ИТ ЭНИГМА

ЗАЩИЩАЕМ ЦЕННУЮ ДЛЯ ВАС ИНФОРМАЦИЮ

Актуальные вопросы защиты объектов КИИ:

категорирование | разработка и внедрение подсистем безопасности

О Центре

ЦЕНТР КОМПЕТЕНЦИЙ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Целью работы Центра является содействие в обеспечении защиты информационных систем организаций и предприятий критических отраслей и сфер экономики Российской Федерации. Основным законодательным актом, определяющим деятельность Центра является Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

В центр компетенций организации - субъекты критической информационной инфраструктуры могут обращаться по вопросам:

- категорирования объектов КИИ
- проведения аудита на соответствие требованиям законодательства и стандартов информационной безопасности
- обучения специалистов
- проектирования и внедрения систем защиты объектов КИИ.

23
проекта
определения объектов КИИ и их категорирования, проектирования подсистем защиты

4
региона
в которых проведены проекты

57
объектов КИИ
выявленных в ходе обследований и описанных в рамках категорирования

КТО ПОПАДАЕТ ПОД 187 ФЗ. ОБЪЕКТЫ И СУБЪЕКТЫ КИИ

ИТ ЭНИГМА

Согласно
п. 7 и 8 Ст. 2
187 ФЗ
«О безопасности
критической
информационной
инфраструктуры
Российской
Федерации»

Субъекты КИИ

- Гос. органы
- Гос. учреждения
- Юридические лица
- Индивидуальные предприниматели

Которым принадлежат

Которые обеспечивают взаимодействие

Объекты КИИ

- Информационные системы
- Информационно-телекоммуникационные сети
- Автоматизированные Системы Управления

Работающие в отраслях

ПРОМЫШЛЕННОСТЬ

- Горно-добывающая
- Металлургическая
- Химическая
- Оборонная
- Ракетно-космическая

- Энергетика
- Атомная энергетика
- ТЭК
- Связь
- Транспорт
- Здравоохранение
- Банки
- Финансовая сфера
- Наука

127
Постановление
Правительства РФ

Объекты КИИ → Значимые / Не значимые

Значимые → 1 категория / 2 категория / 3 категория

↑ Рост значимости объекта КИИ

↑ Рост размера возможных негативных последствий инцидентов информационной безопасности

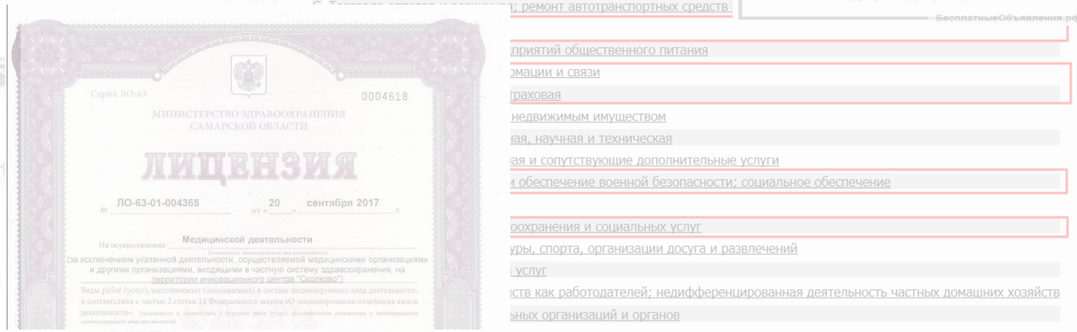
↑ Рост требований по защищенности объекта КИИ

Является ли моя организация субъектом КИИ?

