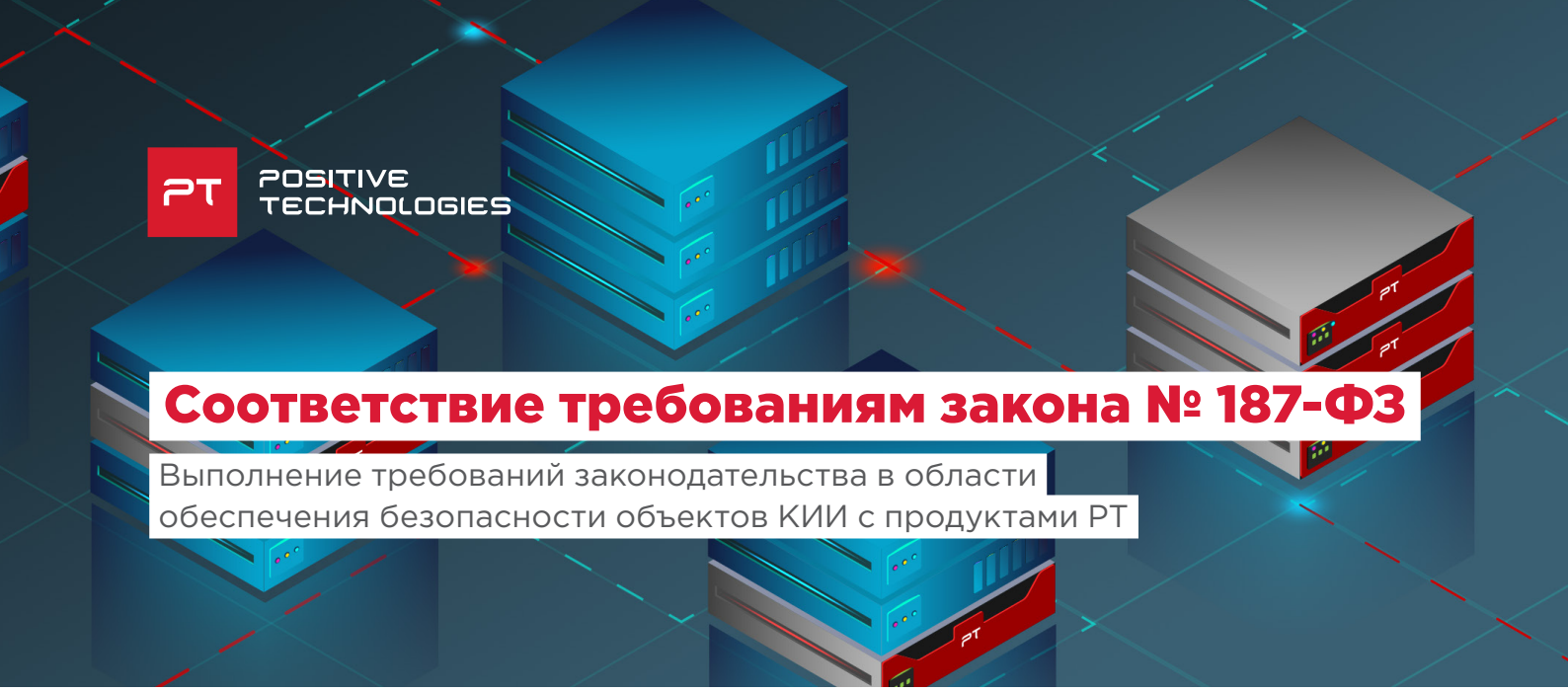

Соответствие требованиям закона № 187-ФЗ

Выполнение требований законодательства в области обеспечения безопасности объектов КИИ с продуктами PT

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	**Ст.10 п. 2** Одна из основных задач системы безопасности значимого объекта КИИ – непрерывное взаимодействие с ГосСОПКА	▪ Система взаимодействия с ГосСОПКА ПТ Ведомственный центр ▪ Комплексное решение для небольших инфраструктур PT Platform 187
	Ст.9 п. 2 Субъекты КИИ обязаны незамедлительно информировать об инцидентах ФСБ России	▪ Система взаимодействия с ГосСОПКА ПТ Ведомственный центр ▪ Комплексное решение для небольших инфраструктур PT Platform 187
Приказ ФСБ России от 24.07.2018 №367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации...»	Перечень информации, представляемой в ГосСОПКА	▪ Система взаимодействия с ГосСОПКА ПТ Ведомственный центр ▪ Комплексное решение для небольших инфраструктур PT Platform 187
Приказ ФСБ России от 24.07.2018 №368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации...»	**прил. 1 п. 6** Уведомления и запросы направляются посредством использования технической инфраструктуры НКЦКИ при наличии подключения к ней	▪ Система взаимодействия с ГосСОПКА ПТ Ведомственный центр
Приказ ФСТЭК России от 25.12.2017 №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»	**п. 6** Системы безопасности должны обеспечивать непрерывное взаимодействие с ГосСОПКА	▪ Система взаимодействия с ГосСОПКА ПТ Ведомственный центр
	п. 10 Структурное подразделение по безопасности, специалисты по безопасности должны выявлять уязвимости в значимых объектах КИИ	▪ Система контроля защищенности MaxPatrol 8 ▪ Система анализа исходного кода PT Application Inspector
	п. 18 В случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом КИИ для обеспечения безопасности значимых объектов КИИ должны применяться только сертифицированные ФСТЭК России средства защиты	▪ MaxPatrol 8, MaxPatrol SIEM, PT ISIM ,PT Network Attack Discovery, PT Application Firewall, PT Application Inspector имеют сертификаты. ▪ PT MultiScanner находится на сертификации. ▪ «ПТ Ведомственный центр» в сертификации не нуждается.

Приказ ФСТЭК России от 25.12.2017 №239

«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры...»

Номер п/п	Меры по обеспечению безопасности информации	Классы защищенности			MaxPatrol 8	MaxPatrol SIEM	PT Network Attack Discovery	PT MultiScanner	PT ISIM	PT Application Firewall	ПТ Ведомственный центр
		3	2	1	Система контроля защищенности и соответствия стандартам	Система выявления инцидентов	Система глубокого анализа трафика	Система выявления вредоносного ПО	Система обнаружения кибератак на АСУ ТП	Система защиты от веб-атак	Система взаимодействия с ГосСОПКА
I. Идентификация и аутентификация (ИАФ)											
ИАФ.2	Идентификация и аутентификация устройств	+	+	+	-	-	-	-	+	-	-
II. Управление доступом (УПД)											
УПД.2	Реализация политик управления доступом	+	+	+	-	-	-	-	-	+	-
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+	-	-	-	-	-	+	-
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+	-	-	-	-	-	+	-
УПД.9	Ограничение числа параллельных сеансов доступа			+	-	-	-	-	-	+	-
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	+	+	-	-	-	-	-	+	-
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	+	+	-	-	-	-	-	+	-
УПД.12	Управление атрибутами безопасности				-	-	-	-	-	+	-
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+	-	-	-	-	-	+	-
V. Аудит безопасности (АУД)											
АУД.1	Инвентаризация информационных ресурсов	+	+	+	+	+	-	-	+	-	-
АУД.2	Анализ уязвимостей и их устранение	+	+	+	+	+	-	-	-	+	-
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+	-	-	-	-	-	+	-

Номер п/п	Меры по обеспечению безопасности информации	Классы защищенности			MaxPatrol 8	MaxPatrol SIEM	PT Network Attack Discovery	PT MultiScanner	PT ISIM	PT Application Firewall	ПТ Ведомственный центр
		3	2	1	Система контроля защищенности и соответствия стандартам	Система выявления инцидентов	Система глубокого анализа трафика	Система выявления вредоносного ПО	Система обнаружения кибератак на АСУ ТП	Система защиты от веб-атак	Система взаимодействия с ГосСОПКА
АУД.4	Регистрация событий безопасности	+	+	+	-	+	-	-	+	+	-
АУД.5	Контроль и анализ сетевого трафика	-	-	+	-	+	+	-	+	-	-
АУД.6	Защита информации о событиях безопасности	+	+	+	-	+	-	-	-	+	-
АУД.7	Мониторинг безопасности	+	+	+	+	+	-	-	+	+	-
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+	-	+	-	-	-	-	-
АУД.9	Анализ действий пользователей			+	-	-	-	-	-	+	-
АУД.10	Проведение внутренних аудитов	+	+	+	+	-	-	-	-	-	-
АУД.11	Проведение внешних аудитов	-	-	+	+	-	-	-	-	+	-
VI. Антивирусная защита (АВЗ)											
АВЗ.1	Реализация антивирусной защиты	+	+	+	-	-	-	-	-	+	-
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+	+	+	-	-	-	+	-	+	-
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	-	-	-	+	-	+	-
АВЗ.5	Использование средств антивирусной защиты различных производителей	-	-	+	-	-	-	+	-	+	-
VII. Предотвращение вторжений (компьютерных атак) (СОВ)											
СОВ.1	Обнаружение и предотвращение компьютерных атак	-	+	+	-	-	+	-	+	-	-
СОВ.2	Обновление базы решающих правил	-	+	+	-	-	+	-	+	-	-
VIII. Обеспечение целостности (ОЦЛ)											
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	-	-	+	-	-	-	-	-	+	-

Номер п/п	Меры по обеспечению безопасности информации	Классы защищенности			MaxPatrol 8	MaxPatrol SIEM	PT Network Attack Discovery	PT MultiScanner	PT ISIM	PT Application Firewall	ПТ Ведомственный центр
		3	2	1	Система контроля защищенности и соответствия стандартам	Система выявления инцидентов	Система глубокого анализа трафика	Система выявления вредоносного ПО	Система обнаружения кибератак на АСУ ТП	Система защиты от веб-атак	Система взаимодействия с ГосСОПКА
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	-	+	+	-	-	-	-	-	+	-
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	-	+	+	-	-	-	-	-	+	-
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)											
ЗИС.6	Управление сетевыми потоками	-	-	-	-	-	-	-	-	+	-
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения («песочница»)	-	-	-	-	-	-	+	-	-	-
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами	-	-	-	-	-	-	-	-	+	-
ЗИС.26	Подтверждение происхождения источника информации	-	-	-	-	-	-	-	-	+	-
ЗИС.33	Исключение доступа через общие ресурсы	-	-	+	-	-	-	-	-	+	-
ЗИС.34	Защита от угроз отказа в обслуживании (DoS-, DDoS-атак)	+	+	+	-	-	-	-	-	+	-
ЗИС.35	Управление сетевыми соединениями	-	+	+	-	-	-	-	-	+	-
XII. Реагирование на компьютерные инциденты (ИНЦ)											
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+	-	+	-	-	+	-	-
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+	-	+	-	-	+	-	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+	-	+	-	-	+	-	-

Номер п/п	Меры по обеспечению безопасности информации	Классы защищенности			MaxPatrol 8	MaxPatrol SIEM	PT Network Attack Discovery	PT MultiScanner	PT ISIM	PT Application Firewall	ПТ Ведомственный центр
		3	2	1	Система контроля защищенности и соответствия стандартам	Система выявления инцидентов	Система глубокого анализа трафика	Система выявления вредоносного ПО	Система обнаружения кибератак на АСУ ТП	Система защиты от веб-атак	Система взаимодействия с ГосСОПКА
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+	-	+	-	-	-	-	-
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+	-	+	-	-	+	-	-
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+	+	+	-	+	-	-	-	-	+
XIII. Управление конфигурацией (УКФ)											
УКФ.4	Контроль действий по внесению изменений	-	-	-	-	+	-	-	+	-	-
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)											
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+	+	+	+	+	-	-	-	-	-
XVI. Обеспечение действий в нештатных ситуациях (ДНС)											
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+	+	+	-	+	-	-	-	-	-

О компании

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях (Facebook, ВКонтакте, Twitter), а также в разделе «Новости» на сайте ptsecurity.com.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays