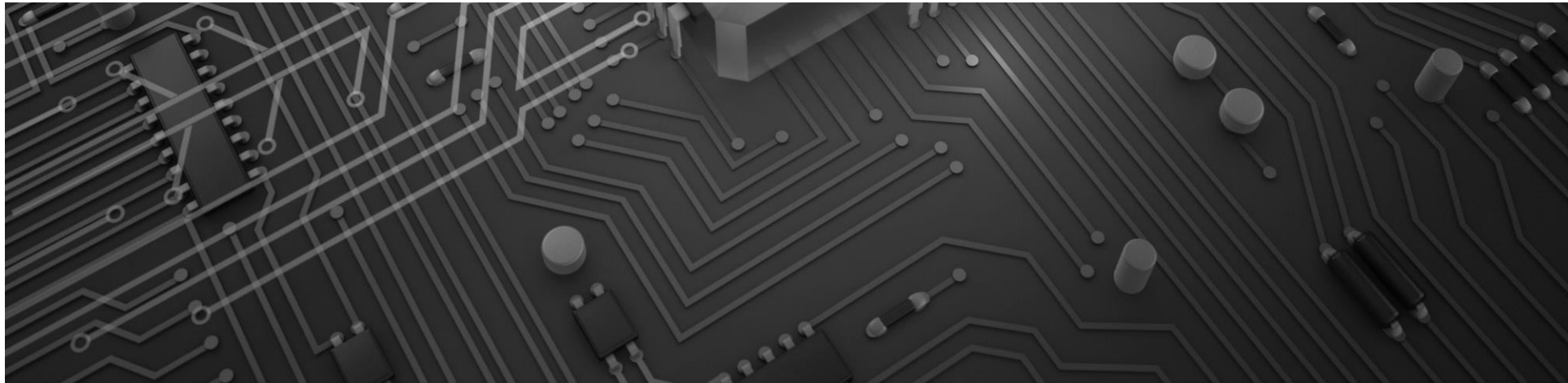
25 ЛЕТ

ARinteg®

Контроль привилегированных пользователей как инструмент дружбы ИТ и ИБ

ВАШ ГАРАНТ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

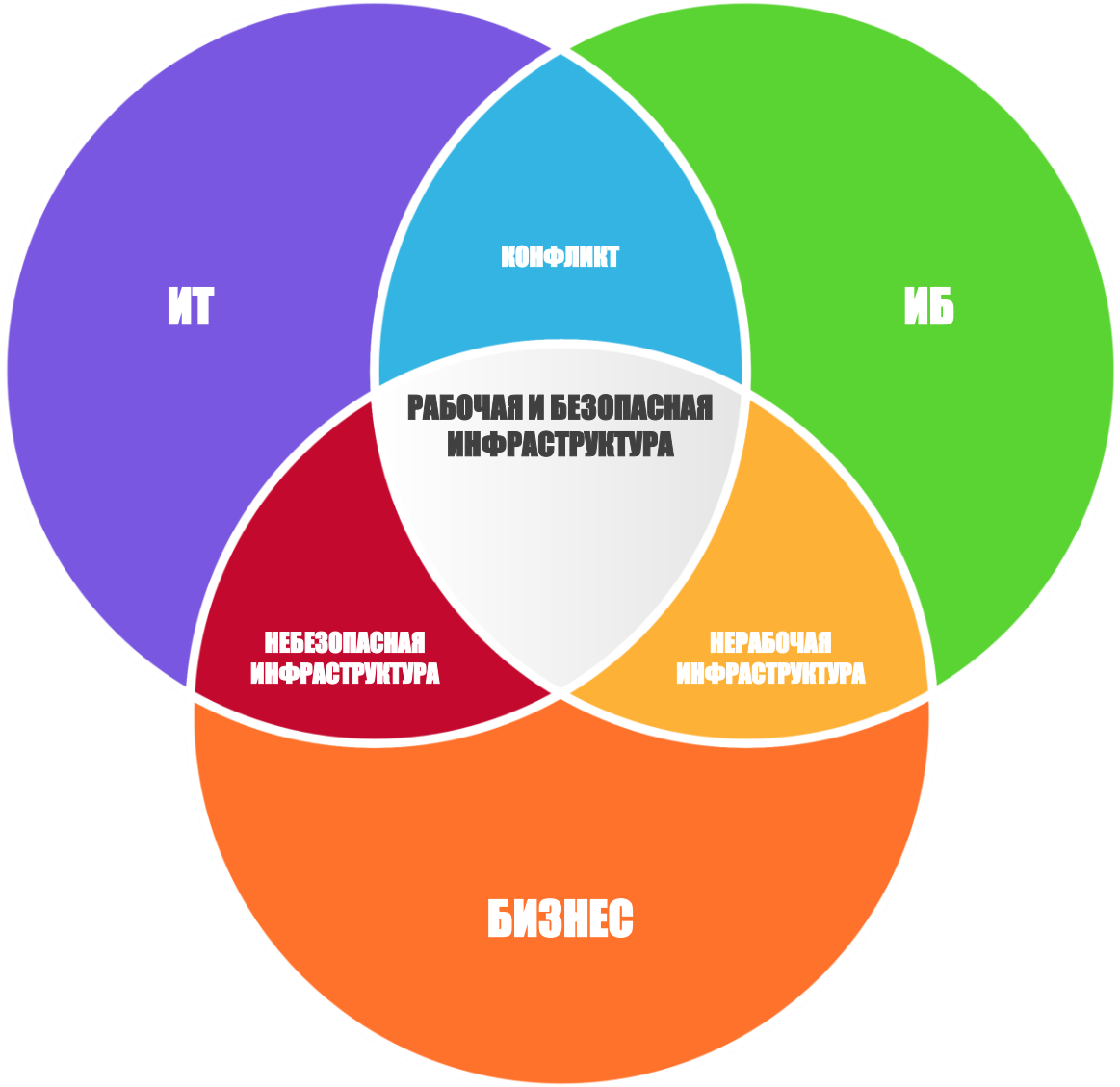


www.ARinteg.ru

Что общего у ИТ и ИБ?

ИТ	ИБ
Важно, что бы всё работало	Важно безопасно или нет
Расширение возможностей пользователя	Ограничение возможностей пользователя
Удобно использовать	Безопасно использовать
Простои	Риски
Превентивное выделение бюджета	Реактивное выделение бюджета
DevOps	DevSecOps

БИЗНЕС


ИТ
КОНФЛИКТ
ИБ
РАБОЧАЯ И БЕЗОПАСНАЯ ИНФРАСТРУКТУРА
НЕБЕЗОПАСНАЯ ИНФРАСТРУКТУРА
НЕРАБОЧАЯ ИНФРАСТРУКТУРА
БИЗНЕС

Почему важно?

LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser

21 июня 2021 г.

Группировка LockBit 2.0 начала вербовать корпоративных инсайдеров, чтобы те помогали им взламывать внутренние сети. Взамен им обещают вознаграждения в **миллион долларов**. Группировка заинтересована в RDP, VPN, учетных данных корпоративной электронной почты и других данных, которые она может использовать для получения доступа к сети. Хакеры поясняют, что они отправят инсайдеру «вирус», который должен быть запущен на компьютере и даст удаленный доступ к сети. Связь с хакерами осуществляется через мессенджер Tox.

8 августа 2021 г.

Австралийский центр кибербезопасности (ACSC) предупредил о росте числа атак программ-вымогателей из семейства LockBit 2.0 на австралийские компании начиная с июля 2021 года

10 августа 2021 г.