Определение объектов КИИ и организации как субъекта КИИ

Работа организации в отраслях, указанных в 187 ФЗ

1) ОКВЭД
2) Устав
3) Лицензия
4) СРО
5) Декларация промышленной безопасности



Работа со специализированными отраслевыми информационными системами

1) Техническая документация на используемые ПО и ИС
2) Договоры с организациями, входящими в отрасли КИИ, о информационном взаимодействии с ними в части выполнения работ по основному профилю организации
3) Обслуживание отраслевых ПО и ИС

Задачи субъекта КИИ

- Необходимость отправки во ФСТЭК перечня объектов КИИ
- Необходимость отправки и согласования со ФСТЭК сведений о категории значимости объектов КИИ
- Риск получения штрафов за неисполнение предписаний ФСТЭК по работам категорирования объектов КИИ (Ст. 19.5 КоАП)

- Необходимость включения в бюджеты 2019г. мероприятий по защите значимых объектов КИИ
- Риски компьютерных атак и др. инцидентов информационной безопасности на значимых объектах КИИ
- Риск наступления уголовной ответственности для специалистов за нарушение условий эксплуатации ПО и ПАК объектов КИИ, приведших к компьютерным инцидентам (Ст. 1 п.4 194-ФЗ)

Проведение работ по определению объектов КИИ. Направление перечня объектов КИИ во ФСТЭК.	Необходимо уже сейчас!!!
Разработка технического задания на системы безопасности значимых объектов КИИ. Включение в бюджет 2019г. мероприятий по созданию систем безопасности значимых объектов КИИ.	ноябрь -декабрь 2018г.
Проведение работ по определению объектов КИИ. Направление и согласование со ФСТЭК сведений о присвоении категории значимости по каждому объекту КИИ	до декабря 2018г.

Общий алгоритм работ в рамках 187 ФЗ

127 Постановление Правительства РФ, 236 Приказ ФСТЭК

235 Приказ ФСТЭК, 239 Приказ ФСТЭК

Проведение категорирования объектов КИИ

1. Определение объектов КИИ
2. Направление во ФСТЭК перечня объектов КИИ
3. Проведение категорирования объектов КИИ
4. Направление во ФСТЭК сведений о категории значимости объектов КИИ

Необходимо провести уже сейчас!

Проектирование систем защиты значимых объектов КИИ

1. Определение типов и видов СЗИ
2. Определение требований к параметрам настройки ПО и ПАК, включая СЗИ
3. Определение мер безопасности при взаимодействии с др. объектами КИИ
4. Разработка рабочей документации

Внедрение систем защиты значимых объектов КИИ

1. Установка и настройка СЗИ
2. Внедрение орг. мер
3. Проведение предварительных испытаний
4. Проведение опытной эксплуатации
5. Проведение анализа уязвимостей
6. Проведение приемочных испытаний

Обеспечение безопасности значимых объектов КИИ

1. Осуществление мероприятий по обеспечению безопасности
2. Контроль состояния безопасности значимых объектов
3. Совершенствование безопасности значимых объектов
4. Проведение обучений
5. Взаимодействие с ГосСОПКА

Проведение ежегодного аудита безопасности значимых объектов КИИ

1. Проведение ежегодно внешних аудитов с привлечением лицензиатов в области информационной безопасности или внутренних проверок (только силами штатных сотрудников)

Категории значимости

Социальная значимость

Показатели критериев значимости	ЗНАЧЕНИЕ ПОКАЗАТЕЛЕЙ		
	III КАТЕГОРИЯ	II КАТЕГОРИЯ	I КАТЕГОРИЯ
Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
на территории, на которой возможно нарушение обеспечения жизнедеятельности населения			
Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений	вся территория 1 МО или 1 внутригородской территории города федерального знач.	выход за пределы территории 1 МО или 1 внутригородской территории города федерального знач., но не за пределы территории 1 субъекта РФ или территории города федерального знач.	выход за пределы территории 1 субъекта РФ или территории города федерального знач.
по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)			
Прекращение или нарушение функционирования объектов транспортной инфраструктуры	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
Прекращение или нарушение функционирования сети связи			
Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12, но более 6	менее 6

Категории значимости

Политическая значимость

Показатели критериев значимости	ЗНАЧЕНИЕ ПОКАЗАТЕЛЕЙ		
	III КАТЕГОРИЯ	II КАТЕГОРИЯ	I КАТЕГОРИЯ
Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	прекращение или нарушение функционирования органа государственной власти субъекта РФ или города федерального значения	прекращение или нарушение функционирования федерального органа государственной власти	прекращение или нарушение функционирования Администрации Президента РФ, Правительства РФ, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ
Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	нарушение условий договора межведомственного характера (срыв переговоров или подписания)	нарушение условий межправительственного договора (срыв переговоров или подписания)	нарушение условий межгосударственного договора (срыв переговоров или подписания)

