softline SOFL

КИБЕРЧЕКАП

Проведем диагностику кибербезопасности и
определим план киберлечения

от 2 недель до 1 месяца

НЕМНОГО О НАС

>15
лет на рынке кибербезопасности

>200
сервисов и услуг для защиты бизнеса

>1000
компаний под нашей защитой

>300
профессионалов в команде

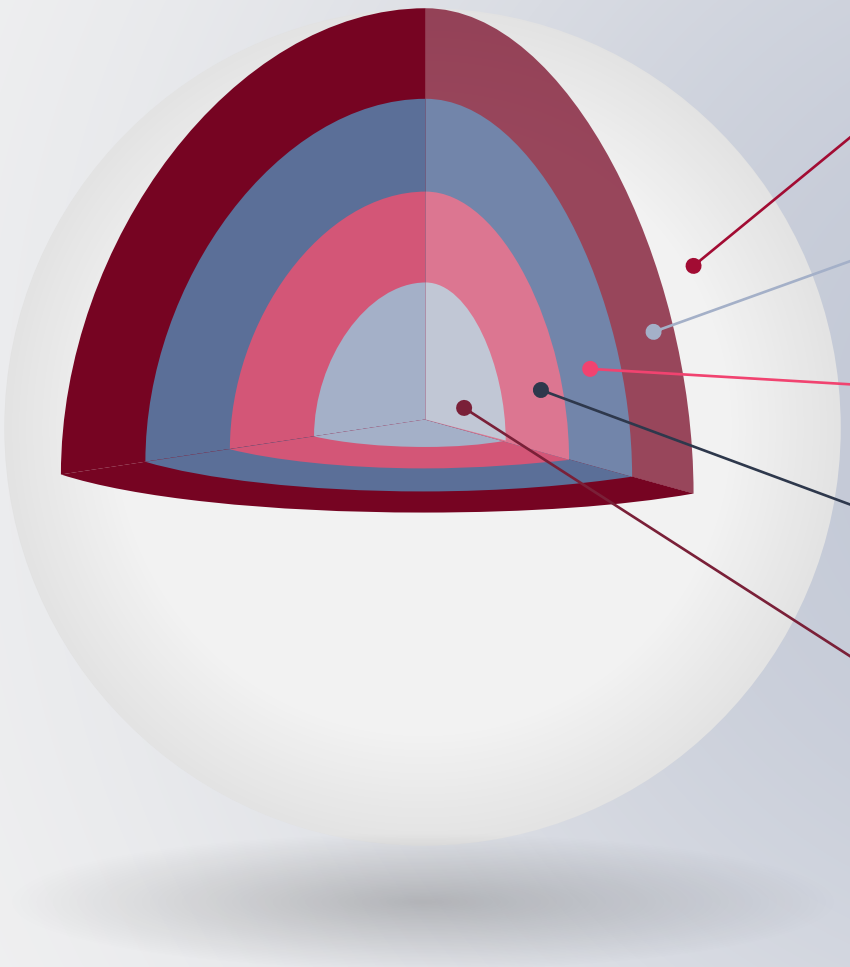
Проекты в сфере кибербезопасности в разных отраслях: ритейл, операторы связи, финансовая отрасль, строительная индустрия, облачные провайдеры, информационные технологии

Auchan RETAIL РОССИЯ · ГТЛК · zetta GROUP · ТРАСТ БАНК НЕПРОФИЛЬНЫХ АКТИВОВ · TAGLEX · MC Bank Rus a subsidiary of Mitsubishi Corporation

ТМК · SBI Bank Strategic Business Innovator · ДОДО ПИЦЦА · синара банк · газэнерго банк · Шоколадница кофе. завтраки. еда

КИБЕРЧЕКАП

Бизнес – это организм, а безопасность – это иммунитет, не позволяющий этому организму сбоить



ЭКСПЕРТНОЕ МНЕНИЕ

Аномалии, выявляемые при аудите у наших заказчиков

Топ уязвимостей, эксплуатируемых на практике

Сведения об инцидентах по России и миру

Трендовые угрозы – что нас ждет в 2026

Аномалии, выявляемые при аудите у наших заказчиков

Внедрили сканер уязвимостей
Да, но:

- Покрытие неполное
- Сканирование завершается с ошибками – траблшутинг не выполняется
- Десятки тысяч строк в отчете – не понятно, как агрегировать
- SLA либо вообще отсутствует, либо есть, но не контролируется
- Процесс управления обновлениями не выстроен

Внедрили систему PAM
Да, но:

- Покрыто лишь 30% ресурсов / учетных записей
- Нет понимания: что именно покрывать, кто такие привилегированные пользователи, надо ли контрагентов пускать через PAM, надо ли покрывать Linux-сервера?
- А что с резервным доступом, если PAM «устанет»?

