



## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

# АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

services.softline.ru  
8 (800) 232 00 23

**АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ (ОИ)** – комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» – подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

### АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ (ОИ)

#### Добровольная

Проводится по инициативе владельца информации или ОИ и может служить для подтверждения соответствия ОИ требованиям безопасности информации, установленным нормативными правовыми актами РФ, а также иными документами (в том числе национальными или международными отраслевыми стандартами и т.д).

#### Обязательная

Проводится для ОИ в случаях, установленных федеральными законами, актами Президента и Правительства РФ, нормативными правовыми актами уполномоченных федеральных органов исполнительной власти. Сегодня аттестация носит обязательный характер для ОИ, предназначенных для обработки сведений, составляющих государственную тайну, а также для государственных и муниципальных информационных систем.

### Кому нужна аттестация ОИ?

- ▶ Организациям и предприятиям, обрабатывающим информацию, доступ к которой ограничен в соответствии с законодательством Российской Федерации.
- ▶ Предприятиям и организациям, которым необходима независимая оценка соответствия объекта информатизации требованиям нормативных документов по безопасности информации.

### КЕМ МОЖЕТ ПРОВОДИТЬСЯ АТТЕСТАЦИЯ?

#### Добровольная

Организациями, имеющими лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

#### Обязательная

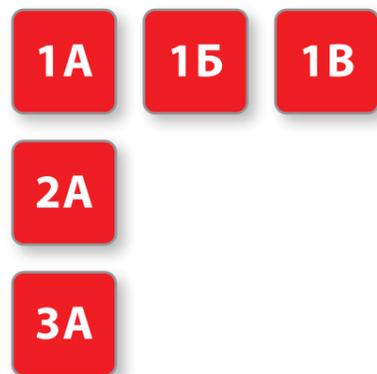
**Проводится для информатизации**, предназначенных для обработки сведений, составляющую государственную тайну, проводится организациями, имеющими аттестат аккредитации органа по аттестации и соответствующие лицензии ФСТЭК России на осуществление мероприятий и оказание услуг в области защиты государственной тайны (в части технической защиты информации).

**Аттестация объектов информатизации**, предназначенных для обработки сведений конфиденциального характера, проводится организациями, имеющими лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

# Порядок проведения аттестации объектов информатизации



По требованиям НМД по ЗГТ:



Категории:  
 1-я категория – особой важности.  
 2-я категория – совершенно секретно.  
 3-я категория – секретно.

По требованиям:



Категории:  
 ПДН.  
 Служебная тайна.  
 Коммерческая тайна.  
 Иная конфиденциальная информация.



## Состав аттестационных испытаний ОИ:

- ▶ Анализ и оценка исходных данных и документации по защите информации на объекте информатизации.
- ▶ Проверка соответствия представленных исходных данных реальным условиям размещения и эксплуатации объекта информатизации.
- ▶ Изучение (проверка) технологического процесса обработки и хранения информации, анализ информационных потоков и т.п.
- ▶ Проверка состояния организации работ и выполнения организационно-технических требований по защите информации:
  - Оценка полноты и уровня разработки организационно-распорядительной, проектной и эксплуатационной документации.
  - Оценка правильности классификации и категорирования объекта информатизации.
  - Оценка уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации.
- ▶ Испытания отдельных технических и программных средств, средств и систем защиты, инженерного оборудования на соответствие требованиям по безопасности информации.
- ▶ Комплексные испытания объекта информатизации на соответствие требованиям по безопасности информации.
- ▶ Подготовка отчетной документации.

## Методы проверок и испытаний, используемые при аттестации ОИ:

- Экспертно-документальный метод.
- Измерения и оценка степени опасности технических каналов утечки информации и эффективности защиты информации от утечки по ним.
- Проверка функций (комплекса функций) защиты информации от несанкционированного доступа.
- Попытки «взлома» систем защиты информации.

