НРК Р.О.С.Т.

От сертификации и оценки соответствия по ОУД-4 до безопасной разработки ПО.

Применение сертифицированного программного обеспечения - «Потёмкинская деревня» или реально выполнимое требование? Путь к безопасному процессу разработки

Андрей Киселев - Директор по информационной безопасности АО «НРК - Р.О.С.Т.» , АО «НРК Фондовый Рынок».

НРК Р.О.С.Т.

АО «НРК -Р.О.С.Т.» - КРУПНЕЙШИЙ РЕГИСТРАТОР РОССИИ
Лицензии специализированного депозитария и депозитарной деятельности.

АО «НРК Фондовый Рынок» - депозитарная, брокерская и дилерская деятельность.

НРК
Р.О.С.Т.

ЦЕЛИ КОМПАНИИ
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью обеспечения информационной безопасности в Компании является предотвращение нанесения Компании и ее клиентам материального, репутационного и иных видов ущерба, вследствие реализации угроз нарушения безопасности информации, обрабатываемой и хранимой Регистратором.

СМИБ основана на:

ISO 27001
ГОСТ 57580

СЕРТИФИКАТ

TÜV AUSTRIA

ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ | شهادة | 证书 | 인증서

соответствия системы менеджмента требованиям стандарта ISO/IEC 27001:2013

В соответствии с процедурами TÜV AUSTRIA настоящим подтверждается, что

Акционерное общество
«Независимая регистраторская компания Р.О.С.Т.»
ул. Стромынка, д.18, корпус 5Б, пом. IX
107076, г. Москва
Российская Федерация

Применяет систему менеджмента, соответствующую вышеназванному стандарту в следующих областях:

Разработка и оказание услуг по: ведению реестра владельцев ценных бумаг, организации и проведению общих собраний акционеров, выплате доходов по ценным бумагам, депозитарной деятельности и деятельности специализированного депозитария.

Действующее заявление о применимости: V2022/OD-04-152, 08.04.2022

Регистрационный номер сертификата: TA420223015376 Действителен до 2025-10-31
Дата первичной сертификации: 2022-12-13

Орган по сертификации
TÜV AUSTRIA GMBH

Вена, 2024-03-26

Данная сертификация была проведена в соответствии с процедурами аудитирования и сертификации TÜV AUSTRIA GMBH и подлежит регулярным надзорным аудитам.
TÜV AUSTRIA GMBH Deutschstraße 10 A-1230 Wien www.tuv.at

Москва 2024г.

НРК Р.О.С.Т.

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

FW	VPN2FA	IDS/IPS	DLP	AAA	AV	SIEM	...

kaspersky

SEARCHINFORM INFORMATION SECURITY

КРИПТОПРО

Rusiem

КОД БЕЗОПАСНОСТИ

FORTINET

Microsoft

UserGate

Check Point SOFTWARE TECHNOLOGIES LTD.

s•terra

НРК Р.О.С.Т.

Сертификация – термин «сертификация» означает подтверждение заявленных характеристик товара, работ, услуг или даже квалификации специалиста третьей стороной. Сертифицированное по требованиям безопасности программное обеспечение (ПО) – это программа, прошедшая процедуру проверки соответствия требованиям государственных стандартов и нормативных документов по защите информации Федеральной службы по техническому и экспортному контролю России (ФСТЭК России) и ФСБ России.

Оценка по ОУД4 -

5.2.3 Доверие - основа для уверенности в том, что продукт ИТ отвечает целям безопасности. Доверие могло бы быть получено путем обращения к таким источникам, как бездоказательное утверждение, предшествующий аналогичный опыт или специфический опыт, однако, ИСО/МЭК 15408 обеспечивает доверие с использованием активного исследования. Активное исследование - это оценка продукта ИТ для определения его свойств безопасности.

НРК Р.О.С.Т.

Сертификация – зачем нужна?

История вопроса ГОСТ 15408 родом из 70х с монолитными архитектурами.

Соответствие требованиям различных стандартов ГОСТ 27001, ГОСТ 57580.1, ГОСТ 15408, …

Органы сертификации СЗИ
- ФСТЭК
- ФСБ

Требование 757-П (ГОСТ 57580 и 15408).

ФЗ 152 по персональным данным.
Требование по использованию сертифицированных СЗИ только к Гос. Системам.
Приказ ФСТЭК России от 18 февраля 2013 г. № 21

187 ФЗ КИИ (требования по сертификации Средств защиты информации на значимых объектах КИИ)
Приказ ФСТЭК России № 235 от 21.12.2017

НРК Р.О.С.Т.

Требования банка России

Проведение оценки соответствия по ОУД4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013 предусмотрено Положениями Банка России:

- 757-П – для некредитных финансовых организаций, реализующих усиленный и стандартный уровни ЗИ;
- 683-П – для кредитных организаций.

Согласно 757-П:

- прикладное программное обеспечение и приложения, распространяемые НФО своим клиентам для совершения действий в целях осуществления финансовых операций;
- программное обеспечение, обрабатывающее защищаемую информацию при приеме электронных сообщений к исполнению в системах и приложениях с использованием сети «Интернет».

1.8. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование для осуществления финансовых операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых некредитными финансовыми организациями своим клиентам для совершения действий в целях осуществления финансовых операций, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"),

прошедших сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю (далее - сертификация) или

оценку соответствия по требованиям к оценочному уровню доверия не ниже, чем ОУД 4, в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности", … (далее - оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений).

НРК Р.О.С.Т.

Сертификация состояния.

НРК Р.О.С.Т.

Сертификация процесса.

НРК
Р.О.С.Т.

Обеспечение доверия ПО разработчиком или заказчиком. Экономика. Рыночные или административные меры?

НФО:

- Регистраторы (31 шт.).
- Депозитарии (256 шт.).
- Брокеры (370 шт.).
- Управляющие (259 шт.).
- Страховые (135 шт.).
- Спец депозитарии (27 шт.).
- Операторы финансовых платформ (9 шт.)
- …..

НРК Р.О.С.Т.

Что делать?

До конца 2024 г. ФСТЭК планирует упростить процесс сертификации софта. Сейчас процедура занимает от девяти месяцев до года, а повторная сертификация при каждом изменении кода — еще несколько месяцев. Новый подход заключается в том, что аттестовывать будут сам процесс разработки ПО. Это значит, что дополнительная сертификация обновлений не потребуется.

Внедрение приемов «защищенного» программирования (SDLC) (совпадает с требованием сертификации процесса разработки).

Анализ уязвимостей (было в 684-П –в 757-П отсутствует) .

Независимый аудит кода (услуги по анализу защищенности приложений и операционных систем).

Рыночные механизмы. Никто не будет покупать рискованное ПО с «дырками» при наличие конкуренции.

НРК Р.О.С.Т.

СПАСИБО ЗА ВНИМАНИЕ

Директор по информационной безопасности АО «НРК- Р.О.С.Т.»
Киселев Андрей Васильевич

a@rrost.ru, www.rrost.ru