- 80 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.
Всего	- 180 мин

Основные теоретические сведения

Криптографический протокол на основе аутсорс-алгоритмов вычисления билинейного отображения

Билинейные отображения позволяют строить широкий спектр криптографических протоколов для самоорганизующихся сетей, использующих устройства с малым вычислительным ресурсом, для которых вычисление билинейного отображения является трудоемкой операцией.

Первый аутсорс-протокол для вычисления спаривания точек эллиптических кривых был предложен в [2]. Здесь использованы два обособленных друг от друга, ненадежных, а значит, и потенциально опасных сервера. Кроме того, в алгоритме необходимо многократно проверять тестовые значения, требующие возведения в степень в конечном поле и вычисления мультипликативно обратных. Позже в тех же условиях использования серверов сложность вычислений была несколько снижена.

В другой модели использования серверов тестовые значения вычисляются во время простоя устройства с ограниченными ресурсами, при этом не требуются операции возведения в степень и нахождения мультипликативно обратных. Кроме того, в этой схеме сокращено число онлайн-вычислений на стороне клиента — маломощного устройства: для вычисления билинейного отображения $e: G_1 \times G_2 \rightarrow G_3$ необходимо произвести пять сложений в группах G_1 и G_2 и четыре умножения в группе G_3 . В [2] предложен еще более эффективный аутсорс-алгоритм, предполагающий четыре сложения в группах G_1 и G_2 и три умножения в группе G_3 .

Наиболее эффективные аутсорс-алгоритмы вычисления билинейных отображений предполагают вычисления в рамках модели OMTUP и выполняются в два этапа: предвычисления и собственно аутсорс-алгоритм.

Алгоритм BilinearMap1

Этап 1. Предвычисления. На данном этапе формируются таблицы: статическая, ST, и динамическая, DT. Значения в динамической таблице заменяются по мере использования, во время простоя устройства таблица восстанавливается. Значения таблицы генерируются заранее доверенным участником и загружаются в память устройства T .

Пусть P_1 и P_2 — образующие групп G_1 и G_2 соответственно. Необходимо сгенерировать n случайных элементов $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_q$ и вычислить точки $\beta_{j1} = \alpha_j P_1$ и $\beta_{j2} = \alpha_j P_2$ для всех $j = 1, \dots, n$.

В статическую таблицу ST записываются значения $\alpha_j, \beta_{j1}, \beta_{j2}$ и значение билинейного отображения $e(P_1, P_2) \in G_3$.

Для формирования новой записи в динамической таблице DT необходимо:

- выбрать случайное подмножество $S \subset \{1, \dots, n\}$ мощности k ;
- для каждого $j \in S$ выбрать случайное значение $K_j \in \{1, \dots, h-1\}$, где $h > 1$ — малое целое число;
- вычислить $x_1 \equiv \sum_{j \in S} \alpha_j K_j \pmod{q}$; при $x_1 \equiv 0 \pmod{q}$ вернуться к началу процедуры, иначе вычислить $x_1 P_1 = \sum_{j \in S} K_j \beta_{j1}$;
- вычислить $2x_1 P_1, -2x_2 P_2, e(P_1, P_2)^{2x_1 x_2}$ и $e(P_1, P_2)^{x_3 x_4}$;
- внести в динамическую таблицу DT запись

$$(x_1 P_1; 2x_1 P_1; x_3 P_1; x_2 P_2; -2x_2 P_2; x_4 P_2, e(P_1, P_2)^{2x_1 x_2}, e(P_1, P_2)^{x_3 x_4}).$$

При каждом вызове функции предвычислений значение для вычислений берется из таблицы DT, таблица очищается. Для очередных вычислений необходимо сгенерировать новый набор значений.

Этап 2. Аутсорс-вычисления. Данная процедура по паре точек (P, Q) , где $P \in G_1, Q \in G_2$, выдает значение билинейного отображения $e(P, Q)$. Участник T (доверенное маломощное устройство) посылает для аутсорс-вычислений серверам U_1 и U_2 значения, полученные с помощью функции предвычислений. Предполагается, что нарушитель не должен знать, что является входом алгоритма BilinearMap1 и что получается на выходе. Выражение $U_i(P, Q) \rightarrow e(P, Q)$ означает, что сервер U_i , где $i = 1, 2$, по входным данным (P, Q) выдает значение $e(P, Q)$.

Устройство T выполняет процедуру предвычислений и получает значения

$$(x_1 P_1; 2x_1 P_1; x_3 P_1; x_2 P_2; -2x_2 P_2; x_4 P_2, \lambda = e(P_1, P_2)^{2x_1 x_2}, e(P_1, P_2)^{x_3 x_4}).$$

В случайном порядке устройство T запрашивает у сервера U_1 результаты вычислений: $U_1(P + 2x_1 P_1, -Q - 2x_2 P_2) \rightarrow \alpha_1$; $U_1(x_3 P_1; x_4 P_2) \rightarrow \alpha'_1$.

Аналогично, устройство T получает от сервера U_2 значения $U_2(P + x_1 P_1, Q + x_2 P_2) \rightarrow \alpha_2$; $U_2(x_3 P_1; x_4 P_2) \rightarrow \alpha'_2$.

T проверяет выполнение равенства $\alpha'_1 = \alpha'_2 = e(P_1, P_2)^{x_3 x_4}$ и в случае успешной проверки вычисляет искомое билинейное отображение $\beta = \alpha_1 \alpha_2^2 \lambda$.

При использовании модели OMTUP для повышения безопасности и ные уменьшения вероятности ошибки вычисления необходимо производить больше одного тестового запроса.

Алгоритм BilinearMap2

Этап 1. Предвычисления. Статическая таблица формируется так же, как в алгоритме BilinearMap1.

Для формирования новой записи в динамической таблице DT необходимо:

- выбрать случайное подмножество $S \subset \{1, \dots, n\}$ мощности k ;
- для каждого $j \in S$ выбрать случайное значение $K_j \in \{1, \dots, h-1\}$, где $h > 1$ — малое целое число;
- вычислить $x_1 \equiv \sum_{j \in S} \alpha_j K_j \pmod{q}$; при $x_1 \equiv 0 \pmod{q}$ вернуться к началу процедуры, иначе вычислить $x_1 P_1 = \sum_{j \in S} K_j \beta_{j1}$;
- аналогично вычислить пары $(x_2; x_2 P_2); (x_3; x_3 P_1); (x_4; x_4 P_2); (x_5; x_5 P_1)$;
- вычислить $(x_2 - x_1^{-1} x_2 x_3) P_2; e(P_1, P_2)^{x_4 x_5}$;
- внести в динамическую таблицу DT запись

$$(x_1 P_1; x_3 P_1; x_5 P_1; x_2 P_2; x_4 P_2; (x_2 - x_1^{-1} x_2 x_3) P_2; e(P_1, P_2)^{x_4 x_5}).$$

При каждом вызове функции предвычислений значение для вычислений берется из таблицы DT, таблица очищается. Для очередных вычислений необходимо сгенерировать новый набор значений.

Этап 2. Аутсорс-вычисления.

Аналогично алгоритму BilinearMap1, устройство T выполняет процедуру предвычислений и получает значения

$$(x_1 P_1; x_3 P_1; x_5 P_1; x_2 P_2; x_4 P_2; (x_2 - x_1^{-1} x_2 x_3) P_2; e(P_1, P_2)^{x_4 x_5}).$$

В случайном порядке устройство T запрашивает у сервера U_1 результаты вычислений: $U_1(P + x_1 P_1, Q + x_2 P_2) \rightarrow \alpha_1$; $U_1(x_5 P_1; x_4 P_2) \rightarrow \alpha'_1$.

Аналогично, устройство T получает от сервера U_2 значения

$$U_2(P + x_3 P_1, -x_2 P_2) \rightarrow \alpha_2; \quad U_2(-x_1 P_1, Q + (x_2 - x_1^{-1} x_2 x_3) P_2) \rightarrow \alpha_3;$$

$$U_2(x_5 P_1; x_4 P_2) \rightarrow \alpha'_2.$$

T проверяет выполнение равенства $\alpha'_1 = \alpha'_2 = e(P_1, P_2)^{x_4 x_5}$ и в случае успешной проверки вычисляет искомое билинейное отображение $\beta = \alpha_1 \alpha_2 \alpha_3$.

Объемы статических таблиц ST для обоих алгоритмов совпадают. Динамическая таблица DT содержит:

- для алгоритма BilinearMap1: три элемента группы G_1 , три элемента группы G_2 , два элемента группы G_3 ;
- для алгоритма BilinearMap2: три элемента группы G_1 , три элемента группы G_2 , один элемент группы G_3 .

Алгоритмы отличаются также числом операций, выполняемых на клиенте и на сервере. Число операций, производимых на клиенте (малоресурсном устройстве):

- для алгоритма BilinearMap1: два сложения элементов группы G_1 , два сложения элементов группы G_2 , два модульных умножения, одно модульное возведение в квадрат;
- для алгоритма BilinearMap2: два сложения элементов группы G_1 , два сложения элементов группы G_2 , два модульных умножения.

Таким образом, алгоритм BilinearMap1 несколько уступает алгоритму BilinearMap2.

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.
2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.
3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

1. Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.
3. А.И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.а. Мельников. — 3-е изд., стер. — М.: Флинта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.:Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли ; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей : учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск : Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -
3. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/> -
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>
5. Интернет портал Защита-информации.SU <http://www.iso27000.ru/>
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>
7. Консорциум сетевых электронных библиотек ЭБС «Лань» <https://e.lanbook.com/>
8. ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/> -
9. ЭБС IPR SMART <https://www.iprbookshop.ru/>
10. ЭБС Znanium <https://znanium.com/>
11. ЭБС «Юрайт» <http://www.biblio-online.ru>
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

1. Используя теоретический материал, представленный в методических рекомендациях к лабораторной работе, исследовать алгоритм BilinearMap1 и BilinearMap2. Особое внимание обратить на то, что наиболее эффективные аутсорс-алгоритмы вычисления билинейных отображений предполагают вычисления в рамках модели OMTUP и выполняются в два этапа: предвычисления и собственно аутсорс-алгоритм. Важной особенностью является то, что алгоритмы отличаются числом операций, выполняемых на клиенте и на сервере. (90 минут).

2. В соответствии с вариантами лабораторной работы осуществить синтез протокола используя для этого алгоритм BilinearMap1 (90 минут.).

№ Варианта	Количество доверенных участников
91.	2
92.	3
93.	4
94.	5
95.	6
96.	7
97.	8
98.	9
99.	10
100.	11
101.	12
102.	13
103.	14
104.	15
105.	16

Цель работы состоит в реализации алгоритма вычислений по этапу предвычисления и этапу аутсорс-вычисления при условии использования модели OMTUP для повышения безопасности и уменьшения вероятности ошибки.

Результаты лабораторной работы занести в отчет

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

- формулировку темы лабораторной работы;
- формулировку цели и решаемых в ходе лабораторной работы задач;
- порядок выполнения лабораторной работы с учетом достижения целевой установки;
- выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

Лабораторная работа №9

Построение криптографического протокола на основе аутсорс-алгоритмов вычисления билинейного отображения.

Реализуемые компетенции

Код	Формулировка	Индикаторы
ПК-2	Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах	Знать политику безопасности вычислительных сетей в киберфизических системах
ПК-3	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	Знать элементы системы управления информационной безопасностью киберфизических систем

Учебно-материальное обеспечение

Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, на 15 посадочных мест, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Программное обеспечение:

1. Защищенная операционная система реального времени «QNX».
2. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».
8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.

9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 ХР».

10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».

11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».

12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».

13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».

14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».

15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.

16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».

17. Программное изделие «Kaspersky Endpoint Security for Aurora».

18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.

19. Программное комплекс Acronis Backup & Recovery.

20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.

21. Программное обеспечение Oracle Identity Access Management Suite.

22. Программное обеспечение SafeNet Authentication Service.

23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.

24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».

25. Программный комплекс «InfoWatch Traffic Monitor».

26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.

27. Программный комплекс защиты информации от НСД «Страж 1.1».

28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Idesco UTM.

29. Программный комплекс обнаружения вторжений «Ребус-СОВ».

30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»

31. Специальное программное обеспечение «АС «ГРИФ».

32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Аппаратное обеспечение:

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».
2. Аппаратно-программный комплекс шифрования «Континент».
3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95».
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1».
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной лабораторной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Подготовка к занятию

1. Повторить теоретический материал лекций по темам «Криптографические протоколы в условиях ограниченных вычислительных ресурсов», «Реализация коллективной упорядоченной подписи в киберфизических системах», «Реализация направленной подписи с делегированием полномочий в киберфизических системах».
2. Изучить теоретический материал данного занятия.
3. Ознакомиться с заданием и методическими указаниями к лабораторной работе.
4. Ответить на контрольные вопросы.

Контрольные вопросы

1. Как ассоциируется при реализации групповой аутентификации каждый участник группы?
2. Что не позволяют сделать пороговые подписи?
3. Какую разновидность представляет собой упорядоченная цифровая?

