

# Что нужно знать медикам о кибербезопасности





# ОЛЬГА ПОЗДНЯК

## **Королева кибербезопасности**

Помогаю предпринимателям защищать свои бизнесы от киберугроз

## **Предприниматель**

Уже 18 лет в бизнесе

## **Организатор**

Провела 780 онлайн и офлайн событий на территории 6 стран и 28 городов

## **Трижды мама**

Мальчишек от 7 до 14 лет

## **Вегетарианка**

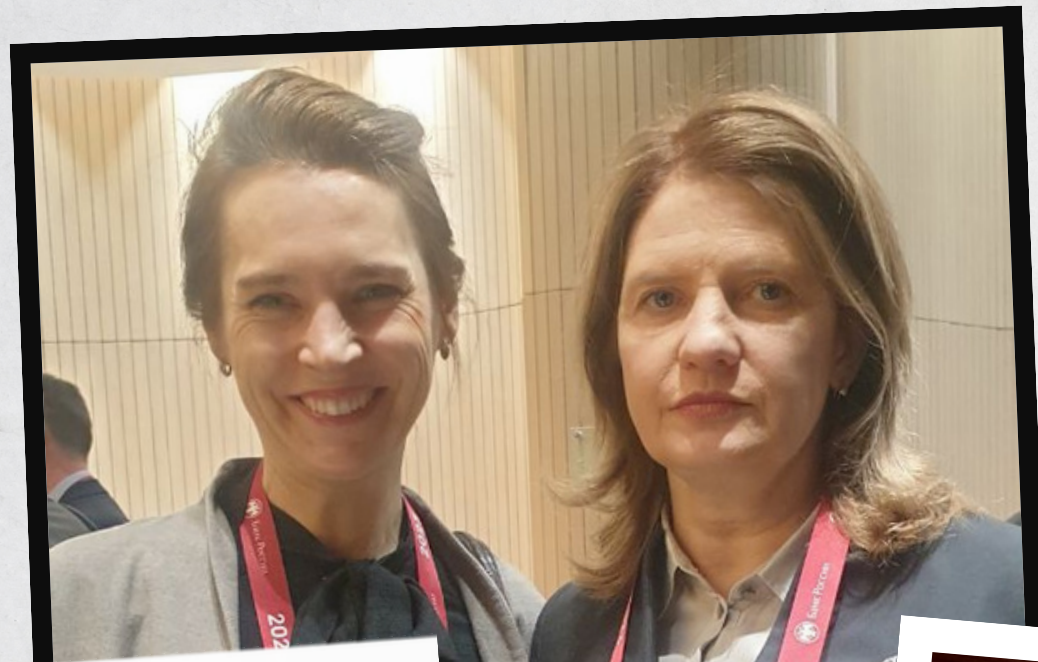
С 18-летним стажем

## **Любитель бега**









→ 13  
→ 13 A

→ 14  
→ 14 A

FILM NEGATIVE

FILM NEGATIVE

FILM NEGATIVE



# КИБЕРБЕЗОПАСНОСТЬ

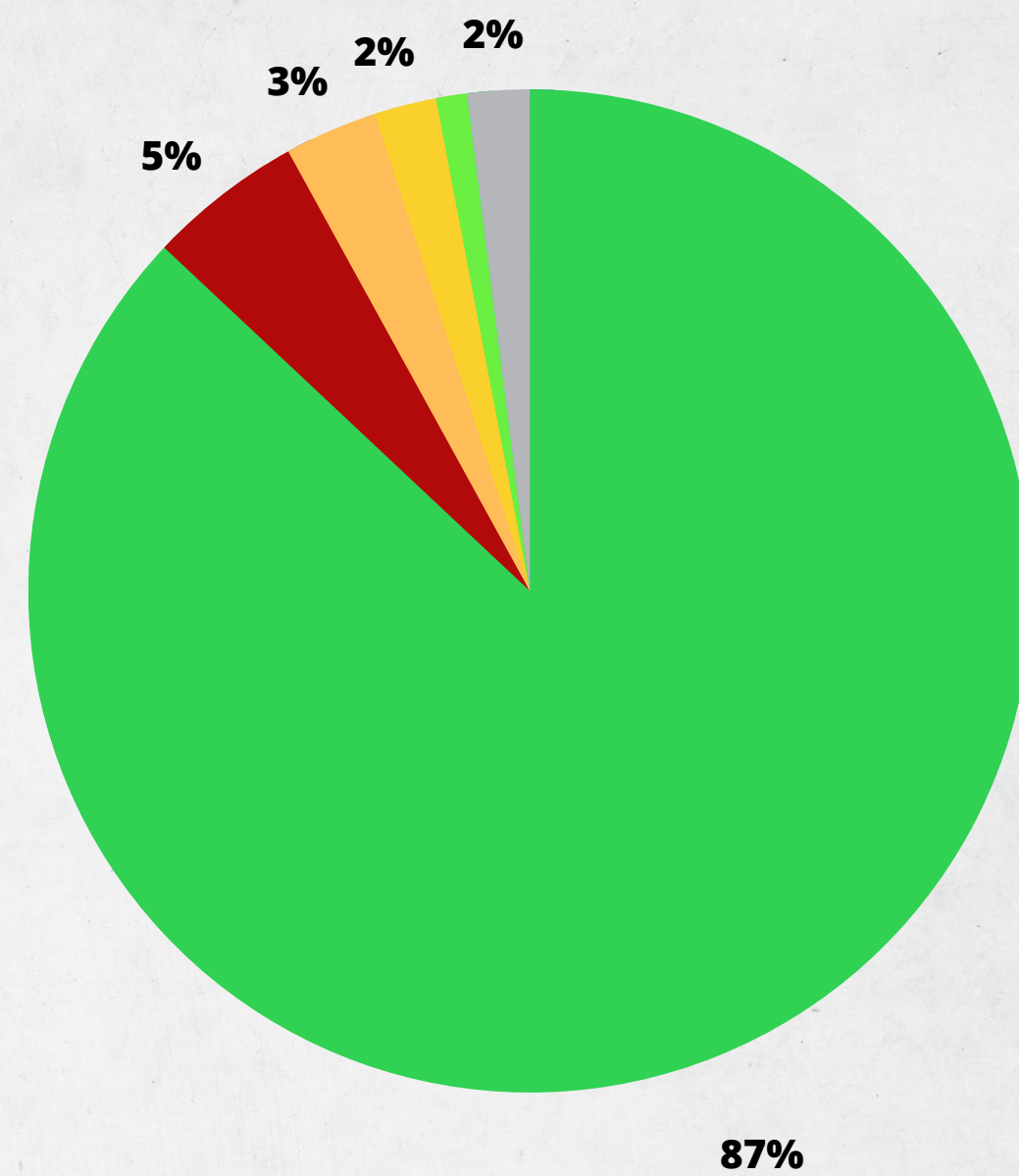
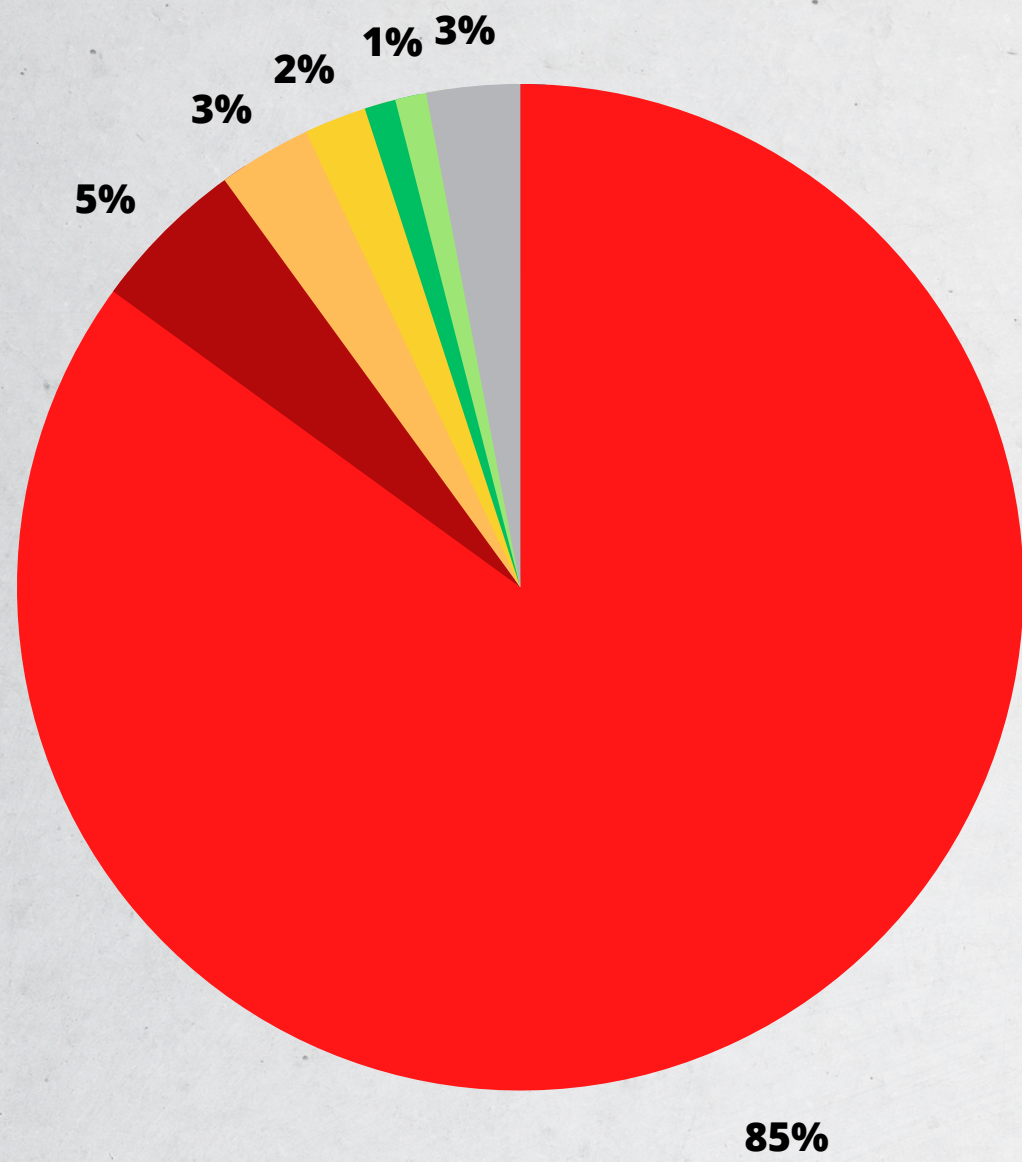
Это защита подключенных к интернету систем (оборудования, программного обеспечения и данных) от киберугроз











- Не выявлено
- Не реализовано
- Инициировано
- Взято в работу
- Определено
- Применено
- Оптимизировано
- Не применимо



# **НЕДОПУСТИМЫЕ ДЛЯ БИЗНЕСА СОБЫТИЯ**



**УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ**

**УТЕЧКА КОММЕРЧЕСКОЙ ИНФОРМАЦИИ**

**ПРОСТОЙ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ**

**КРАЖА ДЕНЕГ**

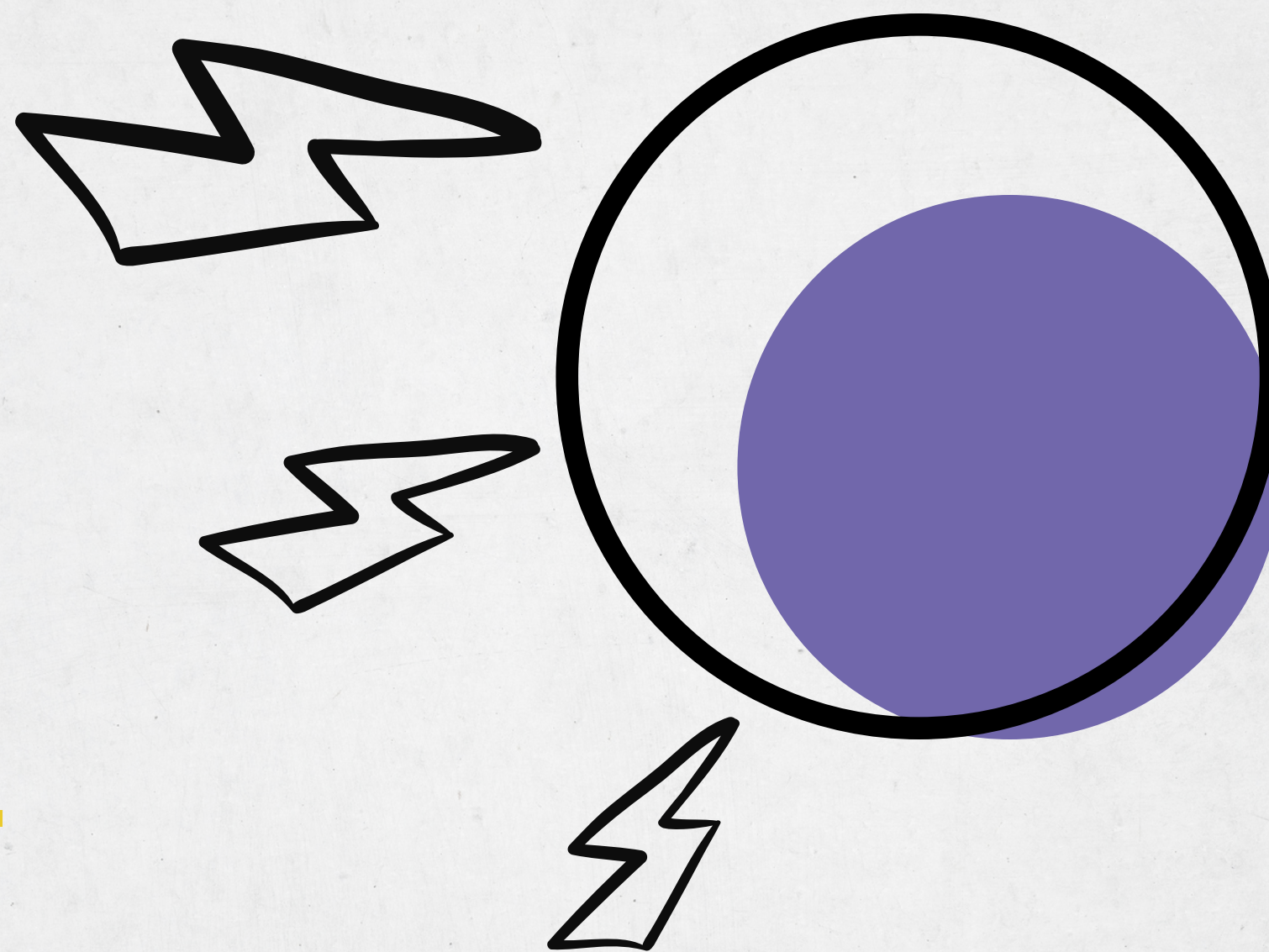
**УРОН РЕПУТАЦИИ**



# ПРИЧИНЫ КИБЕРИНЦИДЕНТОВ



**Злоумышленники**

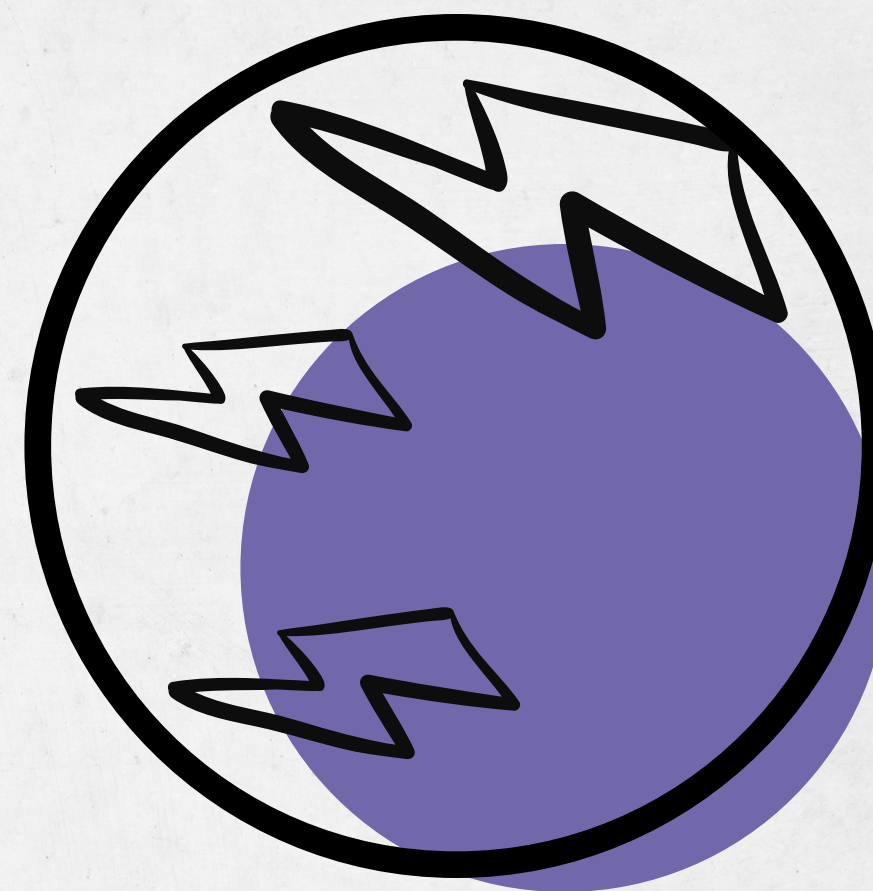




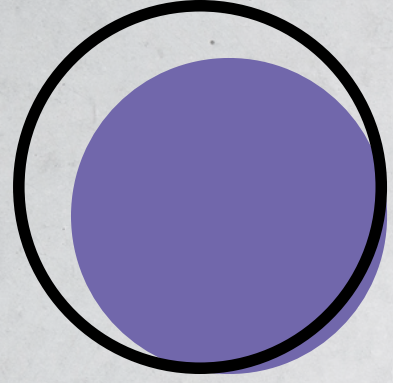
# ПРИЧИНЫ КИБЕРИНЦИДЕНТОВ



**Сотрудники**







# 14 направлений

1. Политики информационной безопасности,
2. Организация деятельности по информационной безопасности,
3. Безопасность, связанная с персоналом,
4. Менеджмент активов,
5. Управление доступом,
6. Криптография,
7. Физическая безопасность,
8. Безопасность при эксплуатации,
9. Безопасность коммуникаций,
10. Приобретение, разработка и поддержка систем,
11. Взаимоотношения с поставщиками,
12. Менеджмент инцидентов информационной безопасности,
13. Непрерывность деятельности организации,
14. Соответствие требованиям.

