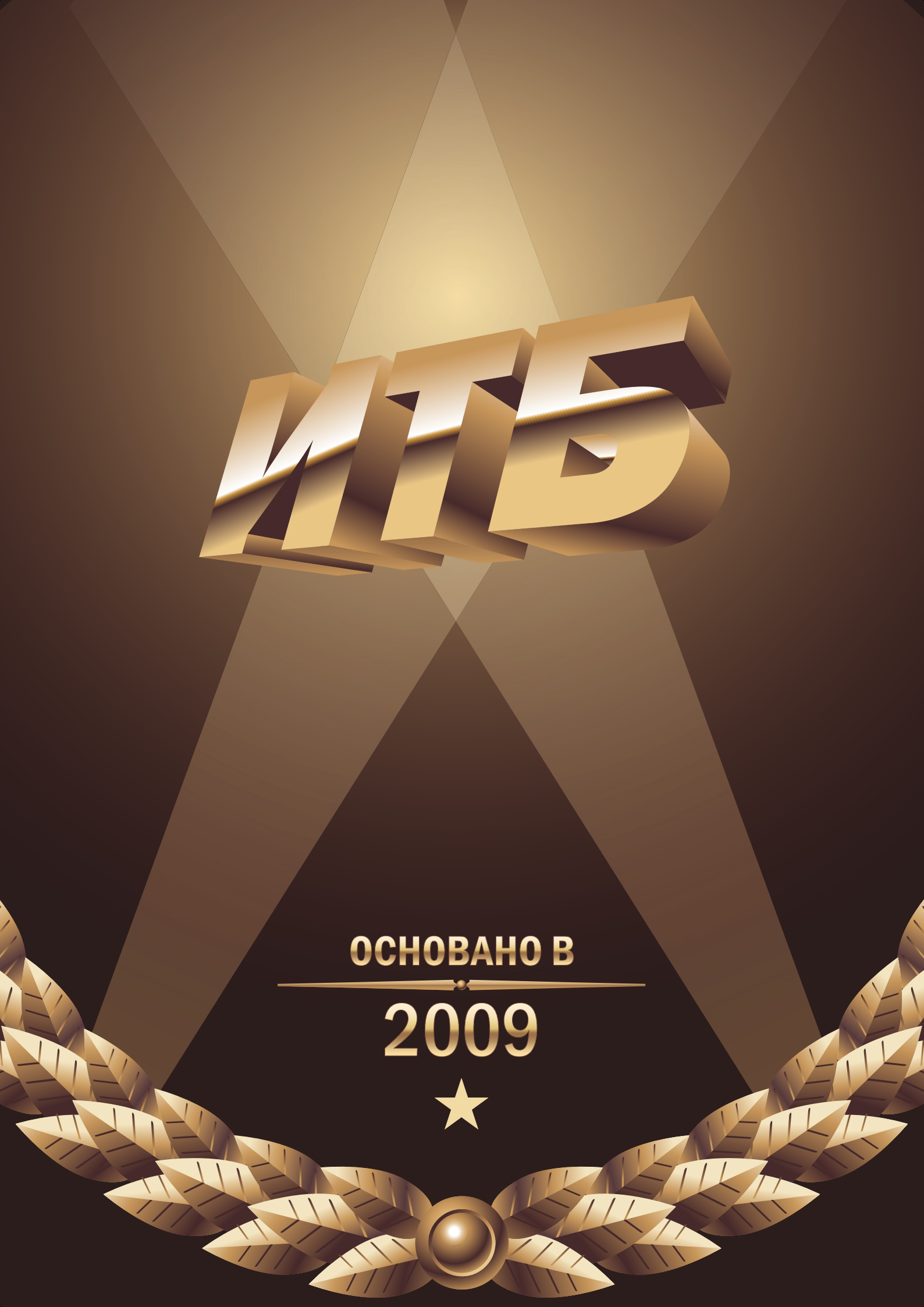

ИТБ
ОСНОВАНО В
2009

ВВЕДЕНИЕ

При подготовке данного материала использовались законодательные и нормативно-методические документы (НМД), практический опыт сертификации ООО «ИТБ», а также профессиональные мнения, подходы и взгляды специалистов испытательных лабораторий и органов по сертификации.

Настоящий материал носит неофициальный характер и представляет собой взгляд на процедуру со стороны разработчика и изготовителя средств защиты информации и защищённых средств обработки информации.

Часто путают понятия сертификации и аттестации. Подчеркнём, что сертификационные испытания (СИ) и аттестационные испытания (АИ) — это две различные процедуры. Сертификат соответствия и аттестат соответствия — два разных по предназначению документа.

КЛЮЧЕВЫЕ ТЕРМИНЫ

Сертификация — форма подтверждения соответствия объектов установленным требованиям, осуществляемая органом по сертификации.

