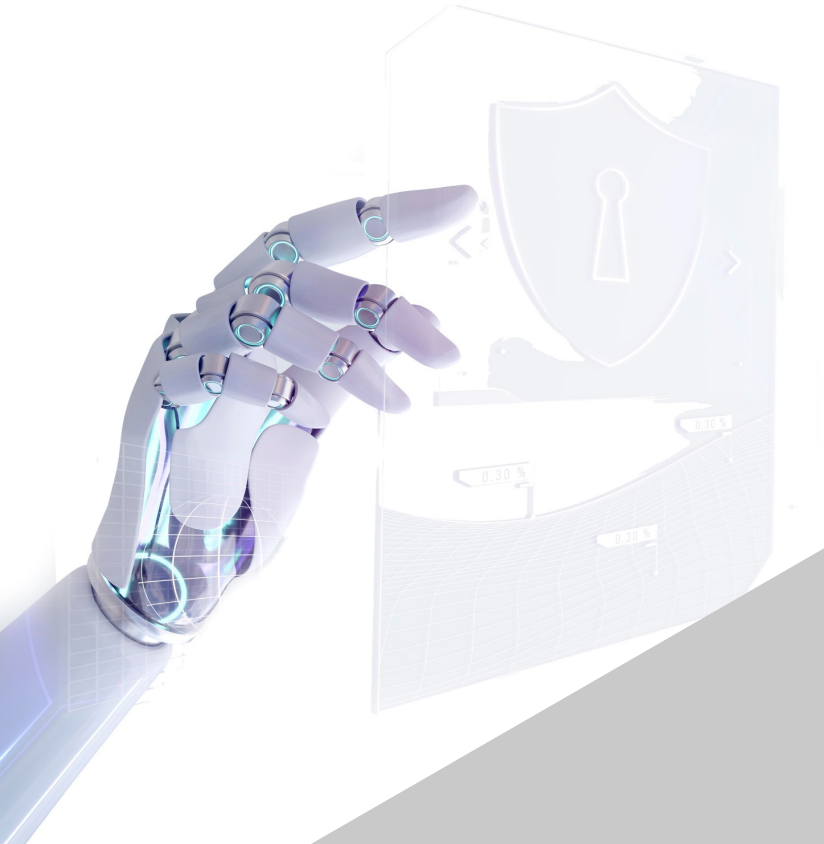
СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

Кибербезопасность

Что это значит для CEO?



РАЗДЕЛЫ КИБЕРБЕЗОПАСНОСТИ

- УПРАВЛЕНИЕ ДОСТУПОМ
- УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ
- ОБУЧЕНИЕ РАБОТНИКОВ СЛУЖБЫ КБ
- ВЗАИМОДЕЙСТВИЕ С ТРЕТЬИМИ ЛИЦАМИ
- СТРАТЕГИЯ КБ
- РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД
- ОТЧЕТНОСТЬ И МЕТРИКИ
- КОМПЛАЕНС КБ
- ТЕСТЫ НА ПРОНИКНОВЕНИЕ
- ОРГАНИЗАЦИОННАЯ СТРУКТУРА
- СЕТЕВАЯ БЕЗОПАСНОСТЬ
- МОНИТОРИНГ КБ
- РАССЛЕДОВАНИЯ
- УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ АКТИВАМИ
- УПРАВЛЕНИЕ ИНЦИДЕНТАМИ КБ
- БЕЗОПАСНОСТЬ КОНЕЧНЫХ УСТРОЙСТВ
- БЕЗОПАСНОСТЬ РАЗРАБОТКИ
- БЕЗАОПАСНОСТЬ ДАННЫХ
- ПОЛИТИКИ И СТАНДАРТЫ
- КУЛЬТУРА КБ
- УПРАВЛЕНИЕ КОМПЛАЕНСОМ
- КОММУНИКАЦИИ В ОБЛАСТИ КБ
- НЕПРЕРЫВНОСТЬ БИЗНЕСА
- АРХИТЕКТУРА КБ
- ЗАЩИТА ПРИЛОЖЕНИЙ В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ

26 ПРОТИВОДЕЙСТВИЕ КИБЕРМОШЕННИЧЕСТВУ

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

5 УРОВНЕЙ КИБЕРБЕЗОПАСНОСТИ

- **Уровень 1**

Вопрос 1. Разработана и внедрена политика использования паролей и политика предоставления доступа к информационным системам Общества.

