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 5. Защита от угрозы нарушения целостности информации на уровне содержания

Защита от угрозы нарушения целостности информации на уровне содержания в обычной практике рассматривается как защита от дезинформации. Пусть у злоумышленника нет возможности воздействовать на отдельные компоненты ТКС, находящиеся в пределах контролируемой зоны, но, если источники поступающей в нее информации находятся вне системы, всегда остается возможность взять их под контроль противоборствующей стороной. При намеренной дезинформации применяют как заведомую ложь, так и полуправду, исподволь подталкивающую воспринимающих ее к ложным суждениям.

Наиболее распространенные приемы дезинформации:

• прямое сокрытие фактов;

• тенденциозный подбор данных;

• нарушение логических и временных связей между событиями;

• подача правды в таком контексте (добавлением ложного факта или намека), чтобы она воспринималась как ложь;

изложение важнейших данных на ярком фоне отвлекающих внимание сведений;

• смешивание разнородных мнений и фактов;

• изложение данных словами, которые можно истолковывать по-разному;

• отсутствие упоминания ключевых деталей факта.

Кроме того, в процессе сбора и получения информации возникают искажения.

Основные причины искажений информации:

• передача только части сообщения;

• интерпретация услышанного в соответствии со своими знаниями и представлениями;

• пропуск фактуры через призму субъективно-личностных отношений.

Для успешности *борьбы с вероятной дезинформацией* следует:

• различать факты и мнения;

• применять дублирующие каналы информации;

• исключать все лишние промежуточные звенья и т. п.

Проблема защиты информации в АС от угрозы нарушения целостности на уровне содержания информации до сих пор не ставилась в силу того, что в качестве автоматизированных систем рассматривались, как правило, системы учета, в которых изменение содержания одной записи практически не вызывало противоречий в содержании остальных записей. Вместе с тем даже в обычных учетных АС необходимо предусматривать наличие подсистем, проводящих первичный смысловой анализ и в определенной степени контролирующих работу оператора. Наличие подобных подсистем позволяет защитить информацию в АС не только от случайных, но и преднамеренных ошибок.