## СОСТАВ АТТЕСТАЦИОННЫХ ДОКУМЕНТОВ:

- ▶ Акт обследования ОИ.
- ▶ Программа и методики аттестационных испытаний (содержит перечень работ, их продолжительность, методики испытаний, сведения о количественном и профессиональном составе аттестационной комиссии, используемых технических и программных средствах и измерительной аппаратуре).
- ▶ Протоколы контроля защищенности информации (содержат информацию о проведении измерений, испытаний, расчетов, результаты и выводы о соответствии полученных результатов нормированным значениям).
- ▶ Протоколы аттестационных испытаний содержат информацию и выводы о соответствии полученных результатов требованиям безопасности информации.
- ▶ Заключение по результатам аттестационных испытаний (содержит краткую оценку соответствия системы защиты ОИ требованиям безопасности информации, рекомендации по контролю за функционированием ОИ, вывод о возможности выдачи аттестата соответствия или рекомендации по устранению выявленных несоответствий).
- ▶ Аттестат соответствия ОИ требованиям безопасности информации содержит информацию об аттестованном объекте информатизации (выдается на срок не более 3 (трех) лет).

## Аттестационный центр Softline выполняет следующие работы:

1

Контроль защищенности информации, составляющей государственную тайну, аттестация на соответствие требованиям по защите информации:

- систем связи;
- систем приема, обработки и передачи данных;
- систем отображения и размножения;
- технических средств, не обрабатывающих информацию, составляющую государственную тайну;
- помещений, предназначенных для ведения секретных переговоров.

2

Проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации

3

Проектирование объектов в защищенном исполнении:

- систем связи;
- систем приема, обработки и передачи данных;
- систем отображения и размножения.

4

Реализация, установка, монтаж, наладка, сервисное обслуживание:

- технических средств защиты информации;
- защищенных программных средств обработки информации;
- программных средств контроля защищенности информации.

На базе аттестационного центра в Softline создан орган по аттестации объектов информатизации, который является составной частью организационной структуры системы сертификации средств защиты информации по требованиям безопасности информации №РОСС RU.0001.01БИ00.

Орган по аттестации в своей деятельности руководствуется законодательством Российской Федерации, национальными стандартами, нормативными и методическими документами ФСТЭК России.

Деятельность органа по аттестации осуществляется на основе лицензии ФСТЭК России (рег. № 3112/1 от 26 декабря 2013 г.) и Аттестата аккредитации, дающих ему право проведения аттестации объектов информатизации.

## ОБУЧЕНИЕ ПО НАПРАВЛЕНИЯМ БЕЗОПАСНОСТИ



Учебный центр Softline имеет статус Learning Partner Specialized – Borderless Networks.



- Проектирование безопасности средствами Check Point R77.
- Обеспечение безопасности средствами Check Point R77.



Authorised Education Delivery Partner

- ▶ Symantec Security Information Manager 4.7: Administration.
- ▶ Symantec Endpoint Protection 12.1: Administration.



- ▶ Kaspersky Endpoint Security and Management. Базовый курс.
- ▶ Kaspersky Endpoint Security and Management. Масштабирование.
- ▶ Kaspersky Endpoint Security and Management. Шифрование.
- ▶ Kaspersky Endpoint Security and Management. Управление системами.
- ▶ Kaspersky Endpoint Security and Management. Управление мобильными устройствами.

Эксплуатация и техническое сопровождение средств криптографической защиты информации с использованием продуктов компании ООО «КРИПТО-ПРО».

<http://edu.softline.ru/>



## ТЕХНИЧЕСКАЯ ПОДДЕРЖКА И АУТСОРСИНГ

- ▶ Полное покрытие всех часовых поясов, режим работы 24x7.
- ▶ Обслуживание всей инфраструктуры заказчика или ее части.
- ▶ Единая служба техподдержки в режиме online по всей России.
- ▶ Поддержка через интернет, по круглосуточному телефону или e-mail, на площадке заказчика.
- ▶ Решение задач на стыке производителей.
- ▶ Аутстаффинг.

### ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ПОЗВОЛИТ ВАМ:

- ▶ Снизить стоимость владения IT-инфраструктурой.
- ▶ Получить максимальную отдачу от инвестиций в IT.
- ▶ Обеспечить бесперебойную работу всех систем и IT-сервисов.
- ▶ Минимизировать время простоя систем из-за технических неполадок.
- ▶ Оперативно устранить возникающие критические сбои.
- ▶ Снизить риски возникновения неисправностей.
- ▶ Повысить производительность систем.
- ▶ Отладить и проверить решения на тестовом стенде.