Категории значимости

Экономическая значимость

Показатели критериев значимости	ЗНАЧЕНИЕ ПОКАЗАТЕЛЕЙ		
	III КАТЕГОРИЯ	II КАТЕГОРИЯ	I КАТЕГОРИЯ
Возникновение ущерба субъекту КИИ, который является гос. корпорацией, гос. унитарным предприятием, муниципальным унитарным предприятием, гос. компанией, организацией с участием государства и (или) стратегическим АО, стратегическим предприятием, оцениваемого в снижении уровня дохода (.....) по всем видам деятельности (% прогноз. объема годового дохода по всем видам деятельности)	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15
Возникновение ущерба бюджетам Российской Федерации	в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета)		
	в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета)		
	более 0,001, но менее или равно 0,05	более 0,005, но менее или равно 0,1	более 0,1
	в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)		
	более 0,01, но менее или равно 0,5	более 0,5 , но менее или равно 1	более 1
Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом КИИ, являющимся... системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно ... или системно значимой инфраструктурной орг. фин. рынка, оцениваемое среднедневным (...) количеством осуществляемых операций, (млн. единиц) (...)	более 3, но менее или равно 70	более 70, но менее или равно 120	более 120

Категории значимости

Экологическая значимость

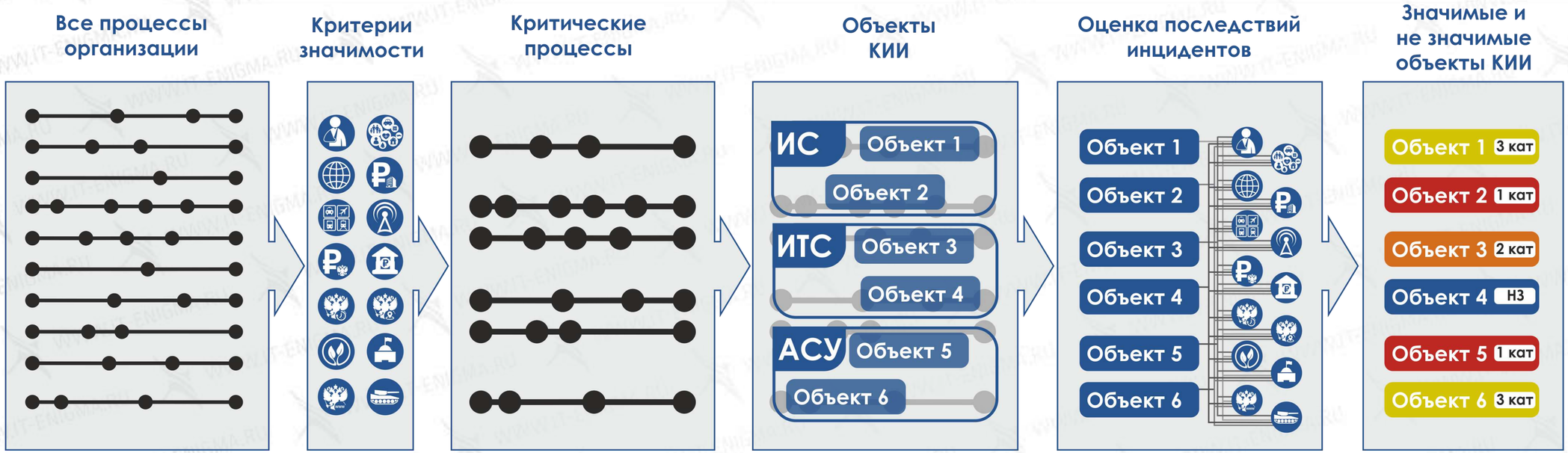
Показатели критериев значимости	ЗНАЧЕНИЕ ПОКАЗАТЕЛЕЙ		
	III КАТЕГОРИЯ	II КАТЕГОРИЯ	I КАТЕГОРИЯ
Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия)			
на территории, на которой окружающая среда может подвергнуться вредным воздействиям			
	вся территория 1 МО или 1 внутригородской территории города федерального знач.	выход за пределы территории 1 МО или 1 внутригородской территории города федерального знач., но не за пределы территории 1 субъекта РФ или территории города федерального знач.	выход за пределы территории 1 субъекта РФ или территории города федерального знач.
по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)			
	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000

