

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

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



офиса в 47  
регионах РФ



переводов  
дивидендов  
в год



собраний  
акционеров  
в год



операций  
в реестре  
в год



сотрудников  
3 сотрудника ИБ



каждый  
5 эмитент  
всей  
регистраторской  
отрасли

## 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**

## 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

## 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.

## 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 соответствие 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 «HPK- P.O.C.T.»

1.1 Положение по защите информации при управлении доступом.docx  
1.2 Положение об организации парольной защиты.docx  
1.3 Положение по организации удаленного доступа к ресурсам доступа.docx  
1.4 Положение по организации физического доступа в помещения.docx  
1.5 Положение по организации и обеспечению межсетевое экранирования и обеспечению защиты  
1.6 Положение об использовании беспроводных сетей.docx  
1.7 Положение о контроле целостности и защищенности информационной инфраструктуры.docx  
1.8 Положение по организации и обеспечению антивирусной безопасности.docx  
1.9 Положение по организации и обеспечению сохранности сведений конфиденциального характе  
1.10 Положение по обеспечению мониторинга информационной инфраструктуры.docx  
1.11 Положение по выявлению и устранению инцидентов информационной безопасности.docx  
1.12 Положение по организации и обеспечению защиты среды виртуализации.docx  
1.13 Положение об обеспечении защиты информации на стадиях жизненного цикла.docx  
1.14 Положение об осведомленности и обучении в области информационной безопасности.docx

A.6\_Организация\_информационной\_безопасности  
A.7\_Безопасность\_людских\_ресурсов  
A.8\_Управление\_активами  
A.9\_Контроль\_доступа  
A.10\_Криптография  
A.11\_Физическая\_безопасность\_и\_безопасность\_окружающей\_среды  
A.12\_Безопасность\_операций  
A.13\_Безопасность\_коммуникаций  
A.14\_Приобретение\_разработка\_и\_обслуживание\_систем  
A.15\_Отношения\_с\_поставщиками  
A.16\_Управление\_инцидентами\_информационной\_безопасности  
A.17\_Непрерывность\_Бизнеса

## 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"

## 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 ИТIL. 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 ИТIL. Все создаваемые учетные записи должны быть уникальными и персонифицированными. "

### Контроль

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

## ПРИМЕРЫ ТРЕБОВАНИЙ ГОСТ 57580

### Требование

РД.9 Запрет использования учетных записей субъектов логического доступа с незадаанными 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.

## 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.



## СПАСИБО ЗА ВНИМАНИЕ

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

[a@rrost.ru](mailto:a@rrost.ru), [www.rrost.ru](http://www.rrost.ru)