Дисциплина «Технологии обеспечения информационной безопасности»

Лекция 4.1. «Модели управления целостностью»

доцент кафедры КБ-4
кандидат педагогических наук, доцент
Пимонов Роман Владимирович

Учебные вопросы:

1. Понятие «целостность информации»
2. Модели контроля целостности
3. Методы контроля целостности
4. Технологии обеспечения контроля целостности

Литература

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / Учебное пособие для вузов. - 3-е изд., перераб. и доп. - Москва: Горячая линия - Телеком, 2023. - 352 с.
2. Модели безопасности компьютерных систем : учеб. пособие / Н. А. Богульская, М. М. Кучеров. – Красноярск : Сиб. федер. ун-т, 2019. – 206 с.
3. https://profsandhu.com/cs6393_s13/
4. https://www.cs.purdue.edu/homes/ninghui/papers/umip_oakland07.pdf

Вопрос 1. **Понятие «целостность информации».**

Вопрос 1. Понятие «целостность информации».

ГОСТ Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации.

3.1.4 **Безопасность информации** [данных] - состояние защищенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность.

3.1.5 **Безопасность информации** (при применении информационных технологий) - состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

3.1.6 **Безопасность автоматизированной информационной системы** - состояние защищенности автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность ее ресурсов.

3.1.7 **Конфиденциальность** (информации [ресурсов автоматизированной информационной системы]) - состояние информации [ресурсов автоматизированной информационной системы], при котором доступ к ней [к ним] осуществляют только субъекты, имеющие на него право.

3.1.8 ***Целостность*** (информации [ресурсов автоматизированной информационной системы]) - состояние информации [ресурсов автоматизированной информационной системы], при котором ее [их] изменение осуществляется только преднамеренно субъектами, имеющими на него право.

3.1.9 **Доступность** (информации [ресурсов автоматизированной информационной системы]) - состояние информации [ресурсов автоматизированной информационной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Вопрос 1. Понятие «целостность информации».

Угрозы целостности информации

- Модификация.
- Имитация источника.
- Повторная передача информации.
- Отказ от сообщения и пр.

База данных угроз безопасности информации содержит 137 угроз, связанных с целостностью (https://bdu.fstec.ru), что составляет более 60% от всех угроз.

Основные процессы, которые должны обеспечиваться в механизмах целостности:

- передача;
- изменение;
- хранение;
- отображение информации.

Контроль целостности цифровой информации обеспечивается, как правило, вычислительной процедурой с использованием Хэш-функции h(T).

Если $h(T)=h(To)$, то $T = To$,

где T – исходная информация

To – переданная информация

В зависимости от превалирования того или иного аспекта целостности и области использования данных **выделяют**:

- специальные технологии разграничения доступа данных, основывающиеся на моделях целостности данных;
- криптографические технологии (шифрование, электронная цифровая подпись);
- технологии параллельного выполнения транзакций в клиент-серверных системах (СУБД).

Вопрос 1. Понятие «целостность информации».

Угрозы | Уязвимости | Тестирование обновлений | Документы | Обратная связь | Обновления | Участники | Обучение | ФСТЭК России

Главная / Список угроз / УБИ.018

УБИ.018: Угроза загрузки нештатной операционной системы

Вид

Описание угрозы	Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки BIOS/UEFI – указания источника загрузки операционной системы
Источники угрозы	Внутренний нарушитель с низким потенциалом
Объект воздействия	Микропрограммное обеспечение BIOS/UEFI
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

Угрозы | Уязвимости | Тестирование обновлений | Документы | Обратная связь | Обновления | Участники | Обучение | ФСТЭК России

Главная / Список угроз / УБИ.213

УБИ.213: Угроза обхода многофакторной аутентификации

Вид

Описание угрозы	Угроза заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в дискредитируемую систему и компоненты, участвующие в процедуре многофакторной аутентификации. Данная угроза обусловлена: наличием уязвимостей программного обеспечения; слабостями мер антивирусной защиты и разграничения доступа. Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; при наличии у него привилегий установки программного обеспечения
Источники угрозы	Внешний нарушитель с высоким потенциалом
Объект воздействия	Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

Угрозы | Уязвимости | Тестирование обновлений | Документы | Обратная связь | Обновления | Участники | Обучение | ФСТЭК России

Главная / Список угроз / УБИ.003

УБИ.003: Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации

Вид

Описание угрозы	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки
Источники угрозы	Внешний нарушитель со средним потенциалом Внутренний нарушитель со средним потенциалом
Объект воздействия	Метаданные, системное программное обеспечение
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности

Угрозы | Уязвимости | Тестирование обновлений | Документы | Обратная связь | Обновления | Участники | Обучение | ФСТЭК России

Главная / Список угроз / УБИ.024

УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера

Вид

Описание угрозы	Угроза заключается в возможности изменения нарушителем режимов работы аппаратных элементов компьютера путём несанкционированного переконфигурирования BIOS/UEFI, что позволяет: за счёт изменения частоты системной шины, режима передачи данных по каналам связи и т.п. повлиять на общую производительность компьютера или вызвать сбои в его работе; за счёт понижения входного напряжения, отключения систем охлаждения временно обеспечить неработоспособность компьютера; за счёт задания недопустимых параметров работы устройств (порогового значения отключения устройства при перегреве, входного напряжения и т.п.) привести к физическому выходу из строя отдельных аппаратных элементов компьютера. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение соответствующих параметров настройки BIOS/UEFI
Источники угрозы	Внутренний нарушитель с высоким потенциалом
Объект воздействия	Микропрограммное и аппаратное обеспечение BIOS/UEFI
Последствия реализации угрозы	Нарушение целостности Нарушение доступности

Вопрос 1. Понятие «целостность информации».

Руководящий документ
Автоматизированные системы. Защита от несанкционированного доступа к информации
Классификация автоматизированных систем и требования по защите информации
Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

ГОСТ Р 51241-2008 СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ
Классификация. Общие технические требования.
Методы испытаний

АС, в которых циркулирует информация, составляющая гостайну: 1А, 1Б и 1В.

1 В - в случае обработки секретной информации с грифом не выше «секретно»
1 Б - в случае обработки секретной информации с грифом не выше «совершенно секретно»
1 А - в случае обработки секретной информации с грифом «особая важность»
1 Г - АС, в которых циркулирует служебная тайна
1 Д - АС, в которых циркулируют персональные данные

Подсистемы и требования	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом					
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:					
в систему	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+	+	+	+
к программам	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
1.2. Управление потоками информации	-	-	+	+	+
2. Подсистема регистрации и учета					
2.1. Регистрация и учет:					
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
изменения полномочий субъектов доступа	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	+	+	+
2.2. Учет носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	-	-	+	+	+
3. Криптографическая подсистема					
3.1. Шифрование конфиденциальной информации	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	+
4. Подсистема обеспечения целостности					
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	-	-	+	+	+

Вопрос 1. Понятие «целостность информации».

Руководящий документ
Автоматизированные системы. Защита от несанкционированного доступа к информации
Классификация автоматизированных систем и требования по защите информации
Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

ГОСТ Р 51241-2008 СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ
Классификация. Общие технические требования.
Методы испытаний

АС, в которых циркулирует информация, составляющая гостайну: 1А, 1Б и 1В.

1 В - в случае обработки секретной информации с грифом не выше «секретно»
1 Б - в случае обработки секретной информации с грифом не выше «совершенно секретно»
1 А - в случае обработки секретной информации с грифом «особая важность»
1 Г - АС, в которых циркулирует служебная тайна
1 Д - АС, в которых циркулируют персональные данные

Подсистемы и требования	2Б	2А
1. Подсистема управления доступом		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+
к программам	-	+
к томам, каталогам, файлам, записям, полям записей	-	+
1.2. Управление потоками информации	-	+
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	+
изменения полномочий субъектов доступа	-	-
создаваемых защищаемых объектов доступа	-	+
2.2. Учет носителей информации	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+
2.4. Сигнализация попыток нарушения защиты	-	-
3. Криптографическая подсистема		
3.1. Шифрование конфиденциальной информации	-	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	+
4. Подсистема обеспечения целостности		
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	+
4.4. Периодическое тестирование СЗИ НСД	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+
4.6. Использование сертифицированных средств защиты	-	+

Вопрос 1. Понятие «целостность информации».

Руководящий документ
Автоматизированные системы. Защита от несанкционированного доступа к информации
Классификация автоматизированных систем и требования по защите информации
Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

ГОСТ Р 51241-2008 СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ
Классификация. Общие технические требования.
Методы испытаний

АС, в которых циркулирует информация, составляющая гостайну: 1А, 1Б и 1В.

