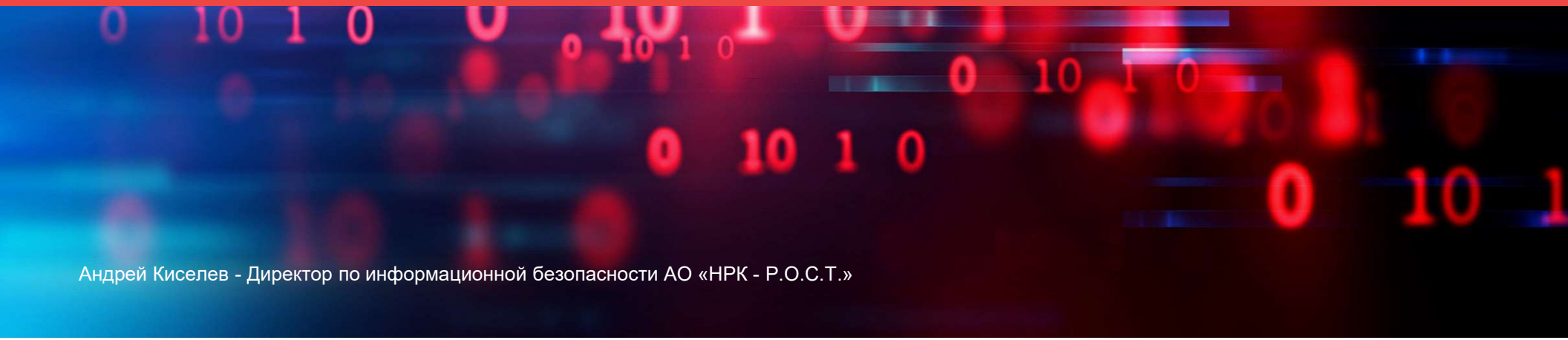
НРК Р.О.С.Т.

Практические вопросы реализации требований Положения № 757-П и ГОСТ Р 57580.1-2018 при разработке внутренних документов информационной безопасности в компании регистраторе.



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

НРК
Р.О.С.Т.

АО «НРК -Р.О.С.Т.» - КРУПНЕЙШИЙ РЕГИСТРАТОР РОССИИ АБСОЛЮТНЫЙ ЛИДЕР НАЦИОНАЛЬНОГО РЕЙТИНГА РЕГИСТРАТОРОВ ПАРТАД, НАЧИНАЯ С 2013 ГОДА

НРК
Р.О.С.Т.

ЦЕЛИ КОМПАНИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью обеспечения информационной безопасности в Регистраторе является предотвращение нанесения Регистратору 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

НРК Р.О.С.Т.

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

FW	VPN 2FA	IDS/IPS	DLP	AAA	AV	SIEM	...

kaspersky

SEARCHINFORM INFORMATION SECURITY

КРИПТОПРО

Rusiem

КОД БЕЗОПАСНОСТИ

tenable

Microsoft

FORTINET

Check Point SOFTWARE TECHNOLOGIES LTD.

s•terra

НРК Р.О.С.Т.

НАЧАЛЬНЫЕ УСЛОВИЯ (НАЧАЛИ В 2019).

1. Определили цели – Соответствие 27001 и 57580.
   Документов должно быть 2-3 и написаны на понятном для работников языке.

2. Уровень защиты. (2 – стандартный) Если О, то достаточно иметь утвержденные требования в НПА и свидетельства их выполнения. Для 2го уровня это достаточно большой % при оценке.

3. Поняли что сами не справимся. Пригласили консультантов.

НРК Р.О.С.Т.

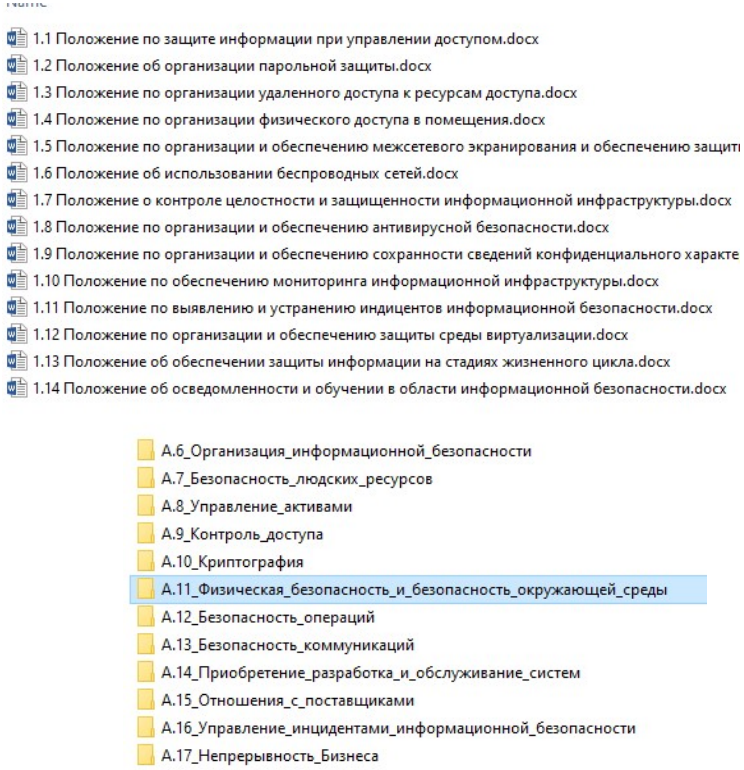
С КАКИМИ СЛОЖНОСТЯМИ СТОЛКНУЛИСЬ.