Определение уровня зрелости процессов по международному стандарту  
**ISO 27002:2013**



# 1

# ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## Политика информационной безопасности

Политика информационной безопасности – это совокупность правил, процедур, практических методов и руководящих принципов области ИБ, используемых организацией в своей деятельности.

Согласно отечественному стандарту ГОСТ Р ИСО/МЭК 17799-2005, политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью. В соответствии с указанным стандартом, необходимо, чтобы политика информационной безопасности предприятия как минимум включала:

- определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации

- изложение целей и принципов информационной безопасности, сформулированных руководством

- краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например, таких как:

\* соответствие законодательным требованиям и договорным обязательствам;

\* требования в отношении обучения вопросам безопасности;

\* предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

\* управление непрерывностью бизнеса;

\* ответственность за нарушения политики безопасности.

- определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности

- ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Политика информационной безопасности компании должна быть утверждена руководством, издана и доведена до сведения всех сотрудников в доступной и понятной форме.

Для того чтобы политика информационной безопасности не оставалась только «на бумаге» необходимо, чтобы она была:

- непротиворечивой – разные документы не должны по-разному описывать подходы к одному и тому же процессу обработки информации

- не запрещала необходимые действия – в таком случае неизбежные массовые нарушения приведут к дискредитации политики информационной безопасности среди пользователей

- не налагала невыполнимых обязанностей и требований.

В организации должно быть назначено лицо, ответственное за политику безопасности, отвечающее за её эффективную реализацию и

1. Краткий !!!
2. С конкретными назначением и целью
3. Написан под конкретную аудиторию и ее ожидания
4. Хорошо структурирован и оформлен
5. Неважные и большие приложения вынесены в конец документа
6. Содержит минимум сокращений и сложных терминов, присутствует их перечень
7. Не дублирует положения других документов
8. Содержит необходимые ссылки
9. Регулярно пересматривается и актуализируется
10. Соответствует шаблону, принятому в организации



# 2

## **ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ИБ**

### **1. ВНУТРЕННЯЯ ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИБ**

- Роли и обязанности по обеспечению ИБ
- Взаимодействие с органами власти
- Взаимодействие с профессиональными сообществами

### **2. МОБИЛЬНЫЕ УСТРОЙСТВА И ДИСТАНЦИОННАЯ РАБОТА**



# 3

## БЕЗОПАСНОСТЬ ПЕРСОНАЛА

### 1. ПРИ ПРИЕМЕ НА РАБОТУ

- Проверка
- Правила и условия работы

### 2. ВО ВРЕМЯ РАБОТЫ

- Обязанности руководства организации
- ! • Осведомленность, обучение и практическая подготовка (тренинги) в области ИБ
- Дисциплинарный процесс

### 3. УВОЛЬНЕНИЕ

- Прекращение или изменение трудовых обязанностей



## **3 ФИШИНГОВЫХ ПИСЬМА, КОТОРЫЕ ТОЧНО ОТКРОЮТ ВАШИ ПОЛЬЗОВАТЕЛИ**

- от Сбербанка
- От Майкрософта
- от ГосУслуг





# 4

## МЕНЕДЖМЕНТ АКТИВОВ

### 1. ОТВЕТСТВЕННОСТЬ ЗА АКТИВЫ

- Инвентаризация активов
- Владение активами
- Допустимое использование активов
- Возврат активов

### 2. КАТЕГОРИРОВАНИЕ ИНФОРМАЦИИ

- Категорирование информации
- Маркировка информации
- Обращение с активами

### 3. ОБРАЩЕНИЕ С НОСИТЕЛЯМИ ИНФОРМАЦИИ

- Управление съемными носителями информации
- Утилизация носителей информации
- Перемещение физических носителей



# 5

## УПРАВЛЕНИЕ ДОСТУПОМ

### 1. ТРЕБОВАНИЕ БИЗНЕСА ПО УПРАВЛЕНИЮ ДОСТУПОМ

- Политика управления доступом
- Доступ к сетям и сетевым сервисам

### 2. ПРОЦЕСС УПРАВЛЕНИЯ ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ

- Регистрация и отмена регистрации пользователей
- Предоставление пользователю права доступа
- Управление привилегированными правами доступа
- Процесс управления секретной аутентификационной информацией пользователей
- Пересмотр прав доступа пользователей
- Аннулирование или корректировка прав доступа