Энергетическая компания ERG из Италии сообщила о сбоях в работе её ИТ-систем после атаки программы-вымогателя. Отмечается, что атака была проведена с применением LockBit

11 августа 2021 г.

«Консалтинговая ИТ-компания Accenture (выручка $32,9 млрд., число сотрудников 384 000 (2016 г.)) стала жертвой вымогателя LockBit 2.0. Однако в компании уверяют, что инцидент не повлиял на ее работу, а пострадавшие системы уже восстановлены из резервных копий»

RAAS

Ransomware as a Service — RaaS

RaaS аналогичны предложениям традиционных поставщиков SaaS и могут принимать одну из следующих форм:

Единовременная плата за лицензию: Предоставляет неограниченный доступ к услуге без будущих платежей.

Ежемесячная ставка: покупатели платят фиксированную ежемесячную плату.

Распределение прибыли: оператор получает долю прибыли от каждой успешной атаки, аналогично партнерской программе.

Некоторые модели могут включать комбинацию типов оплаты. Например, участие в прибыли можно комбинировать с лицензионным платежом или ежемесячной оплатой

Внедрение и подбор продуктов

- Аудит информационных систем
- Пилотные внедрения
- Импортозамещение
- ФЗ-152 «О персональных данных»
- ФЗ-187 КИИ
- ГОСТ 57580

Алексей Курских

Aleksey.Kurskikh@ARinteg.ru

Тел.: +7 (985) 414-42-32

www.ARinteg.ru

Наши офисы:

Москва, ул. Радио, д. 24, к. 1

+7 (495) 221-21- 41

г. Санкт-Петербург, пр. Шаумяна, д. 8

+7 (812) 407-34-71

г. Ростов-на-Дону, ул. Береговая, 8

+7 (963) 320-09-60

Мы в соцсетях:

@arinteg.ru

t.me/ARinteg

facebook.com/ARinteg