

Тенденции

кибербезопасности 2025

*Актуальные вызовы и изменения
в подходах защиты*

2025 г.

*Валерий Ледовской,
директор по развитию*

– ведущий системный интегратор на российском рынке информационной безопасности. Обеспечиваем защиту информационных ресурсов, оказываем экспертно-аналитические, технические, консалтинговые услуги. Имеем собственные разработки по направлениям SIEM систем, архивации данных, УПДн, а также двухконтурным аппаратным комплексам.



ЛИЦЕНЗИИ ФСТЭК

На деятельность по разработке и производству средств защиты конфиденциальной информации от 23 июня 2017 г. № 1764

На деятельность по технической защите конфиденциальной информации от 23 июня 2017 г. № 3319



ЛИЦЕНЗИИ ФСБ

Лицензия УФСБ России на проведение работ, связанных с использованием сведений, составляющих государственную тайну



ЛИЦЕНЗИЯ МЧС

МЧС по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений



СЕРТИФИКАТ

Соответствия системы менеджмента качества стандарту ISO 9001:2015 (ГОСТ Р ISO 9001-2015)



ЛИЦЕНЗИЯ МИНОБОРОНЫ РОССИИ

Направления деятельности

Инфраструктурные решения

Аудит и консалтинг

Информационная безопасность в АСУ ТП

Инженерные решения

Собственные разработки

IT-инфраструктура. Решения для защиты

Импортозамещение в сфере информационной безопасности

Наши решения

ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№15721 от 05.12.2022 г.



ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№16999 от 21.03.2023 г.



ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№10346 от 21.04.2021

Модуль
«Учёт
персональных
данных»

МОДЕЛЬ УГРОЗ
И НИКАКИХ ОБЛАКОВ



Наши партнёры



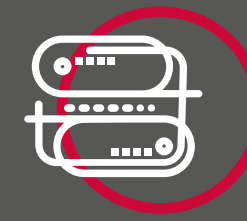
Основные киберугрозы 2024

Вредоносное ПО:



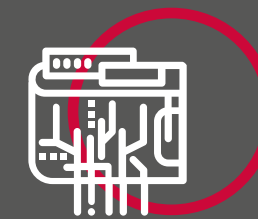
- 26 новых семейств шифровальщиков (LockBit, WannaCry)
- 85% компьютеров заражены рекламным ПО

IoT:



88% атак через Telnet
(ГОСТ на кибериммунные системы)

Тренды:



Рост эксплойтов для Linux (+56,5%)
и Windows (+20%)

Тренды угроз 2024–2025



Рост целевых атак:
APT, RaaS, хактивизм

Использование ИИ: дипфейки,
автоматизация фишинга

Гибридные атаки: внешние +
внутренние нарушители

Уязвимости цепочки поставок
и слабый контроль доступа
подрядчиков

Угрозы для IoT, АСУ ТП
(+160% в РФ) и цифровых валют

Кибератаки на российские компании

5% атак — высокая критичность

Лидеры по инцидентам:

- Госсектор (50%)
- Финансовый сектор, транспорт

Выводы:

- Базовой защиты недостаточно
- Необходимы EDR, NTA, Threat Intelligence

Утечки данных 2024



778 инцидентов (как в 2023), но

1,5 млрд ПДн
утекло (+30%)

Сфера торговли:

35% утечек (2023: 21%)

Основные причины:

- Внешние нарушители (76,9%)
- Умышленные действия сотрудников (95% внутренних инцидентов)

Риски:

малый бизнес (28%),
аутентификационные данные (29%)

Ущерб от утечек

Средние расходы:

- Расследование: до 5,6 млн ₽
- Ущерб: до 15,8 млн ₽

Максимальный ущерб:

До **140** млн ₽
(экспертная оценка)

Рекомендации:

- Периодические тесты на проникновение
- Автоматизация процессов ИБ

Киберустойчивость компаний

53%

компаний подвергались атакам за год

Проблемы:

- Сложность инфраструктуры
- Нехватка кадров и бюджета

Решения:

- 63% компаний планируют закупки новых ИБ-решений

Угрозы для АСУ ТП

Рост атак на промышленные системы: +160%

Основные векторы:

- учетные данные (20%), цепочки поставок (15%)

Цели:

- остановка производства, саботаж

Приоритеты защиты:

- мониторинг сетей (65%), сегментация (32%)



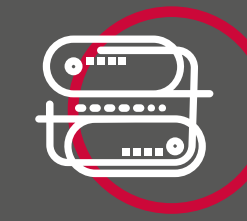
Финансовый сектор 2024

Тренды 2024:



- Атаки через подрядчиков (17 инцидентов)
- Скрытые каналы передачи данных (Ngrok, DNS over HTTPS)

Прогноз 2025:



- Деструктивные атаки, сложности атрибуции
- **Рекомендации:** PAM, DСАР, изоляция резервных копий



Цифровой рубль

Этапы:

- 2025 пилотирование → полноценный запуск к 2027

Угрозы:

- хакерские атаки нового типа

Защита:

- модели угроз, проверка инфраструктуры, соответствие требованиям регуляторов

Рекомендации по защите 2025

1. Доступ: NGFW, MFA, PAM

 <i>UserGate</i>	 <i>Ideco</i>
 <i>Indeed AM</i>	 <i>Мультифактор</i>
 <i>Indeed PAM</i>	 <i>SafeInspect</i>