1 В - в случае обработки секретной информации с грифом не выше «секретно»
1 Б - в случае обработки секретной информации с грифом не выше «совершенно секретно»
1 А - в случае обработки секретной информации с грифом «особая важность»
1 Г - АС, в которых циркулирует служебная тайна
1 Д - АС, в которых циркулируют персональные данные

Подсистемы и требования	3Б	3А
1. Подсистема управления доступом		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-
к программам	-	-
к томам, каталогам, файлам, записям, полям записей	-	-
1.2. Управление потоками информации		
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему (ы) (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-
изменения полномочий субъектов доступа	-	-
создаваемых защищаемых объектов доступа	-	-
2.2. Учет носителей информации	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+
2.4. Сигнализация попыток нарушения защиты	-	-
3. Криптографическая подсистема		
3.1. Шифрование конфиденциальной информации	-	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-
4. Подсистема обеспечения целостности		
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-
4.4. Периодическое тестирование СЗИ НСД	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+
4.6. Использование сертифицированных средств защиты	-	+

Вопрос 2. Модели контроля целостности.

Модель Биба

Определены:

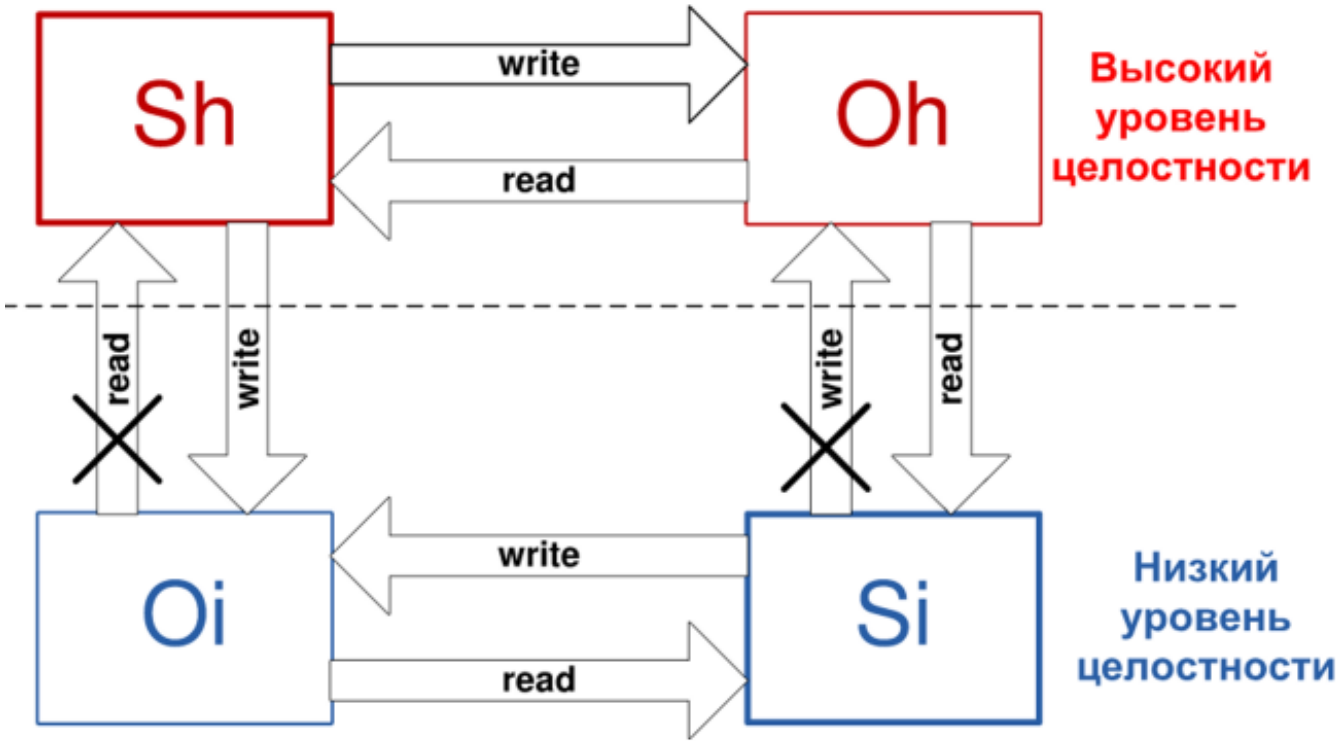
1. Уровни целостности для объектов и субъектов в системе.

2. Правило No Read Down. ***NRD:*** ∀***s***∈ ***S, o***∈***O:*** *разрешить* (s, o, чтение) если и только если уровень (o) *преобладает* уровень (s).