Вопрос 2. Для учетных записей, наделенных правами администратора, в системах разработаны отдельные политики.

Вопрос 3. Процесс управления доступом формализован (может не выполняться в соответствии с политикой).

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

5 УРОВНЕЙ КИБЕРБЕЗОПАСНОСТИ

- **Уровень 2**

Вопрос 1. Внедрены политики управления доступом (возможно, различные по различным ИТ системам).
Вопрос 2. За каждым процессом (создание, обновление, блокировка, восстановление) закреплен владелец (возможно, список таких владельцев формально не определен).
Вопрос 3. Учетные данные хранятся и передаются в защищенном режиме.
Вопрос 4. Удаленный доступ к сети Общества контролируется (как минимум эпизодически).
Вопрос 5. При необходимости проводится мониторинг и составление отчетов по аутентификации пользователей.
Вопрос 6. Процесс согласования доступа автоматизирован (как минимум частично).

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

5 УРОВНЕЙ КИБЕРБЕЗОПАСНОСТИ

- **Уровень 3**

Вопрос 1. Политика по управлению доступом в информационные системы, парольная политика разработаны, внедрены и действуют для всех подразделений Общества (для основных критичных систем).
Вопрос 2. Политики и стандарты управления доступом в Обществе четко определены, задокументированы и распространены среди работников Общества.
Вопрос 3. Аудит для привилегированных пользователей выполняется на регулярной основе (может не включать в рассмотрение неперсонифицированные учетные записи).
Вопрос 4. Запросы на предоставление доступа согласованы в соответствии с политиками по управлению доступом, внедренными в Обществе, и доступ к необходимым ресурсам выдается только после согласования.

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

5 УРОВНЕЙ КИБЕРБЕЗОПАСНОСТИ

- **Уровень 4**

Вопрос 1. Процесс согласования доступа в системы автоматизирован, при этом работники Общества имеют возможность выполнять проверку выполнения процесса управления доступом во время обработки заявки на предоставление доступа.
Вопрос 2. Процессы создания учетных записей, обновления, удаления/отключения автоматизированы. Ручное вмешательство требуется только в исключительных случаях.
Вопрос 3. Политики и стандарты управления доступом и парольными политиками пересматриваются и обновляются в соответствии с лучшими практиками. Разработаны и внедрены политики и стандарты по управлению учетными записями, привилегированными учетными записями, неперсонифицированными и т.д. Внедрены политики по

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

5 УРОВНЕЙ КИБЕРБЕЗОПАСНОСТИ

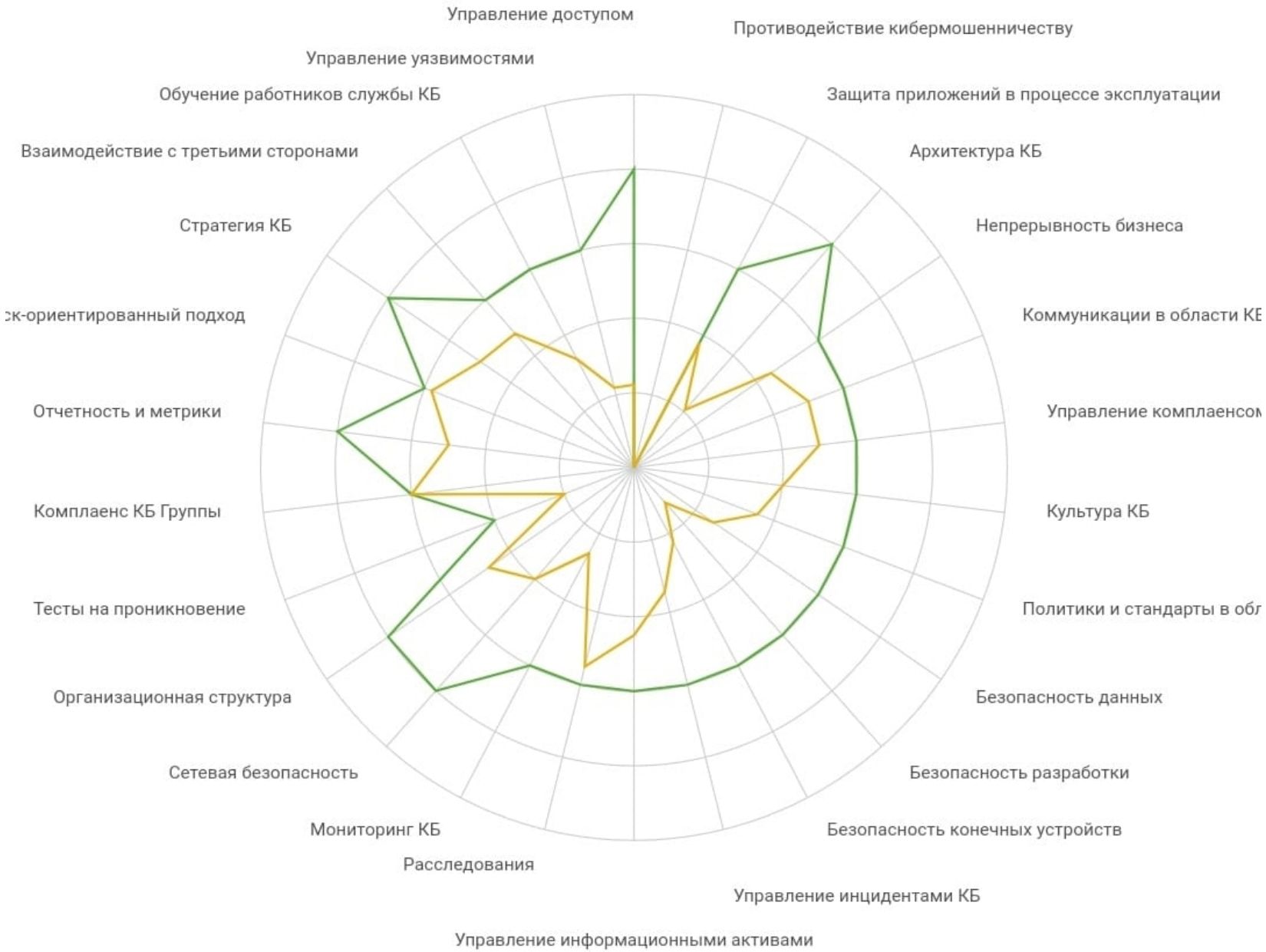
- **Уровень 5**

Вопрос 1. Для всех идентифицированных событий КБ, связанных с управлением доступом, настроены соответствующие уведомления и на основании таких событий выполняются действия по их последующему анализу.

Вопрос 2. Мониторинг и процессы идентификации пользователей автоматизированы. Системы проверки подлинности и авторизации используются для формирования оповещений и принятия соответствующих мер воздействия после обнаружения подозрительного использования учетных записей.

Вопрос 3. Общество продолжает расширять перечень внедренных ролей для дополнительных ИТ систем и согласовывать процессы, основанные на потребностях бизнеса. Роли и процессы автоматически обновляются на регулярной основе.