- Неоднозначность в понимании требований ГОСТа. Консультанты
- предлагали утвердить типовые 14 документов 57580 и более 90 по 27001. У консультантов нет желания вникать в бизнес процессы происходящие в компании.

нашли компромисный вариант.
самостоятельно делали документы, а консультанты проверяли на соответвие 27001 и 57580.

после утверждения проводили внутренний аудит, на

- исполнимость. Столкнулись с тем что некоторые моменты не исполнялись так как написано. Делали новые версии. Меняли «должны» на «следует» и т.д.



Инструкция по обеспечению информационной безопасности в корпоративной информационной системе АО «НРК- Р.О.С.Т.»

НРК Р.О.С.Т.

ПРИМЕРЫ ТРЕБОВАНИЙ 57580

Требование

УЗП.2 Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа

Реализация

«Процедура администрирования прав доступа в программные системы»

7.1 Администратором ПС осуществляется периодический контроль:
соответствия фактического состава разблокированных учетных записей **фактическому составу сотрудников Регистратора**;

Инструкция по обеспечению безопасности ИТ-инфраструктуры администраторами АО «НРК-Р.О.С.Т.»

6.1 Учетные записи пользователей и эксплуатационного персонала, в том числе привилегированные учётные записи, создаются в АО «НРК-Р.О.С.Т.» исключительно по заявкам на доступ в системе заявок 1С ITIL. Все создаваемые учетные записи должны быть уникальными и персонифицированными. "

Контроль

Периодические задания в системе "1С:ITIL Управление информационными технологиями предприятия"

НРК Р.О.С.Т.

ПРИМЕРЫ ТРЕБОВАНИЙ ГОСТ 57580

Требование

УЗП.7 Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа)

Реализация

"Процедура администрирования прав доступа в программные системы»

4.8. Сотрудники авторизующие доступ являются владельцами программной системы (актива) и приведены в Приложении № 3 к настоящей Процедуре. Во время отсутствия (отпуск, по болезни) указанных Сотрудников, допускается авторизация прав доступа сотрудниками, их замещающими.";

5.3. Заявка на включение пользователя в группы доступа ПС, назначение, изменение прав доступа в ПС визируется Сотрудником, указанным как Владелец программной системы согласно приложению 3 к данной процедуре, в 1С ITIL. В случае если указано несколько владельцев у одной программной системы, визирование происходит всеми Владельцами. Если заявка является нетиповой, то она подлежит обязательному согласованию сотрудником ОИБ.

Инструкция по обеспечению безопасности ИТ-инфраструктуры администраторами АО «НРК-Р.О.С.Т.»

6.1 Учетные записи пользователей и эксплуатационного персонала, в том числе привилегированные учётные записи, создаются в АО «НРК-Р.О.С.Т.» исключительно по заявкам на доступ в системе заявок 1С ITIL. Все создаваемые учетные записи должны быть уникальными и персонифицированными. "

Контроль

Организованы заявки в системе "1С:ITIL Управление информационными технологиями предприятия"

НРК Р.О.С.Т.

ПРИМЕРЫ ТРЕБОВАНИЙ ГОСТ 57580

Требование

РД.9 Запрет использования учетных записей субъектов логического доступа с незаданными аутентификационными данными или заданными по умолчанию разработчиком ресурса доступа, в том числе разработчиком АС

Реализация

"Инструкция по обеспечению информационной безопасности в корпоративной информационной системе АО «НРК- Р.О.С.Т.»

16.3 Запрещается использовать стандартный или предустановленный пароль;
Запрещается использовать в качестве пароля информацию, связанную с личностью Пользователя (дату рождения, номер телефона, адрес и т.п.);«

Контроль

Проверки паролей по умолчанию. Подбор паролей по словарю на копии базы АД.

НРК Р.О.С.Т.

ПРИМЕРЫ ТРЕБОВАНИЙ ГОСТ 57580

Требование

ФД.12 Расположение серверного и сетевого оборудования в запираемых серверных стоечных шкафах

Реализация

Положение о пропускном режиме в помещения

"Серверное и сетевое оборудование располагается в запираемых серверных стоечных шкафах. Доступ к серверному и сетевому оборудованию фиксируется в соответствующем Журнале учета доступа к серверному и сетевому оборудованию.

В нерабочее время надежное закрытие помещений обеспечивается путем закрытия входных дверей помещения механическими замками.«

Контроль

Наличие записей в журнале. Актуальный список работников. Наличие замков.

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