Аттестация — процедура, целью которой является подтверждение соответствия системы защиты информации объекта информатизации требованиям по защите информации в реальных условиях эксплуатации.

В данном материале рассматриваются сертификационные испытания и сертификат соответствия средств обеспечения безопасности информационных технологий, включая защищённые средства обработки информации. Для удобства изложения вводится понятие прикладного программного обеспечения (ППО) в защищённом исполнении.

ППО в защищённом исполнении — это защищённые средства обработки информации, в которых реализованы механизмы защиты информации и которые не требуют применения дополнительных наложенных средств защиты информации (СЗИ) от НСД. В таком ППО могут быть реализованы механизмы защиты информации, полностью соответствующие требованиям регулятора (ФСТЭК России), либо частично. В случае частичной реализации механизмов защиты может потребоваться применение дополнительных наложенных средств защиты для нейтрализации актуальных угроз информационной безопасности (ИБ).

1. КОГДА ЦЕЛЕСООБРАЗНО РАЗРАБАТЫВАТЬ И/ИЛИ СЕРТИФИЦИРОВАТЬ ВСТРОЕННЫЕ МЕХАНИЗМЫ ЗАЩИТЫ?

а) **Когда ППО уже разработано и используется:** Если механизмы защиты реализованы, а ППО уже применяется в определённых технологиях, необходимо оценить полноту, качество и соответствие этих механизмов требованиям по безопасности информации.

б) Когда разрабатывается ППО с нуля: Если при создании нового ППО существуют законодательные требования по обеспечению безопасности информации или если ППО планируется использовать в информационных системах (ИС, АСУ ТП, ГИС, ИСПДн, КИИ), необходимо обеспечить безопасность информации в соответствии с требованиями технологического процесса.

в) **При отсутствии наложенных сертифицированных средств защиты:** В ситуациях, когда невозможно использовать уже существующие сертифицированные средства защиты информации, возникает необходимость разработки собственных встроенных механизмов.

г) **При негативном влиянии наложенных средств защиты на производительность:** Когда наложенные сертифицированные средства защиты информации существенно увеличивают нагрузку на серверное оборудование, АРМ пользователей, сети передачи данных, усложняют администрирование или значительно увеличивают затраты на внедрение и эксплуатацию системы. Важно учитывать, что такие средства могут быть причиной сбоев и отказов в технологическом процессе.

1.1 ПРИМЕНЕНИЕ СВОБОДНО РАСПРОСТРАНЯЕМОГО ПО (СРПО)

В настоящее время широко применяется свободно распространяемое программное обеспечение (англ. Open Source, сокращённо СРПО). Такой подход не запрещён, а в ряде случаев даже приветствуется регулятором. Приоритетным направлением при создании ППО в защищённом исполнении является использование встроенных механизмов защиты как в самом ППО, так и в применяемом СРПО.

Примеры ПО со встроенными механизмами защиты:

а) Механизмы защиты операционных систем (ОС).

б) Системы управления базами данных (СУБД).

в) Системы виртуализации.

г) Системы мониторинга.

д) Платёжные системы и других другие.

2. ПОДГОТОВКА СЗИ К СЕРТИФИКАЦИИ И ВЫБОР СХЕМЫ СЕРТИФИКАЦИИ

Прежде всего, необходимо разобраться, кто имеет право разрабатывать и изготавливать СЗИ от НСД или ППО в защищённом исполнении. Эти понятия детально описаны в приказе ФСТЭК России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

2.1 ОСНОВНЫЕ РОЛИ В ПРОЦЕССЕ СЕРТИФИКАЦИИ

а) **Изготовитель:** Изготовитель разрабатывает и производит средства защиты информации в соответствии с требованиями по безопасности информации.

б) **Заявитель:** Заявителем может выступать изготовитель, а также федеральные органы государственной власти, органы государственной власти субъектов РФ, органы местного самоуправления и организации, планирующие использовать средства защиты информации.

Эти роли могут выполнять только юридические или физические лица (как правило, индивидуальные предприниматели), имеющие лицензию ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации. Требования для получения данной лицензии описаны в соответствующем регламенте ФСТЭК РФ.

Если разработчик обладает лицензией ФСТЭК России, он может выступать в качестве заявителя и изготовителя СЗИ. Кроме того, изготовителем может быть лицензиат ФСТЭК России, получивший согласие разработчика на сертификацию и производство сертифицированной версии продукта. Такое согласие подтверждается договором и письмом, направляемым во ФСТЭК России

2.2 СХЕМЫ СЕРТИФИКАЦИИ

а) Единичный экземпляр: Сертификация единичного образца предполагает проведение испытаний данного экземпляра СЗИ и проверку организации его технической поддержки. Сертификат соответствия на единичный экземпляр является бессрочным, но его использование ограничено только конкретным объектом, для которого он был разработан. Тиражирование не допускается.