3. Правило No Write Up. ***NWU:*** ∀***s***∈***S, o***∈***O:*** разрешить (s, o, запись) если и только если уровень (s) преобладает уровень (o).

Модель понижения уровня целостности субъекта до уровня целостности объекта при чтении.

Модель понижения уровня целостности объекта до уровня субъекта при записи (не всегда возможна).



Модель целостности Кларка-Вилсона

Обозначения

S *– множество субъектов;*
D *– множество данных в автоматизированной системе (множество объектов);*
CDI *(Constrained Data Items) – данные, целостность которых контролируется;*
UDI *(Unconstrained Data Items) – данные, целостность которых не контролируется;*
TP *(Transformation Procedure) – процедура преобразования;*
IVP *(Integrity Verification Procedure) – процедура проверки целостности CDI.*

Модель

1. ***D*** = ***CDI*** ∪ ***UDI*** , ***CDI*** ∩ ***UDI*** =∅
2. Элементарные операциии над объектами выполняются процедурами преобразования ***TP*** и контроля целостности ***IVP***.
3. Процедуры ***TP*****,** прошедшие проверки целостности ***IVP*** называются «*корректно сформированными транзакциями*».

Правила

1. Наличие процедур ***IVP***; неизменяемость ***Cdi*** при преобразованиях; допустимости применения ***TP*** к ***CDI***;
2. Строгое определение отношений между ***S, D, TP***. Эти отношения определяются политикой.
3. Учет всех применений ***TP*** (ведение журнала регистрации без прав изменения записей).
4. Наличие специальных процедур ***TP*** для преобразования ***UDI*** в ***CDI*** и распознавания субъектов пытающихся применить ***TP***.

Проблемы целостности информации

1. Все решения по целостности сводятся только к правилам взаимоотношений субъектов, объектов и процедур преобразования информации в текущий момент времени.
2. Управление целостностью информации в длительных периодах времени должно быть построено на доказательной базе контроля целостности при каждом изменении информации в электронном документе.
3. Вопросы изменения целостности в длительном периоде времени при хранении, передаче, отображении информации, модернизации оборудования, форматов хранения информации и ПО не рассматриваются.
4. Механизмы оценки уровня целостности (достоверности) четко не определены и являются самостоятельной очень сложной задачей.
5. Процедуры восстановления целостности информации при частичной её потере в электронных архивах в моделях не рассматриваются.
6. Риски передачи электронных архивов новому поколению владельцев (администраторов) не обсуждаются, а механизмы сохранения целостности для этой ситуации не разработаны.
7. Возможность потери архивов в результате случайного или умышленного воздействия на него его владельца или пользователей с высокими правами не рассматриваются.

Вопрос 3. Методы контроля целостности.

Методы контроля целостности данных:

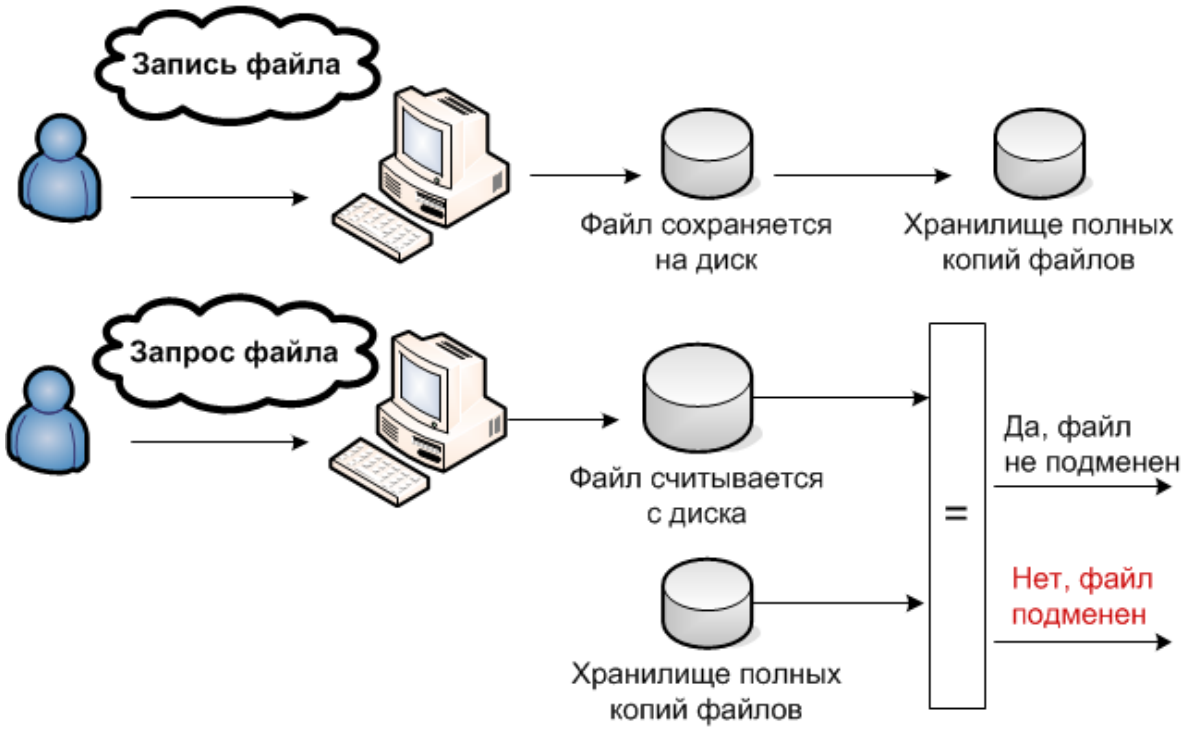
1. Полная копия данных.
2. Контрольная сумма.
3. Хеш.
4. Имитовставка.
5. ЭЦП.