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО



СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

ДОКУМЕНТАЛЬНАЯ БЕЗОПАСНОСТЬ VS РЕАЛЬНАЯ

- ТЕСТ НА ПРОНИКНОВЕНИЕ (ПЕНТЕСТ)
- АНТИВИРУС
- МЕЖСЕТЕВОЙ ЭКРАН
- DDOS И CWAF ЗАЩИТА
- ВЕРСИОННОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ
- НАЛИЧИЕ УЯЗВИМОСТЕЙ, ИХ УРОВНИ И СРОКИ УСТРАНЕНИЯ

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

РЕСУРСЫ ДЛЯ ПРОВЕРКИ УЯЗВИМОСТЕЙ

- https://bdu.fstec.ru/vul
- https://cve.mitre.org/cve/
- https://threats.kaspersky.com/ru/
- https://vulners.com/search?query=order:published%20type:cve

- **РАССЫЛКА ФИНЦЕРТ**

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

ПЕРСОНАЛ И ФИШИНГ

ДО ОБУЧЕНИЯ

ПОСЛЕ ОБУЧЕНИЯ

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

ЧЕК-ЛИСТ

- НАЗНАЧЕН CISO, ЕСТЬ СВИДЕТЕЛЬСТВА, ПОДТВЕРЖДАЮЩИЕ ЕГО КВАЛИФИКАЦИЮ
- РАЗРАБОТАН, УТВЕРЖДЕН ПЛАН РАЗВИТИЯ КБ
- РЕГУЛЯРНО ПРОВОДИТСЯ ОБУЧЕНИЕ ПЕРСОНАЛА И УЧЕБНЫЕ ФИШИНГОВЫЕ АТАКИ
- В ПЕРИМЕТРЕ СЕТЕЙ ОТСУТСТВУЮТ УЯЗВИМОСТИ УРОВНЯ КРИТИЧЕСКИЙ, ВЫСОКИЙ С ДАТЫ ПУБЛИКАЦИИ СВЕДЕНИЙ ОБ УЯЗВИМОСТИ БОЛЕЕ 30 ДНЕЙ
- НА АРМ И СЕРВЕРАХ ОТСУТСТВУЮТ УЯЗВИМОСТИ УРОВНЯ КРИТИЧЕСКИЙ С ДАТЫ ПУБЛИКАЦИИ ОБНОВЛЕНИЯ 90 ДНЕЙ
- АНТИВИРУС С ЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ УСТАНОВЛЕНА НА АРМ (НЕ МЕНЕЕ 95%)
- ОТСУТСВУЮТ УЧЕТНЫЕ ЗАПИСИ С ПАРОЛЕМ, НЕ СООТВЕСТВУЮЩИМ ТИПОВЫМ ТРЕБОВАНИЯМ
- РЕАЛИЗОВАН ЦЕНТРАЛИЗОВАНЫЙ СБОР СОБЫТИЙ И ИНЦИДЕНТОВ КБ
- НА ПЕРИМЕТРЕ СЕТЕЙ УСТАНОВЛЕНЫ МЕЖСЕТЕВЫЕ ЭКРАНЫ
- ОБЕСПЕЧЕНА ПОЛОЖИТЕЛЬНАЯ ДИНАМИКА УРОВНЯ КБ
- МЕРОПРИЯТИ ПЛАНА КБ ВЫПОЛНЕНЫ В СРОК, ОБЕСПЕЧЕНО ПРЕДОСТАВЛЕНИЕ ОТЧЕТНОСТИ НЕ РЕЖЕ 1 РАЗА В МЕСЯЦ
- ИНФОРМАЦИЯ ОБО ВСЕХ КРИТИЧЕСКИХ ИНЦИДЕНТАХ КБ И ХОДЕ РАССЛЕДОВАНИЯ СВОЕВРЕМЕННО ПРЕДОСТАВЛЯЮТСЯ ГД И СД
- СД РАССМАТРИВАЕТ ВОПРОС КБ НА РЕГУЛЯРНОЙ ОСНОВЕ

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

СТАТУС
РЕГИСТРАТОРСКОЕ ОБЩЕСТВО

Спасибо за внимание!