б) Партия: Сертификация партии предусматривает проведение испытаний выборки образцов СЗИ и проверку организации их технической поддержки. Заявитель указывает точное количество экземпляров, которое будет произведено. После исчерпания партии потребуется повторная процедура сертификации. Сертификат соответствия оформляется на срок до 5 лет.

в) Серийное производство: Сертификация серийного производства включает испытания выборки образцов СЗИ, проверку организации серийного производства и технической поддержки. Это наиболее сложная и трудоёмкая схема, требующая проверки множества аспектов. Сертификат соответствия также оформляется на срок до 5 лет.

При любой схеме сертификации обязательно проведение испытаний на соответствие требованиям по безопасности информации, которые устанавливают уровни доверия к средствам защиты информации. Эти требования регламентированы приказом ФСТЭК России от 2 июня 2020 №76г.

3. ТРЕБОВАНИЯ К ППО В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

В приказе № 55 подробно описаны требования, которым должно соответствовать ППО в защищённом исполнении. На практике заявители часто проводят испытания на соответствие требованиям технических условий (ТУ). В ТУ необходимо описать реализуемые механизмы защиты и требования к их реализации.

3.1 ПРИМЕРЫ ПРИКАЗОВ ФСТЭК РОССИИ, СОДЕРЖАЩИХ ТРЕБОВАНИЯ ПО БИ

а) «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (№ 21 от 18 февраля 2013 г.).

б) «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (№ 17 от 11 февраля 2013 г. с изменениями (в ред. Приказов ФСТЭК России от 15.02.2017 N 27, от 28.05.2019 N 106, от 28.08.2024 N 159)).

в) «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами» (№ 31 от 14 марта 2013 г. с изменениями (в ред. Приказов ФСТЭК России от 23.03.2017 N 49, от 09.08.2018 N 138, от 15.03.2021 N 46)).

г) «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ» (№ 239 от 25 декабря 2017 г. в ред. Приказов ФСТЭК России от 9 августа 2018 г. N 138, от 26 марта 2019 г. N 60, от 20 февраля 2020 г. N 35, от 28 августа 2024 г. N 159).

Заявитель может также провести испытания на соответствие требованиям профиля защиты, перечень которых представлен на сайте ФСТЭК России. При этом разрабатывается задание по безопасности (ЗБ), описывающее механизмы защиты и требования к их реализации. ЗБ утверждается ФСТЭК России.

4. ПОДГОТОВКА ЗАЯВКИ НА СЕРТИФИКАЦИЮ

При подаче заявки на сертификацию необходимо представить перечень заимствованных компонентов ПО, если в составе СЗИ используются продукты с открытым исходным кодом (СРПО). Этот перечень оформляется в табличной форме и предоставляется в электронном виде.

5. ВЫБОР ИСПЫТАТЕЛЬНОЙ ЛАБОРАТОРИИ (ИЛ)

Перечень аккредитованных лабораторий опубликован на сайте ФСТЭК России. При выборе ИЛ рекомендуется:

а) Изучить опыт выполнения аналогичных работ лабораторией.

б) Оценить количество положительных технических заключений и выданных сертификатов за последние 1–2 года.

в) Согласовать с ИЛ условия договора, состав работ, сроки, порядок оплаты и взаимодействия.

г) Ознакомить ИЛ с объектом оценки, предоставить документацию, продемонстрировать ППО и его особенности.

Географическая удалённость ИЛ также может сыграть важную роль, так как личные контакты могут ускорить решение возникающих вопросов.

6. ИТОГОВАЯ ПРОВЕРКА ГОТОВНОСТИ ППО К СЕРТИФИКАЦИИ

Перед подачей заявки необходимо убедиться в:

а) Полноте соответствия реализованных функций безопасности требованиям по безопасности информации.

б) Качестве разработанной проектной и эксплуатационной документации.

в) Отсутствии уязвимостей в конфигурации, архитектуре и коде.

7. НАИБОЛЕЕ ЧАСТО РЕАЛИЗУЕМЫЕ ФУНКЦИИ ЗАЩИТЫ

Разработчики СЗИ и ППО в защищённом исполнении обычно реализуют следующие функции:

а) Идентификация и аутентификация субъектов и объектов доступа (ИАФ).

б) Управление доступом (УПД).

в) Ограничение программной среды (ОПС).

г) Регистрация событий безопасности (РСБ).

д) Обеспечение целостности информационной системы и информации (ОЦЛ)

Примечание

В данном материале не рассматриваются средства криптографической защиты информации (СКЗИ).

Полный перечень мер безопасности приведён в приказах ФСТЭК России № 21, 17, 31, 239. С методическими рекомендациями можно ознакомиться на сайте ФСТЭК России.

Таким образом, прежде чем инициировать процедуру сертификационных испытаний ППО в защищённом исполнении, необходимо оценить его готовность по следующим параметрам:

а) Полнота реализации функций безопасности.

б) Качество документации.

в) Отсутствие уязвимостей и потенциально опасных функциональных возможностей.

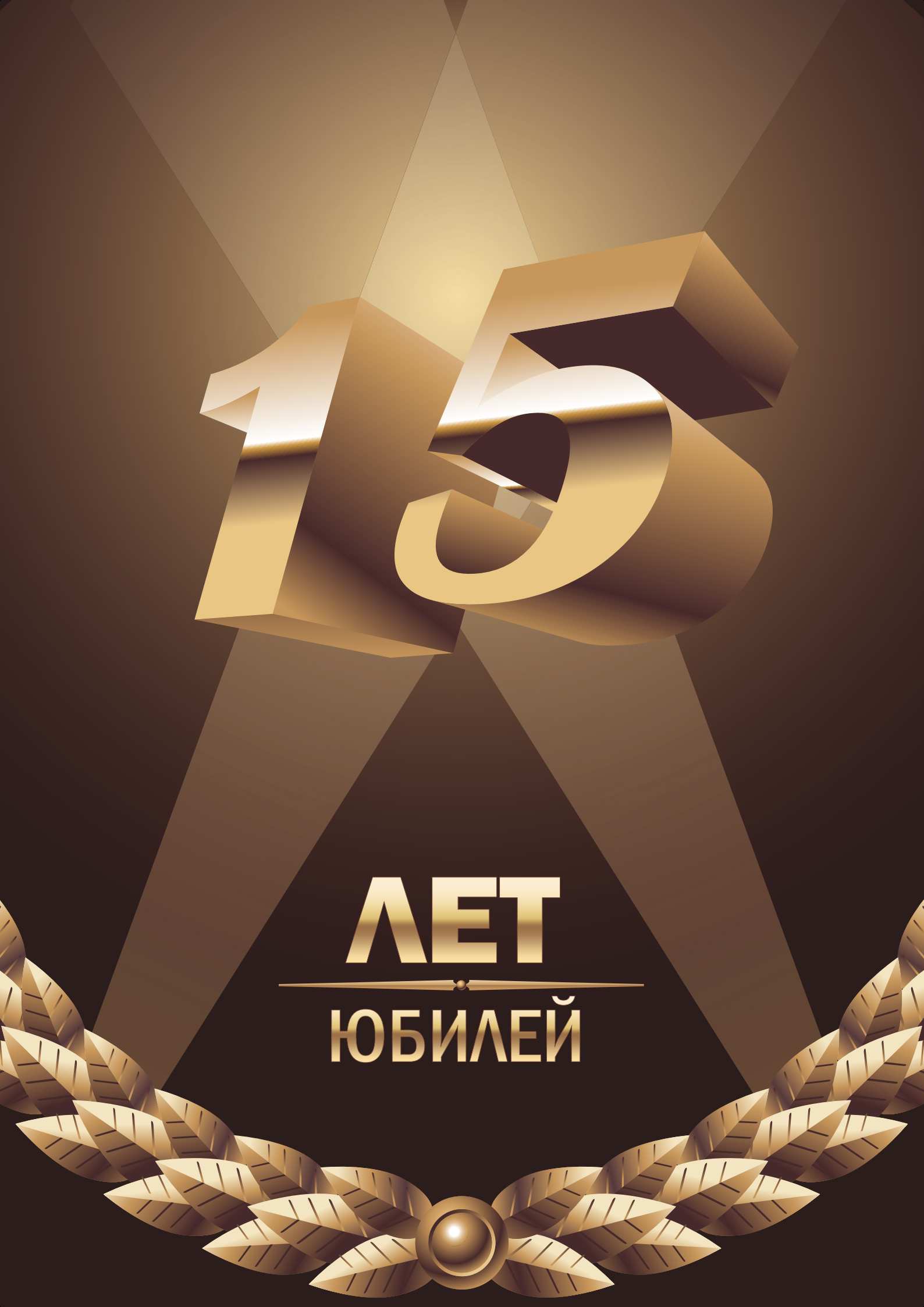
МЫ В СОЦ. СЕТЯХ

/itb_spb/

/channel/47130305/

/profile/14089663908?lr=2

Подпишитесь на канал TTL, чтобы быть в числе первых, кто узнает о новостях и получает эксклюзивные материалы по информационной безопасности


15
ЛЕТ
ЮБИЛЕЙ