



**ЦЕНТР ЗАЩИТЫ
ИНФОРМАЦИИ**
НОВОСИБИРСКОЙ ОБЛАСТИ

Основные направления информационной безопасности

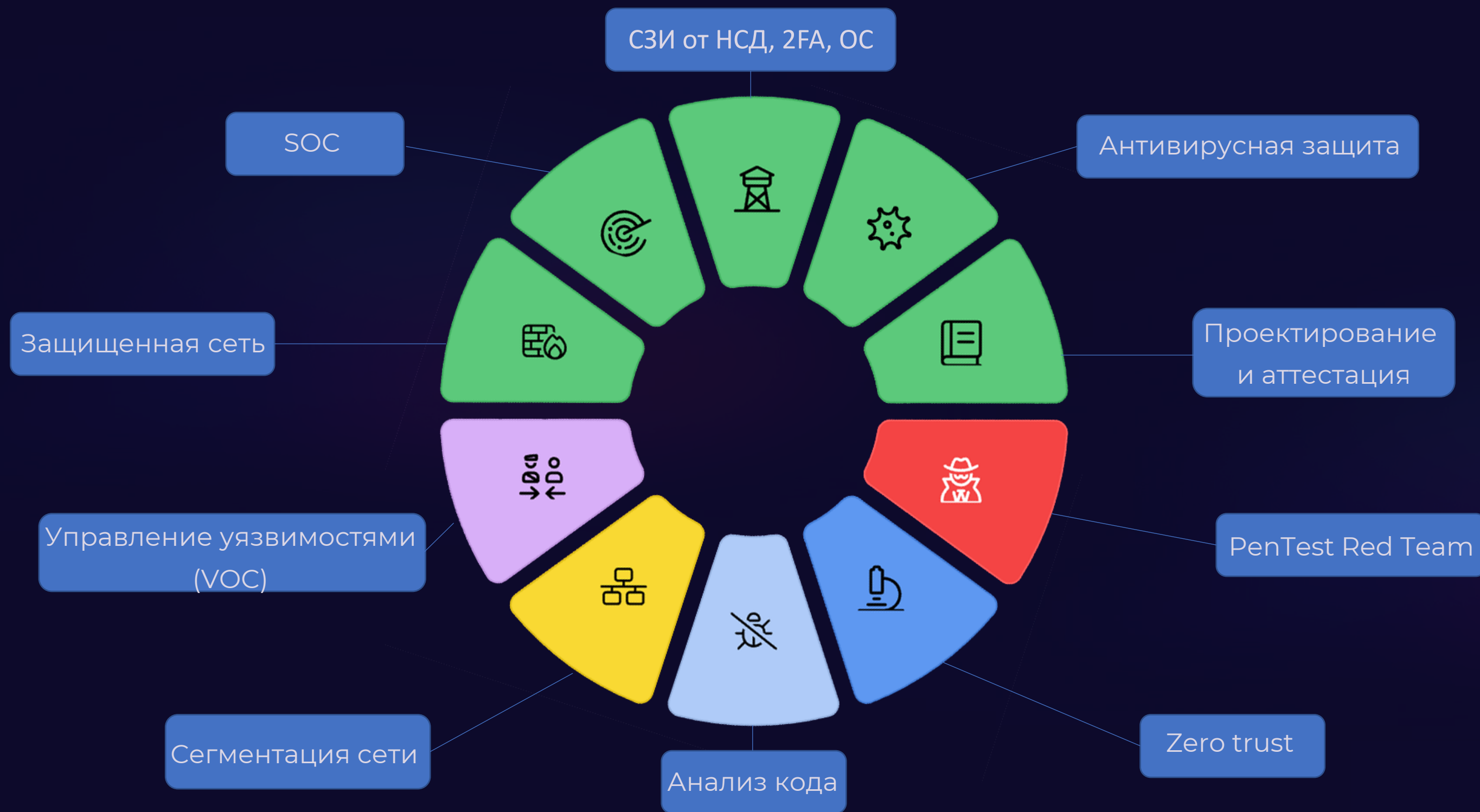
Регулирование защиты информации
со стороны государства

Швецов Валентин
Вячеславович



МИНЦИФРА
НОВОСИБИРСКОЙ
ОБЛАСТИ

Комплексная система информационной безопасности



Проектирование и аттестация

0 Уровень

Проектирование сегментированной инфраструктуры

Анализ кода

Заведомый выбор безопасных решений

1 Уровень

Выбор актуальных угроз и нарушителей (Модель угроз)