1. Полная копия данных.

Создаются полные копии данных
и затем сверяются.

<u>Преимущества:</u>
- простота реализации;
- полный контроль данных (до бита).

<u>Недостатки:</u>
- большой объем;
- копии можно подменить;
- копиями можно воспользоваться
(например: если данные - пароль).

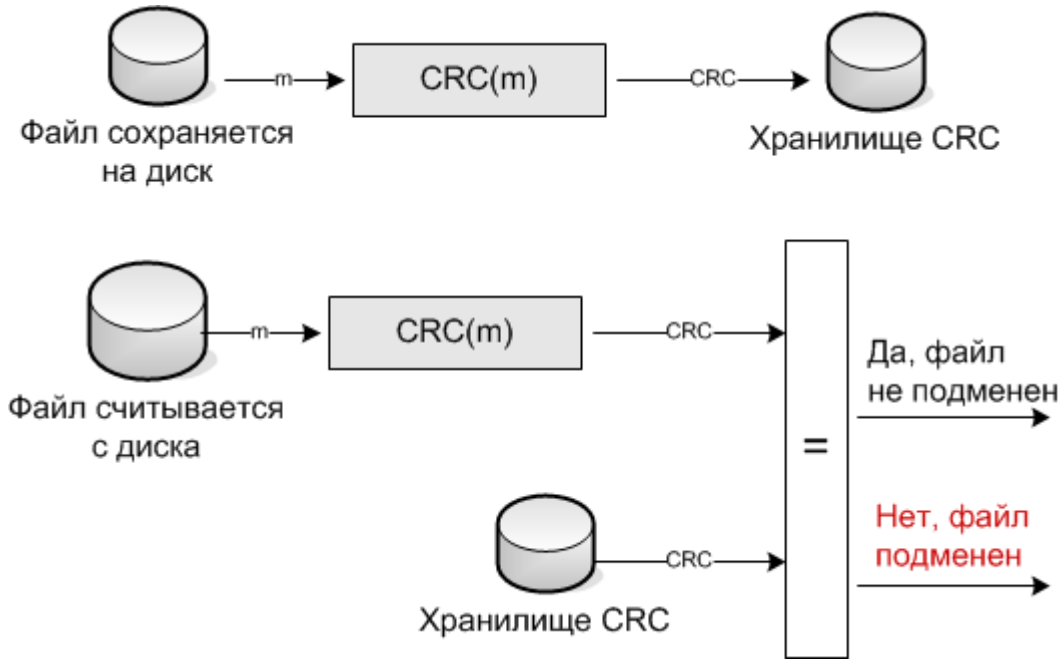


2. Контрольная сумма.

Контрольная сумма - значение, рассчитанное по входным данным с помощью определённого алгоритма.

Преимущества:
- высокая скорость вычисления;
- малый размер;
- стандартный размер.

Недостатки:
- можно подменить;
- для одного значения существует множество исходных данных;
- можно подобрать исходные данные к значению за приемлемое время (например: получить пароль).



Хеш.

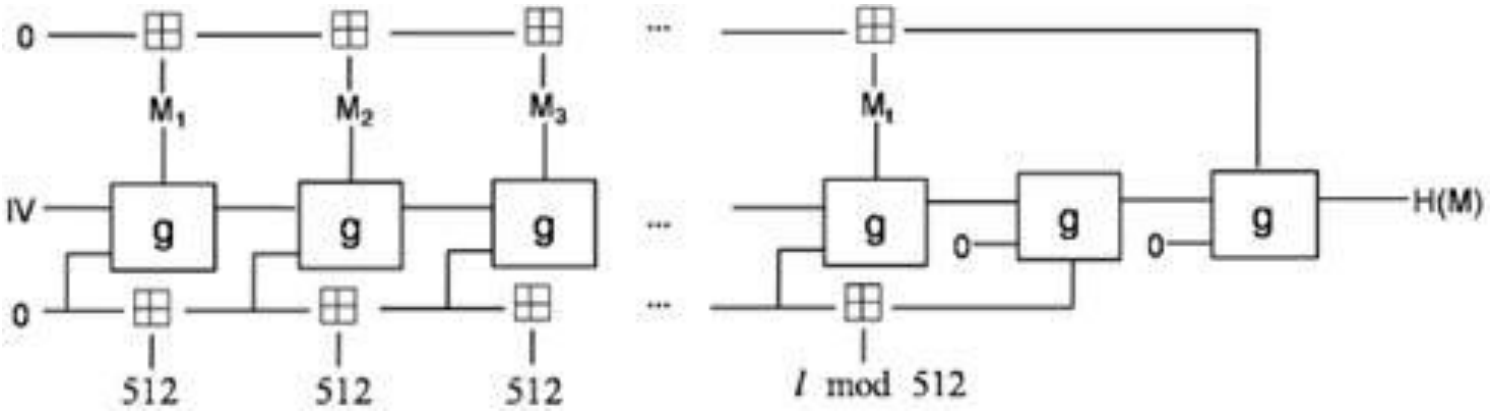
Хеш (хэш, криптографический хеш) - значение, рассчитанное по входным данным с помощью криптографического алгоритма.

Преимущества:
- малый размер;
- стандартный размер;
- нельзя подобрать исходные данные к значению за приемлемое время (например: получить пароль).

Недостатки:
- низкая скорость вычисления (сопоставима с шифрованием);
- можно подменить;
- для одного значения существует множество исходных данных.

3. Хеш

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования



$$h_0 = IV, N = 0, \Sigma = 0 \quad (1)$$

$$h_j = g_N(h_{j-1}, M_j), N = N \boxplus 512, \Sigma = \Sigma \boxplus M_j \text{ для } 0 < j < t \quad (2)$$

$$h_t = g_N(h_{t-1}, M_t), N = N \boxplus (l \bmod 512), \Sigma = \Sigma \boxplus M_t \quad (3)$$

$$h_{t+1} = g_0(h_t, N) \quad (4)$$

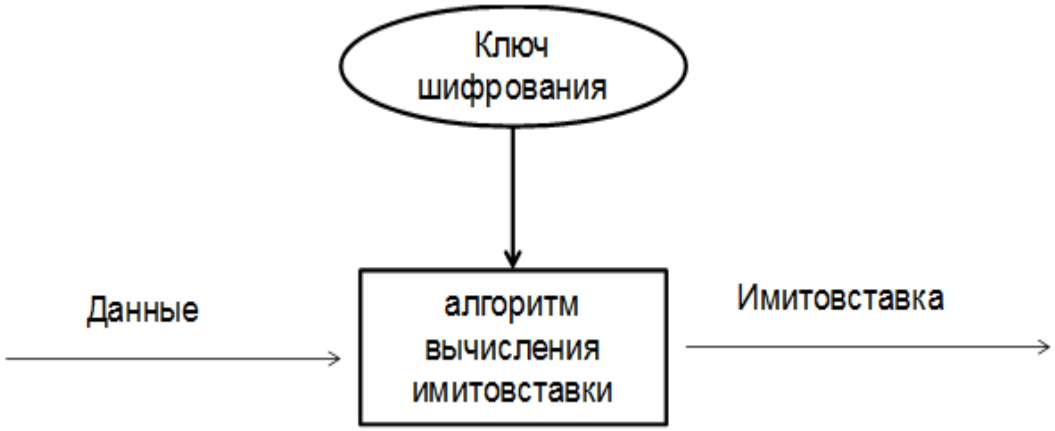
$$H(M) = g_0(h_{t+1}, \Sigma) \quad (5)$$

4. Имитовставка (MAC, message authentication code — код аутентичности сообщения)
ГОСТ 28147-89

Имитовставка - значение, рассчитанное по входным данным с помощью криптографического алгоритма с использованием секретного элемента (ключа), известного только отправителю и получателю.