# 5

## УПРАВЛЕНИЕ ДОСТУПОМ

### 3. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

- Использование секретной аутентификационной информации

### 4. УПРАВЛЕНИЕ ДОСТУПОМ К СИСТЕМАМ И ПРИЛОЖЕНИЯМ

- Ограничение доступа к информации
- Безопасные процедуры входа в систему
- Система управления паролями
- Использование привилегированных служебных программ
- Управление доступом к исходному коду программы





# КРИПТОГРАФИЯ

## 1. СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

- Политика использования средств криптографической защиты информации
- Управление ключами



# 7

## ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

### 1. ЗОНЫ БЕЗОПАСНОСТИ

- Физический периметр безопасности
- Меры и средства контроля и управления физическим доступом
- Безопасность зданий, помещений и оборудования
- Защита от внешних угроз со стороны окружающей среды
- Работа в зонах безопасности
- Зоны погрузки и разгрузки



# 7

## ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

### 2. ОБОРУДОВАНИЕ

- Размещение и защита оборудования
- Вспомогательные услуги
- Безопасность кабельной сети
- Техническое обслуживание оборудования
- Перемещение активов
- Безопасность оборудования и активов вне помещений организации
- Безопасная утилизация или повторное использование оборудования
- Оборудование, оставленное пользователем без присмотра
- Политика "Чистого стола" и "Чистого экрана"



# 8

## БЕЗОПАСНОСТЬ ПРИ ЭКСПЛУАТАЦИИ

### 1. ЭКСПЛУАТАЦИОННЫЕ ПРОЦЕДУРЫ И ОБЯЗАННОСТИ

- Документально оформленные эксплуатационные процедуры
- Процесс управления изменениями
- Управление производительностью
- Раздел сред разработки, тестирования и эксплуатации

### 2. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

- Меры обеспечения ИБ в отношении вредоносных программ

### 3. РЕЗЕРВНОЕ КОПИРОВАНИЕ

- Резервное копирование информации

### 4. РЕГИСТРАЦИЯ И МОНИТОРИНГ

- Регистрация событий
- Защита информации регистрационных журналов
- Регистрационные журналы действий администратора и оператора
- Синхронизация часов



# 8

## **БЕЗОПАСНОСТЬ ПРИ ЭКСПЛУАТАЦИИ**

### **5. КОНТРОЛЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НАХОДЯЩЕГОСЯ В ЭКСПЛУАТАЦИИ**

- Установка ПО в эксплуатируемых системах

### **6. МЕНЕДЖМЕНТ ТЕХНИЧЕСКИХ УЯЗВИМОСТЕЙ**

- Процесс управления техническими уязвимостями
- Ограничения на установку ПО

### **7. ОСОБЕННОСТИ АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ**

- Меры обеспечения ИБ в отношении аудита информационных систем



# 9

## БЕЗОПАСНОСТЬ КОММУНИКАЦИЙ

### 1. МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ

- Меры обеспечения информационной безопасности сетей
- Безопасность сетевых сервисов
- Разделение в сетях

### 2. ПЕРЕДАЧА ИНФОРМАЦИИ

- Политики и процедуры передачи информации
- Соглашения о передаче информации
- ! • Электронный обмен сообщениями
- Соглашения о конфиденциальности или неразглашении



# 10

## ВЗАИМООТНОШЕНИЯ С ПОСТАВЩИКАМИ

### 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВО ВЗАИМООТНОШЕНИЯХ С ПОСТАВЩИКАМИ

- Политика информационной безопасности во взаимоотношениях с поставщиками
- Рассмотрение вопросов безопасности в соглашениях с поставщиками
- Цепочка поставок информационно-коммуникационных технологий

### 2. УПРАВЛЕНИЕ УСЛУГАМИ, ПРЕДОСТАВЛЯЕМЫМИ ПОСТАВЩИКОМ

- Мониторинг и анализ услуг поставщика
- Управление изменениями услуг поставщика



## 1. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

- Анализ и спецификация требований информационной безопасности
- Обеспечение безопасности прикладных сервисов, предоставляемых с использованием сетей общего пользования
- Защита транзакций прикладных сервисов