### IT-АУТСОРСИНГ ПОЗВОЛИТ ВАМ:

- ▶ Сосредоточиться на основном бизнесе.
- ▶ Сократить затраты на обслуживание IT.
- ▶ Добиться роста производительности и стабильности IT-систем.
- ▶ Оперативно восстановить IT-системы после сбоев.
- ▶ Иметь систему контроля качества оказываемых услуг.
- ▶ Работать с высококвалифицированными специалистами.
- ▶ Получить прозрачную систему отчетности.
- ▶ Повысить качество обслуживания и минимизировать простои.
- ▶ Иметь единую точку входа для решения всех задач, связанных с обслуживанием IT.
- ▶ Обеспечить быструю реакцию на изменение бизнес-стратегии компании.

<http://services.softline.ru/support>

## 1 ЭКСПЕРТНЫЕ УСЛУГИ

- Аудит информационной безопасности**
  - Комплексный аудит ИБ
  - Экспресс-аудит информационной безопасности
  - Технический аудит инфраструктуры
  - Аудит безопасности критичных процессов и сервисов
  - Построение моделей угроз и нарушителей, анализ рисков ИБ
- Анализ защищенности приложений и инфраструктуры**
  - Инструментальное сканирование
  - Тестирование на проникновение
  - Анализ защищенности
  - Деобфускация, декомпиляция и анализ кода
  - Написание рекомендаций по устранению уязвимостей
- Тонкая настройка средств защиты информации**
  - Web Application Firewall
  - Security Information and Event Management
  - Data Loss Prevention
- Комплексное сравнение решений**
- Защита информации от утечки по техническим каналам**
  - Защита информации от утечки по акустическим / акустоэлектрическим / виброакустическим каналам
  - Защита информации от утечки по ПЭМИН / оптическим / радиоканалам / электрическим каналам

## 2 УПРАВЛЕНИЕ ИБ

- Планирование и разработка стратегии ИБ**
  - Разработка политик и регламентов по ИБ
  - Построение комплексных систем ИБ
- Построение процесса управления рисками ИБ**
  - Внедрение систем управления рисками и контроля соответствия требованиям (GRC)
  - Разработка процесса управления рисками ИБ
- Построение процесса мониторинга, реагирования и управления инцидентами ИБ**
  - Внедрение специализированных систем по расследованию компьютерных инцидентов (Computer Forensic)
  - Поиск в неструктурированных данных
  - Внедрение систем мониторинга и корреляция событий ИБ (SIEM)
- Построение процесса внутреннего аудита ИБ**
  - Планирование и организация внутреннего аудита
  - Внедрение систем автоматизированного аудита ИБ
- Построение процесса безопасной разработки приложений**
  - Анализ исходного кода приложения "вручную"
  - Выявление причин появления в коде приложения уязвимостей
  - Внедрение процесса безопасной разработки приложений
  - Внедрение специализированных систем контроля безопасности исходного кода приложений
- Построение процесса управления уязвимостями**
  - Внедрение систем управления уязвимостями (Vulnerability Management)
  - Консультации и тонкая настройка средств инструментального сканирования
  - Консультации по применению средств автоматизированного анализа кода

