МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

Методы обеспечения целостности информации

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	бакалавриат
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	09.03.02 «Информационные системы и технологии»
	(код(-ы) и наименование(-я))
Институт	кибербезопасности и цифровых технологий (ИКБ)
	(полное и краткое наименование)
Кафедра	Разработка программных решений и системное программирование
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	К.т.н. Ермакова Алла Юрьевна
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/24

(учебный год цифрами)

Проверено и согласовано «____» _____2023_г.

(подпись директора Института/Филиала с расшифровкой)

Москва 2023 г.

Лекция 2. Защита целостности при обработке информации

При рассмотрении вопроса целостности данных при обработке используем интегрированный подход, основанный на ряде работ Д. Кларка и Д. Вилсона, а также их последователей и оппонентов и включающий в себя девять абстрактных теоретических принципов:

• корректность транзакций;

• аутентификация пользователей;

• минимизация привилегий;

• разграничение функциональных обязанностей;

• аудит произошедших событий;

• объективный контроль;

• управление передачей привилегий;

• обеспечение непрерывной работоспособности;

• простота использования защитных механизмов.

Понятие *корректности транзакций* определяется следующим образом. Пользователь не должен модифицировать данные произвольно, а только определенными способами, т. е. так, чтобы сохранялась целостность данных. Другими словами, данные можно изменять только путем корректных транзакций и нельзя произвольными средствами. Кроме того, предполагается, что «корректность» (в обычном смысле) каждой из таких транзакций может быть некоторым способом доказана. Принцип корректных транзакций по своей сути отражает основную идею определения целостности данных, сформулированного в лекции 1.

Второй принцип гласит, что изменение данных может осуществляться только специально *аутентифицированными* для этой цели пользователями.

Данный принцип работает совместно с последующими четырьмя, с которыми тесно связана его роль в общей схеме обеспечения целостности.

Идея *минимизации привилегий* появилась еще на ранних этапах развития компьютерной безопасности в форме ограничения, накладываемого на возможности выполняющихся в АС процессов и подразумевающего, что процессы должны быть наделены теми и только теми привилегиями, которые естественно и минимально необходимы для выполнения процессов. Практикам администрирования ОС UNIX это положение хорошо знакомо на примере правил использования учетной записи root, обладающей неограниченными полномочиями.

Принцип минимизации привилегий распространяется и на программы, и на пользователей. Пользователям на практике трудно назначить «теоретически достижимый» минимальный уровень привилегий по двум причинам. Во-первых, пользователи выполняют разнообразные задачи, требующие различных привилегий. Во-вторых, если строгое соблюдение принципа минимизации в отношении процессов связано с соображениями стоимости и производительности, то в отношении пользователей оно скорее затрагивает вопросы этики и морали, а также удобства и эффективности работы. Поэтому пользователи имеют, как правило, несколько больше привилегий, чем им необходимо для выполнения конкретного действия в данный момент времени. А это открывает возможности для злоупотреблений.

Разграничение функциональных обязанностей подразумевает организацию работы с данными таким образом, что в каждой из ключевых стадий, составляющих единый критически важный с точки зрения целостности процесс, необходимо участие различных пользователей. Это гарантирует невозможность выполнения одним пользователем всего процесса целиком (или даже двух его стадий) с тем, чтобы нарушить целостность данных. В обычной жизни примером воплощения данного

принципа служит передача одной половины пароля для доступа к программе управления ядерным реактором первому системному администратору, а другой – второму.

Аудит произошедших событий (включая возможность восстановления полной картины происшедшего) является превентивной мерой в отношении потенциальных нарушителей.

Принцип *объективного контроля* также является одним из краеугольных камней политики контроля целостности. Суть данного принципа заключается в том, что контроль целостности данных имеет смысл лишь тогда, когда эти данные отражают реальное положение вещей. Очевидно, что нет смысла заботиться о целостности данных, связанных с размещением боевого арсенала, который уже отправлен на переплавку. В связи с этим Кларк и Вилсон указывают на необходимость регулярных проверок, имеющих целью выявление возможных несоответствий между защищаемыми данными и объективной реальностью, которую они отражают.

Управление передачей привилегий необходимо для эффективной работы всей политики безопасности. Если схема назначения привилегий неадекватно отражает организационную структуру предприятия или не позволяет администраторам безопасности гибко манипулировать ею для обеспечения эффективности производственной деятельности, защита становится тяжким бременем и провоцирует попытки обойти ее там, где она мешает «нормальной» работе.

С некоторыми оговорками иногда в зарубежной научной литературе в основу контроля целостности закладывается и принцип *обеспечения непрерывной работы* (включая защиту от сбоев, стихийных бедствий и других форс-мажорных обстоятельств), который в классической теории компьютерной безопасности относится скорее к проблеме доступности данных.

В основу последнего девятого принципа контроля целостности – *простота использования защитных механизмов* – заложен ряд идей, реализация которых направлена на эффективное применение имеющихся механизмов обеспечения безопасности.

На практике зачастую оказывается, что предусмотренные в системе механизмы безопасности некорректно используются или полностью игнорируются по следующим причинам:

• неправильно выбранные производителем конфигурационные параметры по умолчанию обеспечивают слабую защиту;

• плохо разработанные интерфейсы управления защитой усложняют использование даже простых средств безопасности;

• имеющиеся средства безопасности не обеспечивают адекватный уровень контроля за системой;

• реализация механизмов безопасности плохо соответствует сложившемуся у администраторов интуитивному их пониманию;

• отдельные средства защиты плохо интегрированы в общую схему безопасности;

• администраторы недостаточно осведомлены о важности применения конкретных механизмов защиты и их особенностях.

Простота использования защитных механизмов подразумевает, что самый безопасный путь эксплуатации системы будет также наиболее простым, и наоборот, самый простой – наиболее защищенным.