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

РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ (ПРЕЗЕНТАЦИИ К ЛЕКЦИОННЫМ МАТЕРИАЛАМ)

Безопасность систем баз данных

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

Уровень	специалист
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	10.03.01 «Информационная безопасность автоматизированных систем»
	(код и наименование)
Институт	Кибербезопасности и цифровых технологий
	(полное и краткое наименование)
Кафедра	Информационно-аналитические системы кибербезопасности (КБ-2)
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	К.т.н., доцент Шукенбаев Айрат Бисенгалеевич
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/2024
(учебный год цифрами)

Проверено и согласовано «____» _____20___г.

_____ А.А. Бакаев
(подпись директора Института/Филиала с расшифровкой)

Москва 2024 г.

Ощущение полной безопасности наиболее опасно.
Илья Нисонович Шевелев
Везде, где есть жизнь, есть и опасность.
Ральф Уолдо Эмерсон

Безопасность систем баз данных.

Тема лекции: Политика безопасности.

Сущность политики безопасности. Цель формализации политики безопасности. Принципы построения защищенных систем баз данных. Стратегия применения средств обеспечения информационной безопасности

Сущность политики безопасности

Политика безопасности — это совокупность норм и правил, определяющих принятые в организации меры по обеспечению безопасности информации, связанной с деятельностью организации.

Наибольшее распространение в настоящее время получили две базовые модели безопасности данных: дискреционная и мандатная.

Цель формализации политики безопасности

Цель формализации политики безопасности для информационной системы — ясное изложение взглядов руководства организации на существо угроз информационной безопасности организации и технологий обеспечения безопасности ее информационных ресурсов.

Политика безопасности обычно состоит из двух частей:

общих принципов

конкретных правил работы с информационными ресурсами и, в частности, с базами данных для различных категорий пользователей.

Политика безопасности — это всегда некоторый компромисс между желаемым уровнем защищенности ресурсов информационной системы, удобством работы с системой и затратами средств, выделяемых на ее эксплуатацию.

В руководстве по компьютерной безопасности, разработанном национальным институтом стандартов и технологий США (National Institute of Standards and Technology — NIST), рекомендовано включать в описание политики безопасности следующие разделы.

- *Предмет политики*
- *Описание позиции организации*
- *Применимость*.
- *Роли и обязанности*
- *Соблюдение политики*

Комплект документов, представляющий основные решения организации по реализации политики безопасности, должен включать:

— документацию, определяющую используемые подходы к оцениванию и управлению рисками для организации в целом и при необходимости конкретных подразделений;

— обоснование принятых решений по выбору средств защиты для рассматриваемой информационной системы;

— формальное описание процедуры определения допустимого уровня остаточного риска;

— директиву, определяющую процедуру проверки режима информационной безопасности и журналов, в которых фиксируются результаты проверки;

— документацию, регламентирующую процессы обслуживания и администрирования информационных систем;

— документацию по подготовке периодических проверок по оцениванию и управлению рисками;

— документ «Ведомость соответствия», включающий сведения по организации системы управления информационной безопасностью и регистрации средств управления безопасностью;

— контрмеры для противодействия выявленным рискам.

Принципы построения защищенных систем баз данных

Британский стандарт BS 7799 и созданный на его основе международный стандарт ISO 17799.

Анализ наиболее успешных решений в области обеспечения информационной безопасности баз данных позволил сформулировать несколько полезных принципов, которыми можно руководствоваться при проектировании систем защиты:

— экономическая оправданность механизмов защиты;

— открытое проектирование;

— распределение полномочий между различными субъектами в соответствии с правилами организации;

— минимально возможные привилегии для пользователей и администраторов;

— управляемость системы при возникновении отказов и сбоев;

— психологическая приемлемость работы средств защиты данных.

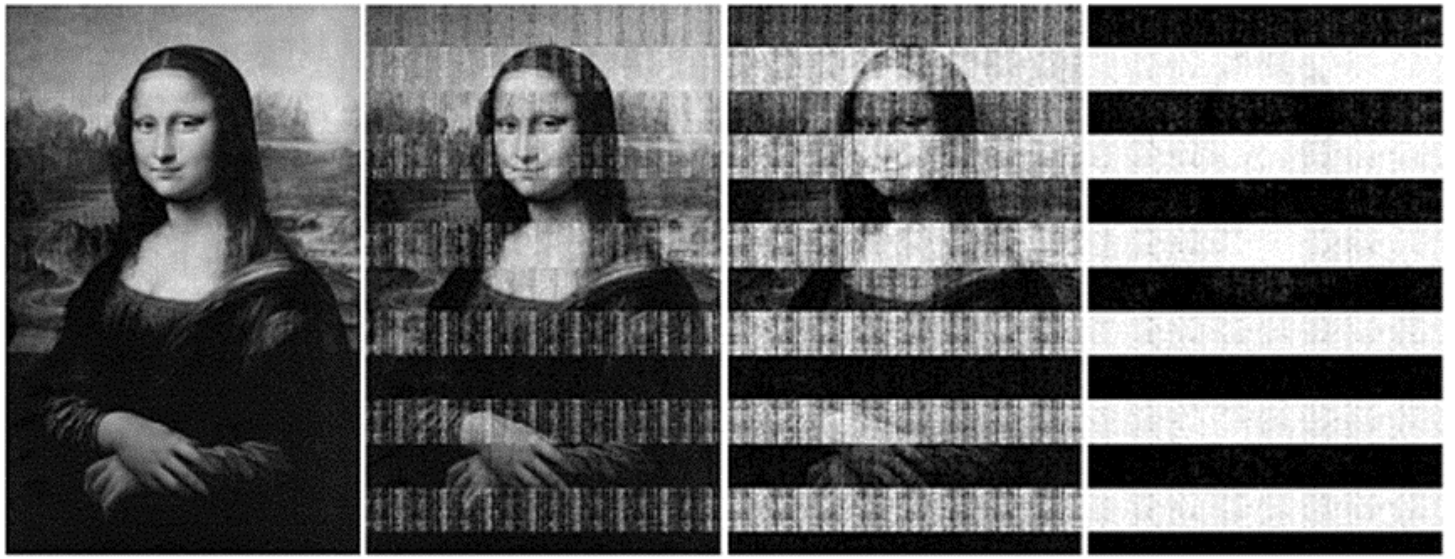

Рис. 1. Серия копий изображения, восстановленных из дампов оперативной памяти, снятых через 5, 30, 60 и 300 секунд после отключения питания

Стратегия применения средств обеспечения информационной безопасности

Стратегия определяет структуру, приоритеты и методы принятия решений при организации и обеспечении соответствующего вида деятельности.

Существует несколько проблем, затрудняющих формальную постановку пары двойственных задач:

— определение ценности информационных ресурсов и оценка ущерба от конкретных действий или событий часто может быть выполнена только на качественном уровне;

— эффективность методов и средств обеспечения информационной безопасности зависит от большого числа случайных и трудно предсказуемых факторов, таких как поведение злоумышленника, воздействие природных явлений, случайные сбои и необнаруженные ошибки в системе обработки информации и т. п.;

— организационные меры по обеспечению информационной безопасности связанны с действиями людей, эффективность которых также трудно оценить количественно.

В реальной практике обычно используются качественные оценки или оценки в ранговых шкалах. Например, можно рассмотреть проектные решения, которые обеспечат требуемый уровень защиты:

— от наиболее опасных из известных угроз;

— от всех идентифицированных угроз;

— от всех потенциально возможных угроз.

Можно выделить несколько вариантов, в значительной степени определяющих существо возможных проектных решений:

— никакое вмешательство в информационную систему не допускается;

— допускается частичное изменение архитектуры информационной системы;

— требования, обусловленные необходимостью обеспечения информационной безопасности, принимаются в полном объеме при проектировании и эксплуатации системы обработки информации.

Таблица 3.1. Стратегия обеспечения информационной безопасности

Учитываемые угрозы	Влияние на информационные системы			
Наиболее опсные	отсутствует	частично	существенные	
Все идентифицированные угрозы	Оборонительная стратегия	Наступательная стратегия		
Все потенциально возможные			Упреждающая стратегия	

Выбирая оборонительную стратегию, проектировщик должен четко понимать и грамотно объяснить руководству, что если исключить вмешательство в процесс функционирования информационной системы, то можно нейтрализовать лишь наиболее опасные угрозы.

Наступательная стратегия предусматривает активное противодействие известным угрозам, влияющим на информационную безопасность.

Упреждающая стратегия предполагает тщательное исследование возможных угроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы.