



ИНФОРМАЦИОННАЯ СПРАВКА

ООО "Региональный Центр информационной безопасности" (ООО "РЦИБ") создано в 2008 году и является аккредитованной Росжелдором и Росавтодором Минтранса организацией на проведение работ по оценке уязвимости объектов транспортной инфраструктуры и транспортных средств (ОТИ и ТС) в соответствии с требованиями Федерального закона от 09.02.2007 г. №16-ФЗ "О транспортной безопасности".

ООО "РЦИБ" аккредитовано в системе сертификации ФСТЭК России в качестве органа по аттестации объектов информатизации, а так же является лицензиатом ФСТЭК России и ФСБ России в части технической защиты информации.

ООО "РЦИБ" имеет все необходимые лицензии ФСБ России и ФСТЭК России для выполнения работ по технической защите и аттестации объектов информатизации.

С 2012 года одним из основных направлений работы организации является оказание услуг в сфере проведения оценки уязвимости, разработки планов обеспечения транспортной безопасности ОТИ и ТС и их реализации.

Деятельность **ООО "Региональный Центр информационной безопасности"** регламентируется следующими документами:

- **Лицензия ФСБ России на осуществление деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну;**
- **Лицензия ФСБ России на право осуществления мероприятий и оказания услуг в области защиты государственной тайны;**
- **Свидетельства Росжелдора и Росавтодора Минтранса об аккредитации на проведение оценки уязвимости ОТИ и ТС;**
- **Приказы ФСТ России об установлении тарифа на выполнение работ при проведении оценки уязвимости ОТИ и ТС;**
- **Лицензия ФСБ России на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств;**
- **Лицензия ФСБ России на предоставление услуг в области шифрования информации;**
- **Лицензия ФСТЭК России на право осуществления мероприятий и оказания услуг в области защиты государственной тайны (в части технической защиты информации);**
- **Лицензия ФСТЭК России на право проведения работ, связанных с созданием средств защиты информации;**
- **Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации.**

В нашем штате состоят квалифицированные сотрудники, прошедшие обучение в Российской академии путей сообщения (г.Москва) по программе оценка уязвимости ОТИ и ТС в сфере железнодорожного транспорта, подразделениях ФСТЭК России, а также проходившие службу в органах ФСБ России, МО России по направлению защиты информации, в т.ч. и сведений, составляющих государственную тайну.

Услуги в области транспортной безопасности (ТБ)

1. **Проведение оценки уязвимости объектов транспортной инфраструктуры и транспортных средств**, т.е. определение степени защищенности объектов транспортной инфраструктуры и транспортных средств в сфере железнодорожного транспорта от потенциальных угроз совершения актов незаконного вмешательства в соответствии с Приказом Минтранса № 515 от 25.10.2011 г.:

- **Изучение технических и технологических характеристик ОТИ или ТС** (включая геологические, гидрологические, климатические и географические особенности дислокации объекта, а также организации их эксплуатации (функционирования) и выявление особенностей влияющих на подготовку, совершение и последствия от АНВ).
- **Определение** границ зоны транспортной безопасности включающей в себя технологический сектор и перевозочный сектор, а также определение зоны свободного доступа в границах объекта транспортной инфраструктуры.
- **Изучение** системы принятых на ОТИ или ТС мер по защите от АНВ в соответствии с Требованиями по обеспечению транспортной безопасности, учитывающих уровни безопасности для различных категорий ОТИ и ТС утвержденных Приказом Минтранса № 43 от 8.02.2011 г.
- **Определение мер**, которые необходимо дополнительно включить в систему принятых мер по защите от АНВ.
- **Изучение** способов реализации потенциальных угроз совершения АНВ в деятельность ОТИ и ТС.
- **Определение** вероятных сценариев совершения АНВ для данного ОТИ или ТС.
- **Выявление** наиболее вероятных целей и способов реализации потенциальных угроз на конкретном ОТИ или ТС.
- **Обследование** периметра, территории ОТИ и прилегающих территорий на предмет выявления путей подъезда, подхода потенциальных нарушителей к ОТИ или ТС и к их КЭ (критические элементы), возможных мест укрытия нарушителей, ближайших точек доступа к коммуникациям ОТИ с целью подготовки совершения АНВ.
- **Определение** конкретных мест установки технических средств обеспечения транспортной безопасности и их общая характеристика (стационарные досмотровые комплексы, передвижные досмотровые комплексы, система видеонаблюдения, комплексы мобильной аппаратуры для обследования предметов, системы подавления радиотелевизионных устройств, технические средства охраны периметра и другие технические средства обеспечения транспортной безопасности).
- **Определение мест** расположения и оборудования инженерно-техническими средствами транспортной безопасности КПП, Пунктов (постов) транспортной безопасности.
- **Определение мест** расположения инженерных сооружений обеспечения транспортной безопасности.
- **Определение** порядка защиты информации и хранения баз данных с технических систем транспортной безопасности на ОТИ.
- **Анализ** осуществления на ОТИ пропускного и внутриобъектового режимов подразделениями по обеспечению транспортной безопасности в соответствии с Требованиями по обеспечению транспортной безопасности (приказ Минтранса России № 43 от 08.02.2011 г.) применяя математическое моделирование различных типов потенциального нарушителя. При выявлении несоответствий требованиям, субъекту транспортной инфраструктуры дается описание необходимых мер по обеспечению транспортной безопасности подразделениями ТБ при осуществлении пропускного и внутриобъектового режимов на ОТИ.

2. **Участие в разработке плана** обеспечения транспортной безопасности ОТИ или ТС:

- **Рекомендации** субъекту транспортной инфраструктуры в отношении мер, которые необходимо включить в систему мер по обеспечению ТБ ОТИ и реализовать в срок, не превышающий 6 месяцев с момента утверждения результатов оценки уязвимости в соответствии с п.5.8 Приказа Минтранса России № 43 от 08.02.2011 г.

3. Реализация плана по обеспечению транспортной безопасности ОТИ или ТС:

- **Проведение проектно-изыскательных работ (ПИР)** по внедрению интегрированной комплексной системы безопасности (ИКСБ) на объекте транспортной инфраструктуры и выполнение строительно-монтажных работ (СМР) по установке технических средств обеспечения транспортной безопасности, инженерных сооружений обеспечения транспортной безопасности и оборудование инженерно-техническими средствами и системами (ИТС) транспортной безопасности КПП, Пунктов (постов) транспортной безопасности и иных элементов ОТИ по согласованию с 11-м центром ФСБ России.
- **Аудит** функционирования существующих инженерно-технических систем (ИТС) обеспечения транспортной безопасности, включая порядок передачи данных с таких систем, уполномоченным подразделениям федерального органа исполнительной власти, осуществляющего функции по выработке государственной политики и нормативно-правовому регулированию в сфере внутренних дел, в области обеспечения безопасности РФ, а также территориальное управление федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере транспорта или составление технического задания на их создание.
- **Установка ИТС** для передачи данных в реальном режиме времени.
- **Проведение компьютерно-технической экспертизы (КТЭ)** с целью определения возможности хранения базы данных обеспечения транспортной безопасности на срок до 30 суток.
- **Установка периметрового ограждения** зоны транспортной безопасности с противотаранными устройствами, противоподкопами, противоперелазами, установка технических средств охраны периметра.
- **Установка системы видеонаблюдения** с возможностью круглосуточного видеомониторинга, видеообнаружения, видеораспознавания событий в произвольном месте и в произвольное время.
- **Установка системы считывания** электронных пропусков с применением биометрических пропусков.
- **Разработка маршрутов выдвижения** для групп быстрого реагирования подразделений транспортной безопасности к различным участкам зоны транспортной безопасности с учетом развития автодорожной инфраструктуры.

4. Профессиональные консалтинговые услуги по всем вышеуказанным вопросам, а также в области безопасности в целом.