## 3 ВНЕДРЕНИЕ МЕР ОБЕСПЕЧЕНИЯ ИБ

- Безопасность серверов и рабочих станций**
  - Контроль целостности серверов
  - Антивирусная защита
  - Шифрование жестких дисков и баз данных
- Контентная фильтрация**
  - Защита корпоративной почты от нежелательных сообщений
  - Обеспечение безопасности доступа в Интернет
- Защита от утечек конфиденциальной информации**
  - Внедрение систем защиты от утечек конфиденциальной информации (DLP)
- Управление правами доступа к информации**
  - Внедрение систем управления правами доступа к конфиденциальной информации (IRM)
- Безопасность электронной почты**
  - Защита с помощью ЭЦП и шифрования
- Безопасность систем ЭДО**
  - Внедрение юридически значимых электронных подписей документов
  - Технический анализ систем ЭДО
  - Повышение защищенности систем ЭДО против атак
- Безопасность критичных и фиксированных систем, АСУТП**
  - Внедрение системы контроля целостности и приложений (замена антивирусов)
  - Внедрение систем контроля действий привилегированных пользователей над целевыми системами
  - Внедрение системы IDS
  - Внедрение систем удаленного безопасного доступа
  - Внедрение системы защиты передачи нежелательной информации из/в подсистемы АСУТП в общую информационную сеть предприятия
  - Внедрение системы дополнительной аутентификации
  - Внедрение системы предотвращения сетевых штормов
- Безопасность удаленного доступа к корпоративным ресурсам**
  - Удаленный доступ пользователей с использованием технологии VPN через SSL
  - Контроль политик устройства, с которого происходит доступ
  - Усиленная аутентификация для предотвращения повторного использования пароля - токены, SMS
- Безопасность сетей и межсетевое взаимодействие**
  - Построение систем VPN, IPS, контроль используемых в сети приложений, построение систем менеджмента конфигурационных файлов сетевых устройств
  - Контроль используемых в сети приложений
  - Построение систем менеджмента конфигурационных файлов сетевых устройств
- Идентификация, аутентификация и управления правами доступа**
  - Решения по управлению учетными записями (IdM)
  - Решения по управлению удостоверениями и доступом (IAG)
  - Усиленная аутентификация в информационных системах
  - Системы организации единой точки входа (SSO)
- Криптографическая защита информации**
  - Удостоверяющие центры PKI
  - Интеграция ЭЦП в инфраструктуру предприятия
- Безопасность использования мобильных устройств**
- Безопасность корпоративных бизнес-приложений**
- Безопасность WEB-ресурсов**
- Контроль носителей информации**
- Безопасность файловых серверов**
- Защита структурной документации (САПР)**
- Аудит Active Directory**
- Безопасность виртуальных сред**
- Защищенный обмен данными**

## 4 ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

- Персональные данные**
  - Разработка модели угроз, модели нарушителя, классификация ИСПДн
  - Проектирование и внедрение систем защиты ПДн
  - Разработка или модернизация организационно-распорядительной документации по обработке ПДн
  - Аттестация ИСПДн по требованиям безопасности информации
- Коммерческая тайна**
  - Категорирование конфиденциальной информации
  - Введение режима коммерческой тайны (разработка документации в соответствии с 98-ФЗ)
- Закон об электронной подписи**
  - Обеспечение юридической значимости электронного документооборота (в соответствии с 63-ФЗ «Об электронной подписи»)
- Стандарт СТО БР ИББС**
  - Оценка соответствия требованиям СТО БР ИББС (аудит)
  - Внедрение СОИБ по требованиям СТО БР ИББС
  - Выполнение требований по защите персональных данных в соответствии с СТО БР ИББС
  - Поддержка соответствия СТО БР ИББС
- Закон о НПС и Положение 382-П**
  - Проведение аудита выполнения требований
  - Разработка рекомендаций по выполнению требований
  - Разработка или актуализация комплекта ОРД
  - Проектирование системы защиты и внедрение необходимых средств защиты информации
  - Подготовка к аттестации
  - Контроль защищенности и аттестация по требованиям безопасности информации
  - Проведение периодического контроля эффективности внедренных на объекте мер и средств защиты информации
- PCI DSS**
  - Аудит на соответствие требованиям PCI DSS / PA DSS
  - Внедрение PCI DSS
  - Поддержка соответствия требованиям PCI DSS
  - ASV сканирование
  - Тестирование на проникновение
- Системы менеджмента ИБ**
  - Проектирование и внедрение систем управления в соответствии с международными стандартами ISO 27001, BS 25999
  - Проектирование и запуск процессов
  - Оценка соответствия требованиям стандартов
  - Аутсорсинг процессов управления и обеспечения систем менеджмента
  - Поддержка систем менеджмента