4. Почему использование единой коллективной подписи фиксированной длины, реализованной при участии нескольких пользователей актуально?
5. Какую подпись необходимо использовать если нужна верификация не только самой подписи, но и порядка ее создания?
6. Что такое композиционный подход?
7. Каким требованиям должны удовлетворять оптимальные схемы упорядоченных подписей?
8. С помощью чего осуществляется формирование упорядоченной подписи?
9. Какую проблему позволяет решить применение упорядоченной цифровой подписи?
10. На какой задаче основаны многие протоколы коллективной, в том числе и упорядоченной, цифровой подписи?
11. Что является особенностью большинства схем цифровой подписи?
12. Что является проблемой неоспоримой подписи?
13. Как реализуется интерактивность при реализации неоспоримой электронной подписи?
14. Что из себя представляет направленная подпись, в чем ее специфика?
15. Какими свойствами обладает направленная подпись?
16. Поясните работу общей схемы направленной подписи.
17. Кто и когда предложил одну из первых частично гомоморфных схем шифрования?
18. Кто предложили криптосистему на основе билинейных отображений на эллиптических кривых?
19. Кто впервые построил теоретическую модель полностью гомоморфной криптосистемы?
20. Что из себя представляет гомоморфная криптосистема, дайте ей характеристику?
21. Какие алгоритмы включает в себя гомоморфная криптосистема?

Распределение времени занятия

Вступительная часть	- 5 мин
Проверка готовности студентов к занятию	- 10 мин
Основная часть	- 160 мин
Программа лабораторной работы	
1. Исследование схемы направленной подписи на изогениях эллиптических кривых	- 80 мин
2. Синтез направленной подписи на изогениях эллиптических кривых	- 60 мин
3. Тестирование по теме 4	20 мин
Заключение	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.
Всего	- 180 мин

Основные теоретические сведения

Направленная подпись на изогениях эллиптических кривых

Объединение свойств изогений и билинейных отображений позволяет адаптировать личностные (identity-based) криптографические протоколы, использующие, как правило, билинейные отображения, к математическому аппарату изогений.

Для изогении $\varphi: E_1 \rightarrow E_2$, дуальной изогении $\hat{\varphi}: E_2 \rightarrow E_1$ и точек $P, R \in E_1$, $Q \in E_2$ выполняются соотношения:

$$\begin{aligned} e(\varphi(P), Q) &= e(P, \hat{\varphi}(Q)); \\ e(\varphi(P), \varphi(R)) &= e(P, R)^{\deg \varphi}. \end{aligned}$$

Если $\psi: E_1 \rightarrow E_2$ — еще одна изогения, то

$$\begin{aligned} e(\varphi(P), \psi(R)) &= e(\varphi(R), \psi(P)); \\ e(\varphi(P), \psi(R)) &= e(\psi(P), -\varphi(R)). \end{aligned}$$

Рассмотрим протокол направленной подписи на изогениях эллиптических кривых, основанный на личностной схеме подписи.

Генерация параметров:

1. $E_{ID}, E_{d_{ID}}, E_{init}$ — изогенные суперсингулярные эллиптические кривые, заданные над полем $\mathbb{F}_{p^2}$ и имеющие одинаковое число точек, где ID — идентификатор.

2. $\gamma: E_{ID} \rightarrow E_{d_{ID}}$, $\varphi: E_{d_{ID}} \rightarrow E_{init}$, $\psi: E_{ID} \rightarrow E_{init}$ — изогении. Здесь сначала генерируется суперсингулярная кривая E_{ID} , из которой менеджером строятся изогении γ, φ, ψ .

3. Вложение идентификатора ID в точку эллиптической кривой: $ID \rightarrow Q_{ID} \in E_{ID}$.

4. $E_{Q_{ID}}[r] = \langle P_{ID} \rangle$ — циклическая группа точек эллиптической кривой с образующей P_{ID} .

5. $P = \psi(P_{ID})$.

6. Хеш-функция $Hash$.

Генерация ключей:

1. Открытый ключ системы: точка $P_{pub} = \varphi\gamma(P_{ID})$, изогения ψ .

2. Открытые ключи пользователей: точки $pk_i = \psi(Q_{ID})$.

3. Закрытые ключи пользователей: точки $sk_i = \varphi\gamma$.

Формирование подписи:

1. Вычислить $V = Hash(ID_s, ID_v, M, e_r(\varphi(d_{ID_s}), \psi(Q_{ID_v})))$, где ID_s — идентификатор отправителя сообщения M ; ID_v — идентификатор получателя.

2. Вложить значение V в точку V_H эллиптической кривой E_{init} , задать изогению $\alpha: E_{init} \rightarrow E_V$ с ядром $\ker(V_H)$.

3. Выбрать случайную точку R на кривой E_{init} и построить изогению $\beta: E_{init} \rightarrow E_R$ с ядром $\ker(R)$.

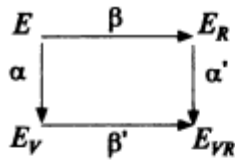


Рис. 1. Диаграмма с изогениями α и β

4. Вычислить коммутативную диаграмму с изогениями α и β (рис. 1).

5. Выбрать случайную точку P_1 на кривой E_{init} .

6. Вычислить билинейное отображение $U = e(\beta(\psi(P)), \beta(P_1))$.

7. Вычислить точку $W = \alpha'(\beta(\varphi(d_{ID_s})) + P_1)$.

8. Вычислить хэш-функцию $H_U = Hash(U^{\deg \alpha})$.

Подпись сообщения M имеет вид $\sigma = (W, V, H_U,$

$\alpha'(\beta(P)), \deg \beta)$.

Проверка подписи пользователем с идентификатором ID_v выполняется по алгоритму:

1. Вычислить значение хэш-функции

$$V' = Hash_1(ID_s, ID_v, M, e_r(\varphi(d_{ID_v}), \psi(Q_{ID_s}))).$$

2. Вложить значение V' в точку V_H эллиптической кривой E_{init} , задать изогению $\alpha: E_{init} \rightarrow E_V$ с ядром $\ker(V_H)$.

3. Вычислить билинейное отображение

$$U' = e_r(W, \beta'(\alpha(P)))e_r(\psi(Q_{ID_s}), -P_{pub})^{\deg \alpha \deg \beta}.$$

4. Если $Hash(U') = H_U$ и $V' = V$, то подпись верна, иначе — отклоняется.

Делегирование права проверки подписи третьей стороне с идентификатором ID_T :

$$Add = e_r(\varphi(d_{ID_v}), \psi(Q_{ID_s})) = e_r(\varphi(d_{ID_s}), \psi(Q_{ID_v}))$$

5. Вычислить $V' = Hash_1(ID_s, ID_v, M, e_r(\varphi(d_{ID_v}), \psi(Q_{ID_s})))$.

6. Вложить значение V в точку V_H эллиптической кривой E_{init} , задать изогению $\alpha: E_{init} \rightarrow E_V$ с ядром $\ker(V_H)$.

7. Вычислить билинейное отображение

$$U' = e_r(W, \beta'(\alpha(P)))e_r(\psi(Q_{ID_s}), -P_{pub})^{\deg \alpha \deg \beta}.$$

8. Если $Hash(U') = H_U$ и $V' = V$, то подпись верна, иначе — отклоняется.

Обозначим $\deg = \deg \alpha \deg \beta$.

Корректность протокола обосновывается выполнением соотношения

$$\begin{aligned} & e_r(W, \beta'(\alpha(P)))e_r(\psi(Q_{ID_s}), -P_{pub})^{\deg} = \\ & = e_r(\alpha'(\beta(\varphi(d_{ID_s})) + P_1), \beta'(\alpha(P)))e_r(\psi(Q_{ID_s}), -P_{pub})^{\deg} = \\ & = e_r(\alpha'(\beta(\varphi(d_{ID_s}))), \beta'(\alpha(P)))e_r(\alpha'(\beta(P_1)), \beta'(\alpha(P)))e_r(\psi(Q_{ID_s}), \\ & -P_{pub})^{\deg} = e_r(\varphi(d_{ID_s}), P)^{\deg}e_r(P_1, \psi(P))^{\deg}e_r(\psi(Q_{ID_s}), -P_{pub})^{\deg} = \\ & = e_r(Q_{ID_s}, P_{pub})^{\deg}e_r(P_1, \psi(P))^{\deg}e_r(\psi(Q_{ID_s}), -P_{pub})^{\deg} = U^{\deg \alpha}. \end{aligned}$$

Следует отметить, что однократное делегирование права проверки подписи одного сообщения от одного пользователя другому дает возможность проверки последующих сообщений, пересылаемых между этими участниками. Этот недостаток можно устранить, добавив случайную составляющую в значение Add .