2. Технологии: EDR/NTA, DСАР, DLP, Patch Management

 <i>Kaspersky</i>	 <i>Positive Technologies</i>
 <i>Makves</i>	 <i>Спектр</i>
 <i>Infowatch</i>	 <i>StaffCop</i>
 <i>Kaspersky</i>	 <i>Rudesktop</i>

3. Обучение: Security Awareness

 <i>Phishman</i>	 <i>Kaspersky</i>
--	---

4. Резервирование: Backup, изоляция резервных копий

 <i>Киберпротект</i>	 <i>RuBackup</i>
--	--

Рекомендации по защите 2025

5. Сотрудничество: Киберучения, обмен данными TI

 SOLAR

Solar

 positive technologies

Positive Technologies

 kaspersky

Kaspersky

6. Организация экосистемы ИБ: SIEM, инвентаризация, мониторинг внешних цифровых угроз

 RUSIEM

RuSIEM

 kaspersky

Kaspersky

 UMA

UMA

 positive technologies

Positive Technologies

 GIS ГАЗИНФОРМ СЕРВИС

GIS

 FUTURE CREW

FutureCrew

7. Оценка уровня внешней и внутренней защищённости

 Pentest

Pentest

 PT Dephaze

PT Dephaze

 CtrlHack

CtrlHack

 Pentest

Pentest

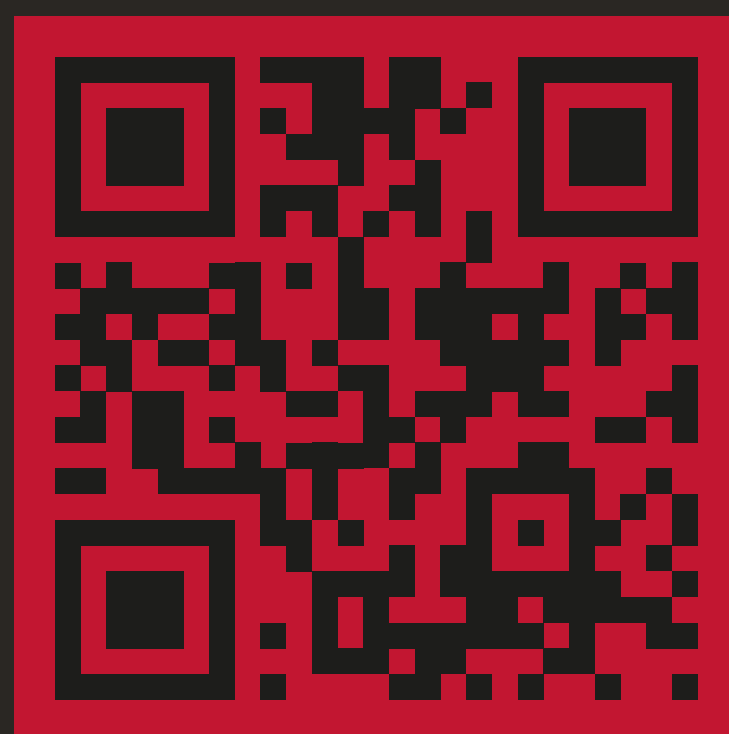
 Метаскан

Метаскан

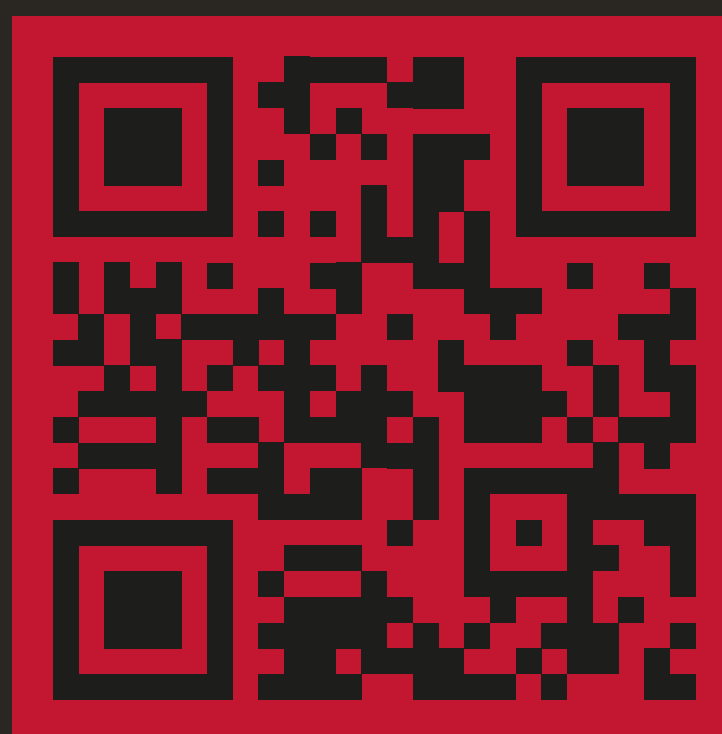
 Cicada8

Cicada8

Спасибо за внимание!



www.ARinteg.ru



t.me/ARinteg



vk.com/ARinteglife