Выбор актуальных мер защиты

Выбор средств и систем защиты

Внедрение

2 Уровень

Проведение испытаний

Аттестация



Средства защиты



- системы криптографической защиты (СКЗИ) для шифрования каналов связи
- межсетевые экраны (межсетевые экраны между сегментами ЛВС и на границе с внешними сетями для фильтрации трафика);
- система обнаружения и предотвращения вторжений (СОВ/СОП, для мониторинга сетевого трафика и событий безопасности);
- система сбора и анализа событий (SIEM);
- система защиты от утечек данных (DLP);
- антивирусная система (на все узлы, где обрабатываются файлы или могут быть вирусные угрозы);
- система защиты от несанкционированного доступа (СЗ от НСД – программные или программно-аппаратные средства, контролирующие доступ пользователей к ресурсам системы);
- система защиты среды виртуализации (СЗ ВИ);
- система контроля действия привилегированных пользователей (РАМ);
- система анализа защищенности (сканер уязвимостей (САЗ)).

Регуляторы и законы



1 Уровень

Федеральные законы

2 Уровень

Постановления правительства

Постановления президента

3 Уровень

Нормативно-правовые акты регуляторов:

ФСТЭК России

ФСБ России

Роскомнадзор

Центральный Банк России

Минцифра РФ

ГОСТы





ФСТЭК России

Обеспечение безопасности критической информационной инфраструктуры России.

Противодействие иностранным техническим разведкам на территории России.

Защита информации, в том числе содержащей сведения, составляющие государственную тайну, и другой информации с ограниченным доступом.

Защита информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

Экспортный контроль. В частности, выдача лицензий на осуществление операций по экспорту и (или) импорту товаров, информации, результатов интеллектуальной деятельности.



ФСБ России

Защита информационного поля. Формирование и реализация мер государственной политики посредством применения криптографических и технических средств защиты телекоммуникационных систем и иных видов связи, а также лицензирование некоторых видов деятельности, связанных с доступом к информации, составляющей гос. тайну.

Роскомнадзор

Контроль за соблюдением законодательства в интернете.

Роскомнадзор блокирует сайты с запрещённым контентом:

экстремистские материалы, пиратские фильмы, детскую порнографию.

Лицензирование и регулирование вещания.

Служба выдаёт разрешения на вещание и распределяет радиочастоты.

Регистрация средств массовой информации (СМИ).

Газеты, журналы, телеканалы и интернет-издания должны быть официально зарегистрированы.

Надзор в сфере связи.

Ведомство следит за качеством услуг операторов связи и распределяет радиочастоты для сотовых компаний.

Защита прав граждан.

Контроль за обработкой персональных данных и качеством услуг связи направлен на защиту интересов потребителей.

Обеспечение стабильности связи.

Распределение частот и контроль за их использованием помогают избежать «хаоса» в эфире и обеспечить качественную связь.



Минцифра Российской Федерации

Регулирование телекоммуникаций.

Ведомство устанавливает правила и тарифы для операторов связи, следит за качеством услуг.

Цифровая идентификация.

Минцифры создаёт системы для безопасной идентификации личности при использовании цифровых сервисов.

Сервисы и клиентский опыт.

Ведомство следит за удобством и качеством электронных услуг для граждан.

Инфраструктура электронного правительства.

Поддерживает цифровые сервисы социальной сферы: здравоохранение, образование, соцзащиту.

Поддержка медиа и печатной продукции.

Минцифры разрабатывает программы развития государственных СМИ, периодической печати и книжной индустрии.

Развитие искусственного интеллекта и больших данных.

Ведомство внедряет ИИ-системы и аналитические решения для государственных органов.



ЦБ России и ГОСТ



ГОСТ Р 57580.1-2017 — национальный стандарт Российской Федерации, который называется
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»

ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования

ISO/IEC 27001: «Информационные технологии. Методы защиты.

Системы менеджмента информационной безопасности. Требования и определения».

Стандарт направлен на сохранение конфиденциальности, целостности и доступности информации.

ISO/IEC 27002: «Информационные технологии. Методы и средства обеспечения безопасности.

Свод норм и правил применения мер обеспечения информационной безопасности».

ISO/IEC 27005: предоставляет руководство по менеджменту рисков информационной безопасности, которое включает в себя рекомендации по оценке, коммуникации, мониторингу и пересмотру рисков.

ISO/IEC 27006: «Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности».

ISO/IEC 27007: «Руководство для аудитора систем менеджмента информационной безопасности».

ISO/IEC 27011: «Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002».





**ЦЕНТР ЗАЩИТЫ
ИНФОРМАЦИИ**
НОВОСИБИРСКОЙ ОБЛАСТИ



МИНЦИФРА
НОВОСИБИРСКОЙ
ОБЛАСТИ

Собираем пазл защиты

Спасибо!

