РФЯЦ ВНИИЭФ

РОССИЙСКИЙ ФЕДЕРАЛЬНЫЙ ЯДЕРНЫЙ ЦЕНТР ВНИИЭФ

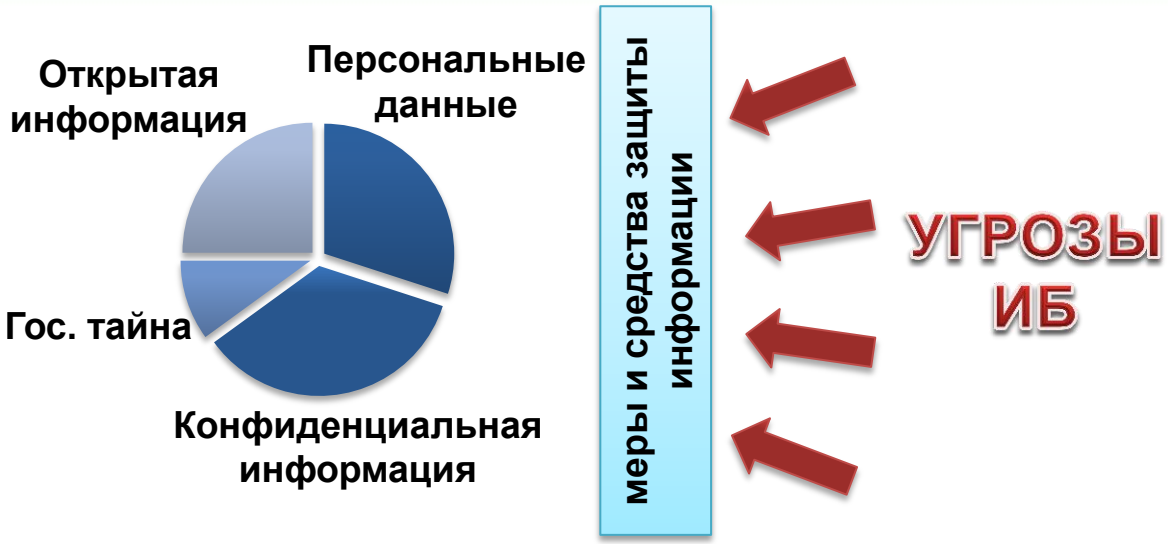
Построение защищенных решений на базе ПО отечественной разработки и проектов Open Source

Докладчик:
Эксперт испытательной лаборатории
ФГУП «РФЯЦ-ВНИИЭФ»
С. В. Холушкина

г. Саров, 2017

ПОЛИТИКА ГОСУДАРСТВА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Российские предприятия под угрозой атак со стороны злоумышленников



Большинство предприятий РФ в своей работе неразрывно связаны с информацией ограниченного доступа, утечка или нарушение которой может подвергнуть **угрозе сохранность активов и реализацию бизнес-целей**, что ставит для них проблему **обеспечения должного уровня защищенности информации на первое место**

- *Закон РФ от 21.08.1993 № 5485-1 «О государственной тайне»*
- *Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»*
- *ФЗ от 27.07.2006 №149-ФЗ Об информации, информационных технологиях и о защите информации»*

На сегодняшний день более 80% программно-аппаратных продуктов, используемых на предприятиях РФ для обработки информации, подлежащей защите, являются зарубежными разработками

Зарубежное ПО невозможно подвергнуть анализу на предмет соответствия требованиям безопасности информации

Отказ большинства зарубежных разработчиков от предоставления исходных кодов ИТ-продуктов для проведения анализа уязвимостей **ставит под сомнение безопасность их использования при обработке защищаемой информации**

В целях повышения уровня защищенности конфиденциальной информации, а также информации, содержащей сведения, составляющие государственную тайну, утверждено

Постановление Правительства РФ от 16.11.2015г. №1236 «Об установлении запрета на допуск ПО, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»

Программа импортозамещения – важный шаг к созданию доверенной программно-аппаратной среды российских предприятий

ПРИОРИТЕТ №1

Задача ИМПОРТОЗАМЕЩЕНИЯ, направленная на

- ✓ формирование **отечественной доверенной программно-аппаратной среды**, реализующей весь спектр функциональных потребностей российских предприятий;
- ✓ создание мощной, независимой от внешнеполитических отношений платформы, обеспечивающей **информационную безопасность бизнеса и оборонно-промышленного комплекса страны**

поддержка государства

- Утверждение плана импортозамещения ПО
  Приказ Минкомсвязи от 01.04.2015г. №96
- Создание единого реестра российского ПО
  ФЗ от 29.06.2015 №188-ФЗ1
- Субсидирование части затрат промышленных предприятий на приобретение и внедрение отечественного ПО
  ПП РФ от 14.11.2014 №1200
- Оказание содействия в реализации особо значимых проектов по Приволжскому федеральному округу
  Распоряжение полномочного представителя Президента РФ в ПФО от 16.10.2015 №А53-52р
- Реестр российских программ для электронных вычислительных машин и баз данных
  ПП РФ от 23.03.2017 №325
- Перечень видов радиоэлектронной аппаратуры для обеспечения государственных и муниципальных нужд
  ПП РФ от 26.09.2016 №968

Сертификат соответствия требованиям безопасности информации – основной показатель надежности

Изделия ИТ со встроенными механизмами защиты

СЕРТИФИКАЦИЯ

Согласно требованиям государственных регуляторов в области защиты информации **все изделия** информационных технологий, применяемые для обработки информации **ограниченного распространения,** в **обязательном** порядке должны быть **сертифицированы по требованиям безопасности информации**

Развитие информационных технологий определяет необходимость совершенствования мер защиты информации

В последние годы осуществляется непрерывное ужесточение требований к реализации функций защиты и изделиях ИТ, используемых для обработки защищаемой информации

- Переход на **сертификацию по требованиям ГОСТ Р ИСО/МЭК 15408**-(1, 2, 3).
- С 2014 года обязательным этапом сертификационных испытаний является проведение **анализа уязвимостей средств защиты информации и сред их функционирования**.
- **Утверждены требования безопасности** к средствам:
  - ✓ обнаружения вторжения (приказ ФСТЭК России от 06.12.2011 № 638);
  - ✓ антивирусной защиты (приказ ФСТЭК России от 20.03.2012 № 28);
  - ✓ доверенной загрузки (приказ ФСТЭК России от 27.09.2013 № 119дсп);
  - ✓ контроля съемных машинных носителей информации (приказ ФСТЭК России от 28.07.2014 № 87);
  - ✓ межсетевого экранирования (приказ ФСТЭК России от 09.02.2016 № 9);
  - ✓ к операционным системам (приказ ФСТЭК России от 19.08.2016 №119).
- Определен порядок классификации и **требования для информационных систем, не обрабатывающих государственную тайну**:
  - ✓ Информационные системы персональных данных (ПП РФ от 01.11.2012 №1119);
  - ✓ Государственные информационные системы (приказ ФСТЭК России от 11.02.2013 №17);
  - ✓ О внесении изменений в требования к ГИС (Приказ ФСТЭК России от 15.02.2017 №27);
  - ✓ Информационные системы общего пользования (Приказ ФСБ и ФСТЭК России от 31.08.2010 №416/489).

OPEN SOURCE КАК БАЗИС ПРИ ПОСТРОЕНИИ ДОВЕРЕННОЙ ПРОГРАММНОЙ СРЕДЫ РОССИЙСКИХ ПРЕДПРИЯТИЙ

Open Source открывает дополнительные возможности

Разработчики Open Source решений охватывают **широкий диапазон прикладных областей.** На сегодняшний день в решениях Open Source существуют **аналоги всевозможных мировых решений** в прикладных областях экономики, управления предприятием, разработки и т.д.

Преимущества проектов с открытым исходным кодом

- функционал охватывает широкий спектр задач;
- открытость библиотеки исходных кодов;
- наличие в свободном доступе сети интернет;
- интегрирует практики мирового сообщества.

Проекты Open Source являются функциональным базисом для создания доверенного прикладного программного продукта на отечественном рынке

Безопасность информации – уязвимое место Open Source

Свойства уязвимого ПО

- ❑ использованы небезопасные функции программирования;
- ❑ использованы недоверенные сторонние модули, библиотеки, средства защиты информации;
- ❑ ненадежная архитектура,
- ❑ уязвимости кода;
- ❑ недокументированные функции;
- ❑ недекларированные возможности;
- ❑ отсутствие сопровождения кода со стороны разработчиков

Методы снижения угроз ИБ

- ✓ использование безопасных версий функций;
- ✓ аудит безопасности используемых функций и использование доверенных источников;
- ✓ уделение особого внимания архитектуре;
- ✓ аудит кода на каждом этапе разработки;
- ✓ документирование всех функций разработки;
- ✓ отсутствие недекларированных возможностей;
- ✓ использование решений предполагающих сопровождение или самостоятельное сопровождение

Обеспечение информационной безопасности достигается методом комплексного подхода и предполагает соблюдение требований по защите информации на всех этапах жизненного цикла программного обеспечения

Механизмы защиты информации качественно дополняют прикладной функционал

Обработка конфиденциальной информации требует ее надежной защиты и, исходя из этого, необходимо понимание: **простое надстраивание функций защиты информации над проектом не эффективно**

Для построения надежного решения требуется:

- ✓ Анализ надежности архитектуры и конфигурации;
- ✓ Реализация механизмов защиты в соответствии с требованиями ИБ;
- ✓ Качественная интеграция функций безопасности;
- ✓ Анализ уязвимостей исходных кодов, тестирование на проникновение.

Сертификация по требованиям ИБ – повышает надежность прикладного решения, а наличие сертификата соответствия повышает степень доверия пользователей и расширяет рынок конечных потребителей

Применение принципов безопасной разработки повышает уровень защищенности создаваемых решений

При применении проектов **Open Source для построения защищенных решений** следует обратить особое внимание на обеспечение **требований безопасности информации**. Использование принципов безопасной разработки при реализации системы защиты информации повышает уровень доверия продукта

- ✓ Использование вспомогательных средств аудита и анализа кода (анализаторы исходных кодов, автоматизированные средства анализа уязвимостей, средства для фазинг-тестирования и т.д.);
- ✓ Декларирование функциональных возможностей продукта;
- ✓ Обеспечение достаточной глубины и качества проводимых тестирований;
- ✓ Проведение периодического анализа защищенности;
- ✓ Привлечение к процессу разработки специалистов ИБ.

Наличие исходных текстов облегчает процесс интеграции наложенных средств защиты информации и обеспечивает возможность проведения сертификации продукта для его применения при обработке конфиденциальной информации

Поддержание необходимого уровня информационной безопасности должно осуществляться во всех направлениях

Являясь предприятием, входящим в состав ядерно-оружейного комплекса России, ФГУП «РФЯЦ-ВНИИЭФ» всецело ощущает условия **жестких ограничений на приобретение и применение зарубежных изделий и технологий** двойного назначения

С целью поддержания требуемого уровня защищенности информации в ФГУП «РФЯЦ-ВНИИЭФ» определен вектор **создания и развития центра компетенций по информационной безопасности**

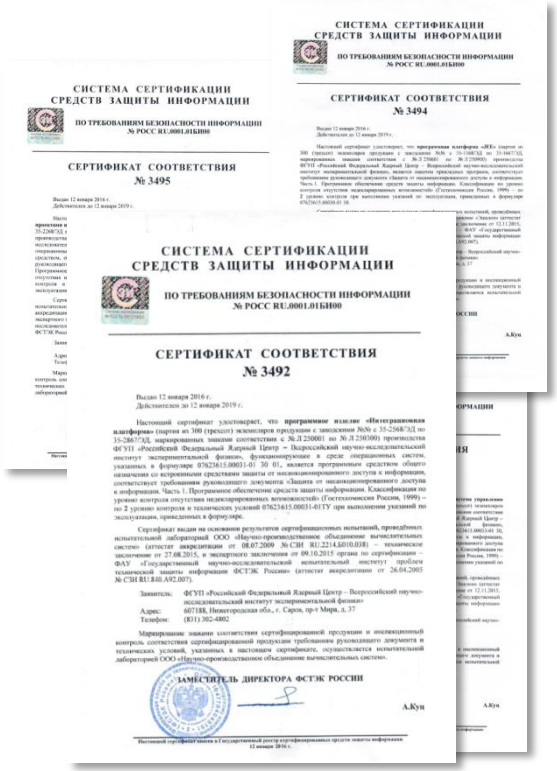
- создание доверенных программных продуктов с использованием принципов безопасного программирования;
- разработка безопасных импортонезависимых решений в области управления жизненным циклом изделий;
- сертификация изделий ИТ по требованиям безопасности информации;
- проектирование и аттестация защищенных информационных и автоматизированных сетей;
- разработка и внедрение положений системы менеджмента информационной безопасности;
- непрерывный аудит требований государственных регуляторов и состояния защищенности информации в институте.

ФГУП «РФЯЦ-ВНИИЭФ» разрабатывает прикладные решения для автоматизации управления процессами предприятия с учетом требований ИБ

ФГУП «РФЯЦ-ВНИИЭФ» имеет опыт разработки импортонезависимых решений, в частности, информационных систем, **соответствующих предъявляемым требованиям безопасности** информации, **подтвержденных наличием сертификатов соответствия** ФСТЭК России, и **основанных, в том числе, на проектах Open Source**

Комплекс программных решений для автоматизации процессов управления предприятием:

- Система управления нормативно-справочной информацией (СУ НСИ),
- Интеграционная платформа (ИП),
- Портальные сервисы (ПС),
- Система управления проектами и программами (СУПП),
- Система управления эффективностью деятельности на основе BI-решений (BI);
- Система управления предприятия (ERP-система);
- Система управления сквозным жизненным циклом изделия (ЛОЦМАН:PLM);
- Система управления процессами производства (MES).



Информационные системы интегрированы в процесс деятельности предприятия и охватывают все этапы ЖЦИ и управления предприятием

Испытательная лаборатория по сертификации средств защиты информации расширяет спектр услуг института

В составе ФГУП «РФЯЦ-ВНИИЭФ» действует Испытательная лаборатория по сертификации средств защиты информации, аккредитованная в системе ФСТЭК России

Федеральная служба
по техническому и экспортному
контролю

АТТЕСТАТ АККРЕДИТАЦИИ
ИСПЫТАТЕЛЬНОЙ ЛАБОРАТОРИИ

СЗИ RU.0001.01БИ00.Б001

выдан 27 ноября 2015 г.

Настоящий аттестат выдан федеральному государственному унитарному предприятию

«Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики»
ИНН 5254001230

607188, Нижегородская обл., г. Саров, проспект Мира, дом 37

и удостоверяет, что федеральное государственное унитарное предприятие

«Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики»

607188, Нижегородская обл., г. Саров, проспект Мира, дом 37

соответствует требованиям Правил аккредитации органов по сертификации и испытательных лабораторий (центров), утвержденных постановлением Правительства Российской Федерации от 3 ноября 2014 г. № 1149, и Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, утвержденных приказом ФСТЭК России от 10 апреля 2015 г. № 33.

Аккредитован(о) в качестве испытательной лаборатории

в соответствии с областью аккредитации, определенной в приложении к настоящему аттестату.

Дата внесения сведений в реестр аккредитованных лиц 27 ноября 2015 г.

Заместитель директора ФСТЭК России А.В.Куц

Основные услуги:

- **Сертификация изделий ИТ** по требованиям безопасности информации в системе сертификации ФСТЭК России;
- **Подготовка к сертификации изделий ИТ**:
  - функциональное тестирование;
  - анализ уязвимостей средств защиты информации и сред их функционирования;
  - тестирование проникновения;
  - анализ программных кодов на отсутствие НДВ;
  - разработка документации;
- **Сопровождение работ по сертификации.**

Проекты ИЛ ВНИИЭФ по сертификации ИТ-изделий

Сопровождение сертификации в рамках проекта ФГУП «РФЯЦ-ВНИИЭФ» по созданию Типовой информационной системы состоящей из:

- Системы управления нормативно-справочной информацией (сертификат соответствия №3363);
- Интеграционной платформы (сертификат соответствия №3492);
- Портальных сервисов (сертификат соответствия №3493);
- Системы управления проектами и программами (сертификат соответствия №3495);
- Системы управления эффективностью на основе BI-решений (сертификат соответствия №3496);
- Программной платформы «JEE» (сертификат соответствия №3494).

Проведение сертификации по требованиям безопасности информации:

- Сертификация межсетевого экрана Cisco ASA 5585-S20-K8 (сертификат соответствия № 3647).
- Сертификация системы управления базами данных Oracle Database 11 g (Release 2) Enterprise Edition версии 11.2.0.4 (решение ФСТЭК России от 08.11.2016 №5362).
- Сертификация информационно-аналитической системы QMStatus.
- Сертификация информационной системы «Техэксперт» (решение ФСТЭК России от 16.01.17 №5435).
- Сертификация системы управления базами данных Oracle Database Standart Edition 2 версии 12.1.0.2.

СПАСИБО ЗА ВНИМАНИЕ

Контактные данные ИЛ ФГУП «РФЯЦ-ВНИИЭФ»:

Телефон: 8 (83130) 2-96-44

Факс: 8(83130) 2-95-68

E-mail: il@vniief.ru

Контактные лица ИЛ ФГУП «РФЯЦ-ВНИИЭФ»:

- Людмила Юрьевна Застылова – руководитель ИЛ ФГУП «РФЯЦ-ВНИИЭФ»

Тел.: 8(83130)2-96-24; 8(910)872-42-55

E-mail: LYZastylova@rosatom.ru; LYZastylova@vniief.ru

- София Владимировна Холушкина – специалист ИЛ ФГУП «РФЯЦ-ВНИИЭФ»

Тел.: 8(83130)2-96-44 (доб. 213); 8(910)381-88-77

E-mail: SVKholushkina@rosatom.ru; SVKholushkina @vniief.ru