## 2. ТЕСТОВЫЕ ДАННЫЕ

- Защита тестовых данных



## 3. БЕЗОПАСНОСТЬ В ПРОЦЕССАХ РАЗРАБОТКИ И ПОДДЕРЖКИ

- Политика безопасной разработки
- Процедуры управления изменениями системы
- Техническая экспертиза приложений (прикладных программ) после изменений операционной платформы
- Ограничения на изменения пакетов программ
- Принципы безопасного проектирования систем
- Безопасная среда разработки
- Разработка с использованием аутсорсинга
- Тестирование безопасности систем
- Приемо-сдаточные испытания системы





- Обязанности и процедуры
- Сообщения о событиях информационной безопасности
- Сообщение о недостатках информационной безопасности
- Оценка и принятие решений в отношении событий ИБ
- Реагирование на инциденты информационной безопасности
- Извлечение уроков из инцидентов информационной безопасности
- Сбор свидетельств



# НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ

## 1. НЕПРЕРЫВНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Планирование непрерывности информационной безопасности
- Реализация непрерывности информационной безопасности
- Проверка, анализ и оценивание непрерывности информационной безопасности

## 2. РЕЗЕРВИРОВАНИЕ ОБОРУДОВАНИЯ

- Доступность средств обработки информации



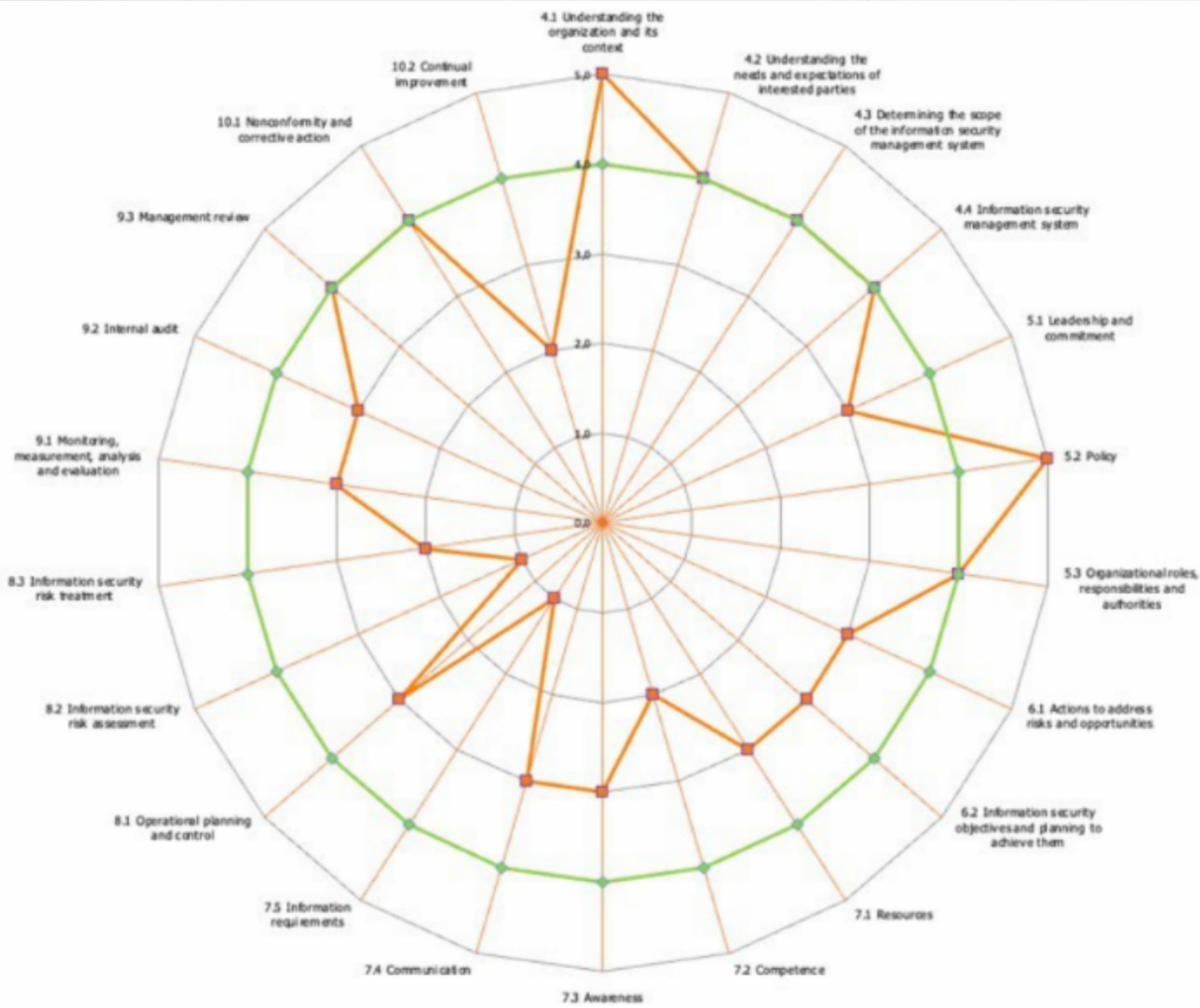
## 1. СООТВЕТСТВИЕ ПРАВОВЫМ И ДОГОВОРНЫМ ТРЕБОВАНИЯМ