Учебно-методическое и информационное обеспечение занятия

Перечень основной и дополнительной литературы

Перечень основной литературы:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. - М.: Горячая линия - Телеком, 2020. - 560 с.: ил.
2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.
3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Перечень дополнительной литературы

1. Коршунов, Г. И. K70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.
3. А.И. Астайкина. Саратов: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.а. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.: Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)

9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей: учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск: Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине «Аутентификация в киберфизических системах»
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Аутентификация в киберфизических системах»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) <https://rkn.gov.ru/> -
3. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/> -
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции <http://www.consultant.ru/>
5. Интернет портал Защита-информации.SU <http://www.iso27000.ru/>
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru>
7. Консорциум сетевых электронных библиотек ЭБС «Лань» <https://e.lanbook.com/>
8. ЭБС «Университетская библиотека ОНЛАЙН» <https://www.biblioclub.ru/> -
9. ЭБС IPR SMART <https://www.iprbookshop.ru/>
10. ЭБС Znanium <https://znanium.com/>
11. ЭБС «Юрайт» <http://www.biblio-online.ru>
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

Методические рекомендации по выполнению лабораторной работы

1. Используя теоретический материал, представленный в методических рекомендациях, исследовать схемы направленной подписи на изогениях эллиптических кривых. Особое внимание обратить на то, что объединение свойств изогений и билинейных отображений позволяет адаптировать личностные (identity-based) криптографические протоколы, использующие, как правило, билинейные отображения, к математическому аппарату изогений. В лабораторной работе мы рассматриваем протокол направленной подписи на изогениях эллиптических кривых, основанный на именно личностной схеме подписи (90 минут).

2. Сформировать алгоритм протокола по его основным этапам: генерация параметров; формирование подписи; проверка подписи пользователем с идентификатором; представление корректности протокола. Следует учесть, что однократное делегирование права проверки подписи одного сообщения от одного пользователя другому дает возможность проверки последующих сообщений, пересылаемых между этими участниками. Этот недостаток можно устранить, добавив случайную составляющую в значение *Add* (90 минут).

Цель работы состоит в реализации алгоритма направленной подписи на изогениях эллиптических кривых по всем этапам протокола и формирования доказательной базы его корректности.

Результаты лабораторной работы занести в отчет

3. За 20 минут до окончания занятий проводится тестирование по теме №4. Вопросы тестирования охватывают теоретический материал, выданный на лекционных занятиях.

Перечень вопросов выносимый на процедуру тестирования.

1. Как ассоциируется при реализации групповой аутентификации каждый участник группы?
2. Что не позволяют сделать пороговые подписи?
3. Какую разновидность представляет собой упорядоченная цифровая?
4. Почему использование единой коллективной подписи фиксированной длины, реализованной при участии нескольких пользователей актуально?
5. Какую подпись необходимо использовать если нужна верификация не только самой подписи, но и порядка ее создания?
6. Что такое композиционный подход?
7. Каким требованиям должны удовлетворять оптимальные схемы упорядоченных подписей?

8. С помощью чего осуществляется формирование упорядоченной подписи?
9. Какую проблему позволяет решить применение упорядоченной цифровой подписи?
10. На какой задаче основаны многие протоколы коллективной, в том числе и упорядоченной, цифровой подписи?
11. Что является особенностью большинства схем цифровой подписи?
12. Что является проблемой неоспоримой подписи?
13. Как реализуется интерактивность при реализации неоспоримой электронной подписи?
14. Что из себя представляет направленная подпись, в чем ее специфика?
15. Какими свойствами обладает направленная подпись?
16. Поясните работу общей схемы направленной подписи.
17. Кто и когда предложил одну из первых частично гомоморфных схем шифрования?
18. Кто предложили криптосистему на основе билинейных отображений на эллиптических кривых?
19. Кто впервые построил теоретическую модель полностью гомоморфной криптосистемы?
20. Что из себя представляет гомоморфная криптосистема, дайте ей характеристику?
21. Какие алгоритмы включает в себя гомоморфная криптосистема?

Содержание отчета по лабораторной работе

Отчет должен иметь следующую структуру:

- формулировку темы лабораторной работы;
- формулировку цели и решаемых в ходе лабораторной работы задач;
- порядок выполнения лабораторной работы с учетом достижения целевой установки;
- выводы по результатам работы.

По результатам выполнения лабораторной работы студенты оформляют отчет по лабораторной работе и защищают его в индивидуальном порядке в форме беседы.

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Аутентификация в киберфизических системах»

для студентов направления подготовки

10.04.01 «Информационная безопасность»

Направленность (профиль):

«Информационная безопасность киберфизических систем»

Ставрополь

2026

СОДЕРЖАНИЕ

Введение.....	133
1. Общая характеристика самостоятельной работы студента	134
2. Технологическая карта самостоятельной работы обучающихся дисциплине «Проектирование траектории профессионального роста и личностного развития»	136
3. Контрольные точки и виды отчетности по ним	137
4. Методические указания по подготовке к лабораторным работам	138
5. Список рекомендуемой литературы.....	142

Введение

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные работы и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области теоретической основы управления. На лабораторных работах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным занятиям, завести новую тетрадь для конспектирования лекций и выполнения лабораторных заданий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная - поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным занятиям, оформление отчета по выполненному практической работе и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

- чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

- работа с нормативными документами;

- поиск информации в Интернет;

2) для закрепления и систематизации знаний:

- работа с конспектом лекции (обработка текста);

- повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

- составление плана и тезисов ответа или графическое изображение структуры ответа;

- составление таблиц для систематизации учебного материала;

- изучение нормативных документов;

- ответы на контрольные вопросы;

3) для формирования умений:

- подготовка к лабораторным занятиям;

- решение задач и лабораторных работ;
- подготовка отчетов по лабораторным занятиям;
- рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, лабораторные занятия, контрольные вопросы) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным занятиям.

2. Технологическая карта самостоятельной работы обучающихся дисциплине «Проектирование траектории профессионального роста и личностного развития»

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объём часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
3 семестр					
ИД-1пк-2 ИД-1пк-3 ИД-2пк-3 ИД-6пк-3	Самостоятельное изучение литературы	Собеседование	14.00	4.00	18.00
ИД-2пк-2 ИД-2пк-3 ИД-4пк-2	Подготовка к экзамену	Вопросы к экзамену	14.00	4.00	18.00
Итого за 3 семестр			28.00	8.00	36.00
Итого			28.00	8.00	36.00

3. Контрольные точки и виды отчетности по ним

По дисциплине предусмотрен текущий контроль на каждом учебном занятии и по каждому разделу учебной дисциплины.

Формы текущего контроля:

- устный опрос;
- защита отчетов по лабораторным работам;
- защита отчета по самостоятельному решению разноуровневых задач.

Устный опрос осуществляется на каждом учебном занятии (лекции, лабораторные работы). Все лабораторные работы, выполняемые по разделам дисциплины, подлежат оцениванию по результатам проверки отчета и собеседованию.

Критерии оценки для проверки умений при выполнении лабораторных работ:

- оценка «отлично» выставляется, если студент продемонстрировал высокое умение применять полученные знания на практике через решение конкретной задачи, свободно без затруднений справился с поставленной задачей, показав владение разносторонними приемами и навыками ее выполнения, не допустил ошибок и неточностей;
- оценка «хорошо» выставляется, если студент продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, справился с поставленной задачей, показав владение необходимыми приемами и навыками ее выполнения, при этом допустил не более одной ошибки;
- оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретной задачи, с трудом справился с поставленной задачей, при этом допустил не более двух ошибок;
- оценка «неудовлетворительно» выставляется, если студент не продемонстрировал умение применять полученные знания на практике через

решение конкретной задачи, не справился с поставленной задачей или допустил при ее решении три и более серьезные ошибки.

4. Методические указания по подготовке к лабораторным работам

При подготовке к практической работе студенту следует:

1. изучить (повторить) теоретический материал, посвящённый теме практической работы;
2. ознакомиться с заданием на лабораторную работу;
3. проверить свой уровень подготовки с помощью вопросов и заданий для самоконтроля.

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практической работы.

Требования безопасности перед началом работ:

4. ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
5. убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
6. включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы:

7. выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практической работе;
8. подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
9. при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или

лаборанту.

Требования безопасности по окончании работы:

10. доложить руководителю занятий или лаборанту о завершении работ.

11. привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

По результатам выполнения практической работы студенты оформляют и защищают в индивидуальном порядке в форме собеседования результаты выполнения заданий.

При подготовке и выполнении лабораторных работ совместно с оформлением отчетов по лабораторным занятиям позволяет успешно овладеть умениями, необходимыми для дальнейшей учебной и профессиональной деятельности.

Задания, выполняемые по лабораторным работам

Лабораторная работа №1. Реализация процедуры групповой подписи BBS на билинейных отображениях.

Типовые задачи:

Задания базового уровня:

1. Перечислите свойства киберфизической системы.
2. Опишите состав блока управления ПКС.
3. Дайте характеристику надежностного подхода для оценки устойчивости КФС.

Задания повышенного уровня:

1. Каков механизм выработки компенсирующего воздействия в КФС?

Лабораторная работа №2. Реализация процедуры групповой подписи на базе динамической схемы ED-BBS.

Типовые задачи:

Задания базового уровня:

1. Опишите внешний вид схемы групповой подписи BBS.

2. Перечислите свойства расширенной схемы ED-BBS.
3. Объясните алгоритм проверки подписи.

Задания повышенного уровня:

1. Опишите схему линейного шифрования Крамера-Шоупа для схемы BBS.

Лабораторная работа №3. Реализация процедуры групповой подписи BBS с отзывом права подписи.

Типовые задачи:

Задания базового уровня:

1. Объясните, для чего необходимо добавление временных меток при отзыве права подписи.
2. Перечислите модели взаимодействия субъектов с целью отзыва права подписи.
3. Перечислите недостатки при использовании записи отзыва для вычисления нового открытого ключа группы.

Задания повышенного уровня:

1. Перечислите временные метки, добавляемые при отзыве права подписи у пользователя.

Лабораторная работа №4. Реализация процедуры групповой подписи BBS с отзывом права подписи.

Типовые задачи:

Задания базового уровня:

1. Перечислите параметры, которые используются для описания протокола DKV.
2. Дайте определение протоколу NIWI.
3. Объясните назначение неинтерактивного доказательства NIWI.

Задания повышенного уровня:

1. Объясните алгоритм протокола Sign DKV.

Лабораторная работа №5. Построение схемы групповой подписи на решетках по протоколу LLS.

Типовые задачи:

Задания базового уровня:

1. Объясните основную особенность протокола LLLS.
2. Перечислите недостатки протокола LLLS.
3. Объясните причину, по которой схема с размером подписи $O(t^2 \log N)$ является некорректной.

Задания повышенного уровня:

1. Объясните алгоритм протокола Setup LLLS.

Лабораторная работа №6. Построение схемы групповой подписи на решетках с процедурой отзыва по протоколу DKV-DVLR.

Типовые задачи:

Задания базового уровня:

1. Опишите принцип работы механизма VLR-отзыва в модели DKV-DVLR.
2. Перечислите особенности представленной расширенной схемы принцип работы механизма VLR-отзыва в модели DKV-DVLR.

Задания повышенного уровня:

1. Объясните алгоритм протокола In_Revoked и для чего он используется в схеме DKV-DVLR.

Лабораторная работа №7. Построение схемы групповой подписи на решетках с процедурой отзыва по протоколу LLLS-VLR.

Типовые задачи:

Задания базового уровня:

1. Опишите принцип работы механизма VLR-отзыва в модели LLLS-VLR.
2. Перечислите особенности представленной расширенной схемы принцип работы механизма VLR-отзыва в модели LLLS-VLR.

Задания повышенного уровня:

1. Объясните алгоритм протокола In_Revoked и для чего он используется в схеме LLLS-VLR.

Лабораторная работа №8.

Типовые задачи:

Задания базового уровня:

1. Перечислите этапы работы аутсорс-алгоритмов.
2. Обозначьте основные отличия алгоритмов BilinearMap1 и BilinearMap2.

Задания повышенного уровня:

1. Опишите цепочку вычислений в алгоритме BilinearMap1.

Лабораторная работа №9.

Типовые задачи:

Задания базового уровня:

1. Опишите протокол генерации параметров.
2. Опишите протокол формирования подписи.
3. Опишите протокол проверки подписи пользователем с идентификатором ID.

Задания повышенного уровня:

1. Какие алгоритмы включает в себя гомоморфная криптосистема?

5. Список рекомендуемой литературы

Основная литература:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.
2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.
3. Nayan M. Kakoty, Rupam Goswami, Ramana Vinjamuri, Introduction to Embedded Systems and Robotics : A Practical Guide, Springer, 2024 .

Дополнительная литература:

1. Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.
2. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред. Астайкиной А.И. Саратов: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
3. Астайкина А.И. Саратов: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.
4. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.
5. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.А. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.
6. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.
7. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.:Лаборатория знаний, 2020. — 482 с.
8. Ли, П. Архитектура интернета вещей / П. Ли.; перевод М. А. Райтман. — Москва: ДМК Пресс, 2020. — 454 с. — ISBN 978-5-97060-784-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124712.html> (дата обращения: 14.10.2022)
9. Дубков, И. С. Решение практических задач на базе технологии интернета вещей: учебное пособие / И. С. Дубков, П. С. Сташевский, И. Н. Яковина. — Новосибирск: Новосибирский государственный технический университет, 2017. — 80 с. — ISBN 978-5-7782-3161-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/91510.html> (дата обращения: 22.10.2022). — Режим доступа: для авторизир. пользователей.