Преимущества:

- малый размер
- стандартный размер
- нельзя подобрать исходные данные к значению за приемлемое время (например: получить пароль)
- нельзя подменить без секретного элемента (ключа)



Недостатки:

- низкая скорость вычисления (сопоставима с шифрованием)
- для одного значения существует множество исходных данных
- секретный ключ известен как минимум двоим

Вычисляют имитовставку шифрованием данных блочным алгоритмом в режимах CBC. Имитовставкой является последний шифрованный блок.

5. Электронная цифровая подпись

(ГОСТ 34. 10-2018. Информационная технология.КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ.Процессы формирования и проверки электронной цифровой подписи)

Электронная подпись

(Федеральный закон "Об электронной подписи"

Электронная цифровая подпись - зашифрованное значение вычисленного хеша по входным данным.

Преимущества:

- малый размер
- стандартный размер
- нельзя подобрать исходные данные к значению за приемлемое время (например: получить пароль)
- нельзя подменить без секретного элемента (ключа)
- секретный ключ известен одному

Недостатки:

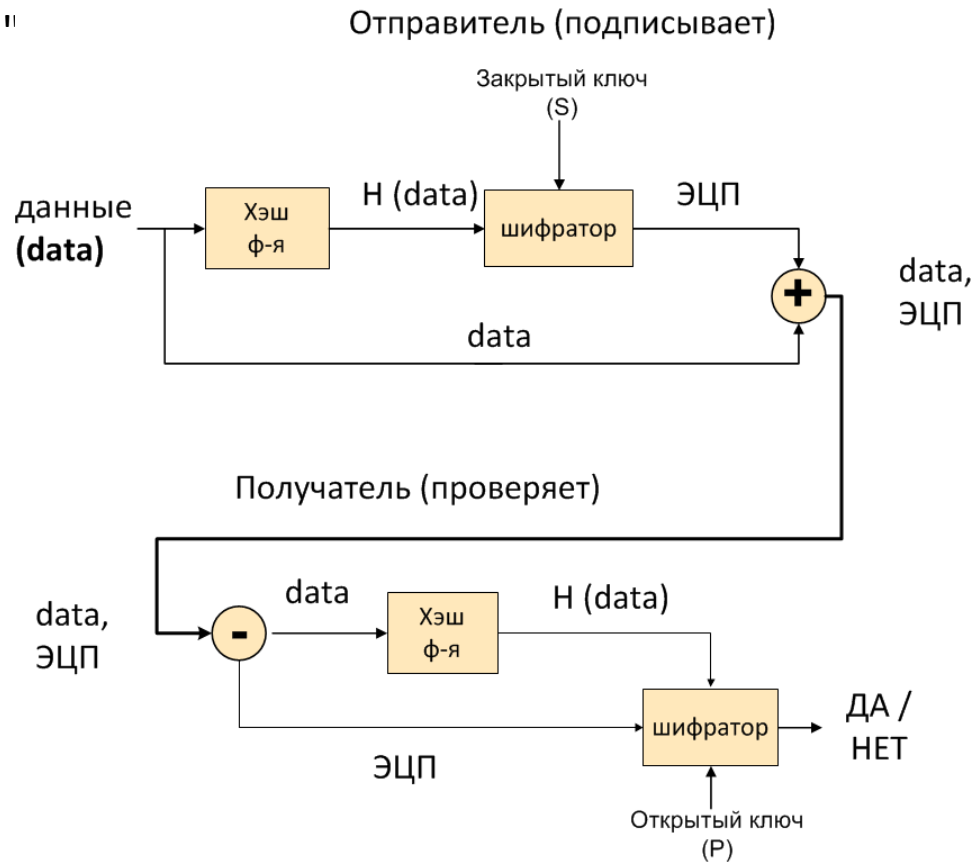
- низкая скорость вычисления (сопоставима с шифрованием)
- для одного значения существует множество исходных данных

Алгоритм:

1. вычисляется хеш
2. шифруется хеш

Применение:

1. контроль целостности файлов
2. контроль передаваемых данных по каналам связи
3. аутентификации источника данных (кто создал подпись)



Вопрос 4. Технологии обеспечения контроля целостности.

Вопрос 4. Технологии обеспечения контроля целостности.

Технологии параллельного выполнения транзакций в клиент-серверных системах (СУБД)

Основа функционирования многопользовательских клиент-серверных систем – эффективное управление **транзакциями**.

Единичные действия пользователей с базой данных ассоциированы с транзакциями.

Монитор транзакций -
обеспечивает специальнуютехнологию параллельного (параллельно-последовательного) выполнения транзакций и изоляции (устранения взаимного влияния и затруднений друг другу)

Ограничения целостности непосредственно проверяются по завершению очередной транзакции, которая либо фиксируется при выполнении условий ограничения целостности (выполняется SQL–инструкция COMMIT), либо происходит "откат" транзакции (выполняется SQL–инструкция ROLLBACK) в противном случае.

Издержки параллельной обработки данных:
- потерянные изменения;
- "грязные" данные;
- неповторяющиеся чтения.

Сериализация транзакций -
план (способ) выполнения совокупности транзакций, при котором результат их совместного выполнения эквивалентен результату некоторого последовательного их выполнения.

Подходы сериализации транзакций:
- синхронизационные захваты (блокировки) объектов базы данных;
- временные метки объектов базы данных.

Мандатный контроль целостности

Мандатный контроль целостности (также известный как обязательный контроль целостности) – это механизм, который используется для обеспечения целостности данных в информационных системах.

Основные аспекты мандатного контроля целостности :

1. Проверка целостности данных: Этот контрольный механизм проверяет, что данные не были изменены, повреждены или скомпрометированы в процессе передачи или хранения. Это достигается путем вычисления хеш-сумм (например, MD5, SHA-256) данных и сравнения их с хеш-суммами, рассчитанными при их отправке и/или хранении. Если хеш-суммы не совпадают, это может указывать на потенциальное нарушение целостности данных.

2. Аутентификация: Для обеспечения мандатного контроля целостности, информационная система должна иметь механизм аутентификации, чтобы удостовериться в том, что данные были отправлены или получены от легитимного источника.

3. Авторизация: Для предотвращения несанкционированных изменений данных система должна иметь механизмы авторизации, чтобы убедиться, что только авторизованные пользователи или процессы имеют доступ к данным.

4. Шифрование: Защита данных с использованием шифрования помогает предотвратить изменение данных в пути между отправителем и получателем.

5. Логирование и мониторинг: Ведение журнала и мониторинг системы позволяют быстро обнаружить и реагировать на попытки нарушения целостности данных.

Замкнутая программная среда

Замкнутая программная среда (ЗПС) является средством повышения безопасность ОС путем контроля целостности (неизменности) файлов. Доступ и управление программами и ресурсами в ЗПС ограничены и контролируются владельцем или администратором системы. Эта концепция противоположна открытой программной среде, где доступ и разработка программного обеспечения могут быть более свободными и децентрализованными.

За счет строгого контроля и ограничения доступа, она может предотвращать несанкционированные изменения данных и обеспечивать целостность информационной системы. Особенности:

1. **Ограничение доступа:** В замкнутой программной среде доступ к данным и ресурсам контролируется и ограничивается. Это означает, что только авторизованные пользователи или процессы имеют доступ к этим ресурсам.
2. **Авторизация:** Владелец системы имеет возможность назначать различные уровни разрешений и прав доступа для пользователей. Это ограничивает, какие операции могут выполнять пользователи, что предотвращает несанкционированные изменения данных.
3. **Контроль версий:** В замкнутой среде владелец может контролировать версии программного обеспечения и обновления. Это позволяет поддерживать стабильность и целостность системы, предотвращая изменения, которые могли бы повредить работоспособность или безопасность.
4. **Защита от внешних угроз:** Замкнутая среда обычно включает в себя меры безопасности, которые помогают защитить систему от внешних угроз, таких как вредоносное программное обеспечение и несанкционированный доступ. Это также способствует обеспечению целостности данных.
5. **Контроль версий программ:** Владелец системы может контролировать, какие версии программ используются, что позволяет избегать несовместимости и сохранять целостность системы.
6. **Мониторинг и журналирование:** Замкнутые среды часто включают механизмы мониторинга и журналирования событий, что позволяет быстро выявлять и реагировать на любые потенциальные нарушения целостности.

Дисциплина «Технологии обеспечения информационной безопасности»

Лекция 4.1. «Модели управления целостностью»

доцент кафедры КБ-4
кандидат педагогических наук, доцент
Пимонов Роман Владимирович