Услуги в области информационной безопасности (ИБ)

1. **Аттестация** объектов информатизации по требованиям безопасности информации, составляющей *государственную тайну*;

2. **Аттестация** объектов информатизации по требованиям безопасности *конфиденциальной* информации;

3. **Выявление электронных устройств**, предназначенных для негласного получения информации, в помещениях и технических средствах;

4. **Разработка и внедрение систем защиты персональных данных**, обрабатываемых в информационных системах в соответствии с требованиями **Федерального закона № 152-ФЗ "О персональных данных"**:

- Аудит и классификация существующих информационных систем обработки персональных данных;
- Построение актуальных моделей угроз информационной безопасности персональных данных (в соответствии с требованиями ФСТЭК России, ФСБ России);
- Разработка технического задания и проектирование системы информационной безопасности для информационных систем обработки персональных данных;
- Разработка необходимых организационно-распорядительных документов (уведомления, концепции, положения, инструкции и пр.);
- Внедрение технических средств защиты персональных данных;
- **Аттестация** системы на соответствие требованиям по защите персональных данных;
- Консультации и повышение квалификации персонала по вопросам организации и эксплуатации систем защиты персональных данных.

5. **Аудит информационной безопасности:**

- Аудит существующих информационных систем управления информационной безопасностью на соответствие требованиям законодательства в области ИБ;
- Аудит безопасности web-приложений;
- Разработка мер по устранению недостатков, выявленных в ходе аудита.

6. Услуги по подготовке, оперативному и техническому **сопровождению конфиденциальных переговоров:**

- Обследование места проведения переговоров для выявления потенциальных каналов утечки информации;
- Сканирование радиоэфира во время проведения переговоров для выявления технических средств съема информации;
- Подготовка рекомендаций и консультации по проведению конфиденциальных переговоров для обеспечения безопасности;
- Оборудование места проведения переговоров техническими средствами для фиксации результатов или защиты;
- **Проектирование и внедрение систем защиты помещений для проведения конфиденциальных переговоров.**

7. **Разработка и сопровождение web-сайтов в защищенном исполнении:**

- Разработка требований безопасности сайта;
- Создание сайта с соблюдением требований безопасности;
- Тестирование системы безопасности сайта;
- Сопровождение информационного наполнения сайта, дизайна.

8. Разработка и внедрение систем управления информационной безопасностью (СУИБ):

- Аудит существующих информационных систем или составление технического задания на их создание;
- Классификация и инвентаризация информационных ресурсов;
- Описание модели возможных угроз;
- Разработка базовых требований по защите;
- Внедрение СУИБ;
- Тестирование и устранение недостатков;
- Сопровождение.

9. Расследование инцидентов информационной безопасности:

- Анализ инцидента;
- Выявление каналов утечки, причин повреждения, блокирования информации, обнаружение инсайдеров и пр.;
- Разработка рекомендаций по нейтрализации последствий инцидента и его недопущению в будущем;
- Проведение компьютерно-технической экспертизы (КТЭ).

10. Осуществление мероприятий и оказание услуг в области защиты государственной тайны:

- Подготовительные мероприятия для получения Лицензии ФСБ России на осуществление деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну;
- Ведение секретного делопроизводства в соответствии с Инструкцией по обеспечению режима секретности в Российской Федерации, утвержденной постановлением Правительства Российской Федерации от 05.01.2004 г. № 3-1.;
- Проведение специальных экспертиз по поручению Управления ФСБ России по Воронежской области для получения Лицензии ФСБ России на осуществление деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

11. Профессиональные консалтинговые услуги по всем вышеуказанным вопросам, а также в области безопасности в целом.

ООО "Региональный Центр информационной безопасности"

394028, г. Воронеж, ул. Ильюшина, д.3 "е", офис № 22.

Тел./факс: (473) 257-36-13, (473) 233-09-51

ИНН 3663072220, КПП 366301001, ОГРН 1083668019456

Р/счет № 40702810313000014542 в

Центрально-Черноземный банк Сбербанка России г. Воронеж

394006, г. Воронеж, ул. 9 Января, д.28 (банк);

394006, г. Воронеж, ул. Платонова, д.8 (Дополнительный офис № 0175)

БИК 042007681

К/счет № 30101810600000000681

(473) 257-36-13

(473) 233-09-51

www.rcibvrn.ru

394028, г. Воронеж,

ул. Ильюшина, д.3 "е",

офис № 22

ОГРН 1083668019456

ИНН 3663072220

КПП 366301001