Категории значимости

Значимость для обеспечения обороны страны, безопасности государства и правопорядка

Показатели критериев значимости	ЗНАЧЕНИЕ ПОКАЗАТЕЛЕЙ		
	III КАТЕГОРИЯ	II КАТЕГОРИЯ	I КАТЕГОРИЯ
Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	прекращение или нарушение функционирования пункта управления или ситуационного центра органа гос. власти субъекта рф или города федерального значения	прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа гос. власти или государственной корпорации	прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента рф, Правительства РФ, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ
Снижение показателей гос. оборонного заказа, выполняемого субъектом критической информационной инфраструктуры	в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции)		
	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15
	в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)		
	более 3, но менее или равно 10	более 10, но менее или равно 40	более 40
Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)	менее или равно 4, но более 2	менее или равно 2, но более 1	более 1

Процесс категорирования объектов КИИ



Действия	▶ Обследование и описание процессов ▶ Оценка возможности наступления последствий	▶ Обследование и инвентаризация ИС, ИТС, АСУ ▶ Формирование перечня объектов КИИ ▶ Утверждение перечня объектов КИИ ▶ Отправка перечня объектов КИИ во ФСТЭК	▶ Поиск уязвимостей ▶ Анализ угроз ▶ Определение последствий инцидентов ▶ Оценка ущерба ▶ Определение мер по ЗИ	▶ Формирование актов и сведений для ФСТЭК ▶ Утверждение акта о категорировании ▶ Отправка сведений во ФСТЭК
Документы	▶ Акт обследования процессов ▶ Описание процессов	▶ Акт обследования ИС, ИТС, АСУ ▶ Перечень объектов КИИ	▶ Акт о категорировании ▶ Сведения о категории значимости объектов КИИ	▶ ТЗ на создание системы защиты ЗОКИИ ▶ Акт о категорировании ▶ Сведения о категории значимости объектов КИИ
Сроки	▶ **Необходимо уже сейчас!**	▶ **Необходимо уже сейчас!** ▶ **Перечень объектов КИИ направляется во ФСТЭК в течении 5 раб. дней с момента его утверждения**	▶ **В течении 12 месяцев с момента подачи перечня объектов КИИ во ФСТЭК** ▶ **10 дней со дня утверждения акта отправка сведений** ▶ **10 дней на исправление предписаний ФСТЭК**	
ФСТЭК		▶ Принимает перечень объектов КИИ		▶ Проверяет сведения о результатах присвоения категорий значимости, далее их принимает или вносит предписания

Присвоение категории значимости объектам КИИ

Варианты проведения работ по категорированию объектов КИИ

Вариант проведения работ	Плюсы (+)	Минусы (-)	Для кого подходит
Самостоятельно своими силами	• Экономия средств бюджета организации	• Риск недостаточной экспертизы собственных сотрудников • Высокая загрузка работников оформлением большого количества документов • Риск получения предписаний по категорированию от ФСТЭК и срыва сроков их исправления	• Крупные предприятия и холдинги с собственными службами информационной безопасности численностью от 10 специалистов
Самостоятельно своими силами с использованием систем автоматизации документооборота	• Получение готовых шаблонов необходимых документов • Автоматическое заполнение типовых документов	• Риск недостаточной экспертизы собственных сотрудников • Риск получения предписаний по категорированию от ФСТЭК и срыва сроков их исправления • Неприменимость к нетиповым ИС, АСУ, ИТКС	• Организации с типовыми ИС и с собственными службами информационной безопасности численностью от 5 специалистов
Привлечение к работам организаций лицензиатов ФСБ и ФСТЭК	• Получение надежной высокой экспертизы подготавливаемой документации • Гарантии своевременного исправления всех предписаний ФСТЭК • Корректное описание нетиповых ИС, АСУ и ИТКС	• Дополнительные затраты в бюджете организации	• Организации без собственных служб информационной безопасности или с небольшой численностью специалистов в них (до 5); • Организации с нетиповыми ИС, АСУ и ИТКС