- Идентификация применимых законодательных и договорных требований
- Права на интеллектуальную собственность
- Защита записей
- Конфиденциальность и защита персональных данных
- регулирование криптографических мер обеспечения информационной безопасности

## 2. ПРОВЕРКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Независимая проверка информационной безопасности
- Соответствие политикам и стандартам безопасности
- Анализ технического соответствия





- 5 - Оптимизировано
- 4 - Применено
- 3 - Определено
- 2 - Взято в работу
- 1 - Инициировано
- 0 - Не реализовано

—■— текущий уровень  
—■— плановый уровень





# КОД ИБ ЭКСПЕРТ

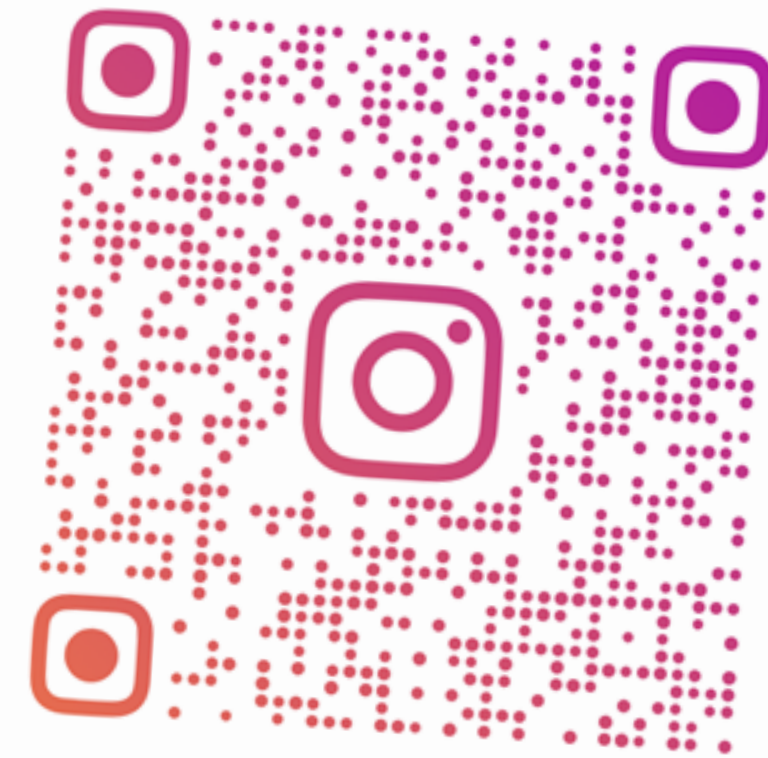
ОПЫТ ТОПОВЫХ CISO  
ДЛЯ БЕЗОПАСНОСТИ ВАШЕГО БИЗНЕСА

## СПАСИБО ЗА ВНИМАНИЕ

**ОЛЬГА ПОЗДНЯК**  
ПРОДЮСЕР КОД ИБ

✉ [OLGA@CODEIB.RU](mailto:OLGA@CODEIB.RU)

📩 [POZDNYAKOLGA](#)



**POZDNYAKOLGA**





**УЗНАТЬ БОЛЬШЕ**







**КОД ИБ**  
**ЭКСПЕРТ**

ОПЫТ ТОПОВЫХ CISO  
ДЛЯ БЕЗОПАСНОСТИ ВАШЕГО БИЗНЕСА

# НАСТАВНИЧЕСТВО

## ПО ЗАЩИТЕ БИЗНЕСА ОТ КИБЕРУГРОЗ

Уровень угроз и сложность задач растут так быстро, что не всегда у ваших специалистов есть достаточно времени, чтобы осваивать ранее непрофильные для себя темы






**КОД ИБ  
ЭКСПЕРТ**

ОПЫТ ТОПОВЫХ CISO  
ДЛЯ БЕЗОПАСНОСТИ ВАШЕГО БИЗНЕСА

**ЗАПИШИТЕСЬ НА  
БЕСПЛАТНУЮ ДИАГНОСТИКУ**

**ОЛЬГА ПОЗДНЯК  
ПРОДЮСЕР КОД ИБ**

 [OLGA@CODEIB.RU](mailto:OLGA@CODEIB.RU)

 [POZDNYAKOLGA](https://t.me/POZDNYAKOLGA)