## 5 СЕРВИСНЫЕ УСЛУГИ

- Техническая поддержка**
  - Консультации по вопросам установки, настройки и администрирования
  - Решение технических проблем с учетом моделирования ИТ-структуры заказчика на виртуальном стенде
  - Сессии удаленного подключения для оказания поддержки
  - Документирование ИТ-структуры
  - Проведение аудита
  - Выезд на площадку заказчика для решения в случае невозможности удаленного решения проблемы
  - Профилактические выезды
  - Удаленный периодический мониторинг с выдачей рекомендаций
  - Осуществление эскалации запросов производителю (при необходимости)
  - Предоставление статистики по поступившим инцидентам за отчетный период
- Обучение специалистов в области ИБ**
  - Обучение на курсах в авторизованном УЦ Софтлайн
  - Обучение в рамках проекта (передача знаний по настроенной установке обслуживающему персоналу заказчика)
- Аутсорсинг и аутстаффинг**
  - Аутсорсинг - обслуживание сервиса заказчика, проактивная техподдержка
  - Аутстаффинг - аутсорсинг со 100%-ым присутствием инженера исполнителя на площадке заказчика
- Консультационное сопровождение**
- Юридическая поддержка в области ИБ**
  - Юридическая помощь при прохождении проверок регуляторов и правовая помощь в сфере защиты персональных данных, коммерческой тайны и других видов конфиденциальной информации

## НАШИ ЛИЦЕНЗИИ И КЛИЕНТЫ

### Лицензия ФСТЭК России

на деятельность по технической защите конфиденциальной информации (с правом проведения аттестации по требованиям безопасности).

### Лицензия ФСТЭК России

на деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

### Лицензия ФСБ России

на осуществление разработки, производства и распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, технического обслуживания шифровальных (криптографических) средств.

### Лицензия ФСБ России

на выполнение работ, связанных с использованием сведений, составляющих государственную тайну.

### Лицензия ФСТЭК России

на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации).

### Лицензия ФСТЭК России

на проведение работ, связанных с созданием средств защиты информации.



**Москва**  
+7 (495) 232 00 23  
info@softline.ru

**Санкт-Петербург**  
+7 (812) 777 44 46  
info.spb@softline.ru

**Архангельск**  
+7 (8182) 635 922  
info.arh@softline.ru

**Белгород**  
+7 (4722) 585 255  
Info.BGD@softline.ru

**Владивосток**  
+7 (423) 260 00 10  
info.vlk@softline.ru

**Волгоград**  
+7 (8442) 900 202  
info.vgd@softline.ru

**Воронеж**  
+7 (473) 250 20 23  
info.vrn@softline.ru

**Екатеринбург**  
+7 (343) 278 53 35  
info.ekt@softline.ru

**Ижевск**  
+7 (3412) 936 651  
Info.izh@softline.ru

**Иркутск**  
+7 (3952) 500 632  
info.irk@softline.ru

**Казань**  
+7 (843) 526 552  
info.kzn@softline.ru

**Калининград**  
+7 (4012) 777 650  
info.kld@softline.ru

**Краснодар**  
+7 (861) 251 65 14  
info.krd@softline.ru

**Красноярск**  
+7 (391) 252 59 91  
info.krs@softline.ru

**Мурманск**  
+7 (8152) 688 846  
Info.MRK@softline.ru

**Нижний Новгород**  
+7 (831) 220 00 36  
info.nnov@softline.ru

**Новосибирск**  
+7 (383) 347 57 47  
info.nsk@softline.ru

**Омск**  
+7 (3812) 433 190  
info.oms@softline.ru

**Оренбург**  
+7 (3532) 452 010  
info.orb@softline.ru

**Пермь**  
+7 (342) 214 42 01  
info.prm@softline.ru

**Ростов-на-Дону**  
+7 (863) 237 99 49  
info.rd@softline.ru

**Самара**  
+7 (846) 270 04 80  
info.sam@softline.ru

**Саратов**  
+7 (8452) 247 732  
info.srt@softline.ru

**Сургут**  
+7 (3462) 223 500  
info.sgt@softline.ru

**Томск**  
+7 (3822) 900 081  
info.tmk@softline.ru

**Тюмень**  
+7 (3452) 696 063  
info.tmn@softline.ru

**Уфа**  
+7 (347) 292 44 50  
info.ufa@softline.ru

**Хабаровск**  
+7 (4212) 747 724  
info.khb@softline.ru

**Челябинск**  
+7 (351) 247 28 36  
info.chk@softline.ru

**Ярославль**  
+7 (4852) 588 809  
info.yar@softline.ru