Законодательство в области защиты объектов КИИ

Обеспечение безопасности объектов КИИ

235 Приказ ФСТЭК от 21.12.2017.
«Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»

- Описывает назначение и состав систем безопасности значимого объекта КИИ
- Описывает требования к службам, ответственным за безопасность значимого объекта КИИ
- Описывает требования к СЗИ и ОРД обеспечивающих безопасность значимого объекта КИИ
- Описывает требования к мероприятиям, обеспечивающих функционирование системы безопасности значимого объекта КИИ

808 Постановление Правительства РФ
от 11.07.2018г.
«О внесении изменения в Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса»

239 Приказ ФСТЭК от 25.12.2017.
«Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»

- Описывает требования и этапы создания систем безопасности значимого объекта КИИ
- Описывает состав этапов создания систем безопасности значимого объекта КИИ и требования к ним
  - в составе этапов:
    - Разработки технического задания
    - Разработки организационных и технических мер
    - Внедрения организационных и технических мер (установка СЗИ, внедрение орг. мер, предварительные испытания, опытная эксплуатация, анализ уязвимостей, приемочные испытания)
    - Обеспечения безопасности в ходе эксплуатации
    - Обеспечения безопасности при выводе из эксплуатации
- Описывает требования к организационным и техническим мерам, обеспечивающим безопасность значимого объекта КИИ
- Содержит перечень и состав мер по обеспечению безопасности значимого объекта КИИ в соответствии с категорией значимости объекта (17 типов мер)

Дополнительно, если объект КИИ обрабатывает:

Государственную тайну	Персональные данные	ГИС	ИТКС
Законодательство в области защиты гостайны	Постановление Правительства РФ №1119	17 Приказ ФСТЭК	НПА Минкомсвязи РФ

239 Приказ ФСТЭК

Типы средств защиты информации и ПО

Состав мер по обеспечению безопасности для значимого объекта КИИ

I	Идентификация и аутентификация (ИАФ)
II	Управление доступом (УПД)
III	Ограничение программной среды (ОПС)
IV	Защита машинных носителей информации (ЗНИ)
V	Аудит безопасности (АУД)
VI	Антивирусная защита (АВЗ)
VII	Предотвращение вторжений (компьютерных атак) (СОВ)
VIII	Обеспечение целостности (ОЦЛ)
IX	Обеспечение доступности (ОДТ)
X	Защита технических средств и систем (ЗТС)
XI	Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
XII	Реагирование на компьютерные инциденты (ИНЦ)
XIII	Управление конфигурацией (УКФ)
XIV	Управление обновлениями программного обеспечения (ОПО)
XV	Планирование мероприятий по обеспечению безопасности (ПЛН)
XVI	Обеспечение действий в нештатных ситуациях (ДНС)
XVII	Информирование и обучение персонала (ИПО)

Средства защиты информации

- Антивирусы
- Сканеры уязвимостей
- Средства резервного копирования
- Средства криптографической защиты информации
- Межсетевые экраны
- Средства защиты от несанкционированного доступа и DLP
- Средства доверенной загрузки
- Средства защиты виртуализации
- Средства обнаружения и предотвращение атак (IDS / IPS)
- Системы сбора и анализа событий информационной безопасности (SIEM)
- Эмуляторы среды функционирования программного обеспечения - Песочницы (Sandbox)
- Системы повышения осведомленности по ИБ (Security Awareness)
- Сервисы автоматизации документооборота ИБ

Спасибо за внимание!

АЛЕКСАНДР МЕТАЛЬНИКОВ
Эксперт-консультант в области
информационной безопасности,
ИТ ЭНИГМА

ТЕЛЕФОН: +7 (351) 734-95-00

EMAIL: METALNIKOV@IT-ENIGMA.RU

FACEBOOK: www.facebook.com/groups/itenigma74/