Внедрили антивирусное средство
Да, но:

- Покрыты только хосты Windows
- Отключен ряд модулей, базы не обновляются
- Некорректные настройки несут риски отказа в обслуживании, потере контроля над хостами
- Большое количество ошибок– траблшутинг не выполняется

Внедрили средство защиты от DDoS
Да, но:

- Правила выставлены по умолчанию
- Существенная доля операций ручного переключения трафика
- Планы BCP и DRP не учитывают сценарий реагирования на DDoS-атаки
- Обучение специалистов не проводится

Внедрили NGFW
Да, но:

- Доступ к интернету никак не ограничен
- SSL инспекция не работает
- Песочница не настроена
- Везде ANY-ANY

Внедрили резервное копирование
Да, но:

- Покрытие неполное
- Политика копирования – единая для всех систем, без учета бизнес-контекста
- В момент восстановления выясняется, что копия не консистентна

Аномалии, выявляемые при аудите у наших заказчиков

Управление доступом

- Учетные записи с пустыми паролями и с паролями в Description
- Использование учетных данных по умолчанию
- Использование слабых паролей (*Например, компания называется Ромашка. Пароли будут «Ландыши001!» или «Ромашка2025*)»
- Отсутствие блокировки уволенных работников
- Избыточные права доступа к системам

Удаленный доступ

- «Зоопарк» агентов со стороны работников ИТ
- Профили пользователей в VPN-системе не разделены по категориям доступа
- Контроль доступа к терминальным серверам реализован фрагментарно

Безопасность ИИ

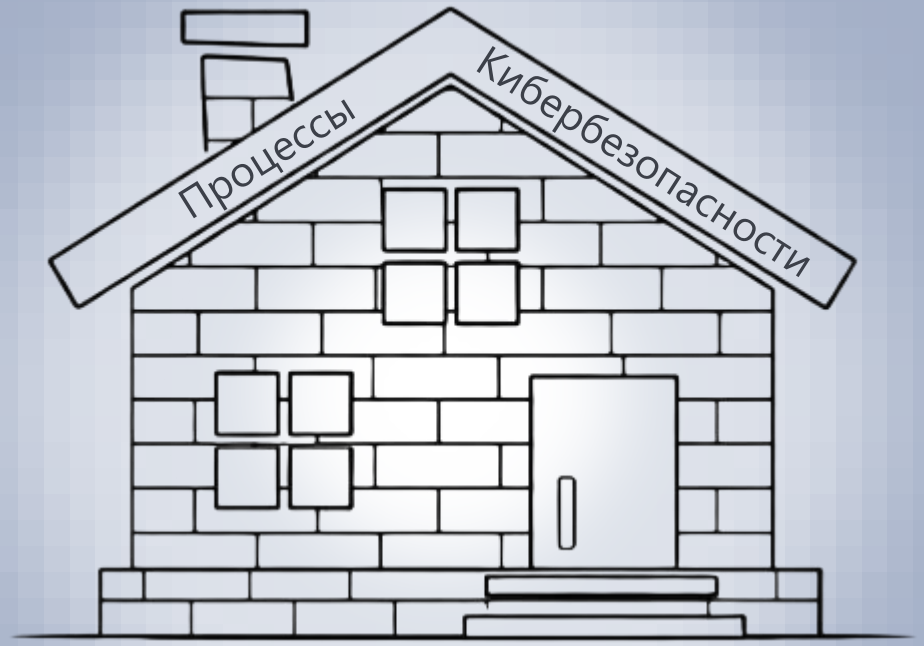
- Специфичные для ИИ-систем угрозы и векторы атак не проанализированы (отравление данных, промпт-инъекция и галлюцинация модели)
- Требования по защите не учтены на стадии разработки и не применяются на стадии эксплуатации

Персональные данные

- Заявляемые в Политике цели обработки ПДн не совпадают с целями, указанными в уведомлении в РКН
- Некорректные формы сбора ПДн на сайте
- Использование иностранных сервисов (например, Google Analytics), подпадающих под нарушение требований по локализации ПДн
- ПДн передаются третьим лицам без согласия субъектов ПДн

Только средства защиты

Комплексный подход к защите



Сами по себе средства защиты не обеспечивают достаточный уровень безопасности — только тщательно выстроенные процессы обеспечивают реальную защиту

ТОП УЯЗВИМОСТЕЙ, ЭКСПЛУАТИРУЕМЫХ НА ПРАКТИКЕ

ПОСЛЕДСТВИЯ:

- Контроль над доменом
- Управление ключевыми ИС и серверами
- Компрометация резервных копий
- Полный доступ в критичные сегменты сети (сеть безопасности, АСУ ТП и пр.)
- Эскалация привилегий до уровня администраторов домена
- Построение скрытого долгосрочного контроля над инфраструктурой

Несоблюдение гигиены КБ = Системное ослабление кибериммунитета

ПРИМЕРЫ ИНЦИДЕНТОВ ПО РОССИИ И МИРУ

АВИАКОМПАНИЯ
Лето 2025

Утечка, уничтожение:
атака через поставщика, слабые пароли, известные уязвимости, аномалии в архитектуре безопасности сети

НЕФТЯНАЯ КОМПАНИЯ
Весна 2025

Шифрование:
фишинг, аномалии в архитектуре безопасности сети, аномалии в конфигурациях СЗИ

БАНК
Зима 2024

Шифрование:
фишинг, аномалии в архитектуре безопасности сети, аномалии в конфигурациях СЗИ

ФИНАНСОВЫЕ ОРГАНИЗАЦИИ
Лето 2024

DDoS:
аномалии в конфигурациях СЗИ

ИТ-КОМПАНИЯ
Зима 2024

Утечка:
компрометация УЗ, отсутствие 2FA, отсутствие аудита привилегированных УЗ

ПРОВАЙДЕР УСЛУГ
Лето 2024

Утечка:
Использование УЗ уволенного работника, компрометация действующих УЗ, отсутствие 2FA, аномалии в архитектуре безопасности сети

РИТЕЙЛЕР
Зима 2025

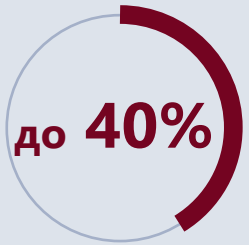
Шифрование:
атака через поставщика, отсутствие контроля доступа поставщика и блокировки УЗ уволенных работников

РАЗРАБОТЧИК ПО
Лето 2025

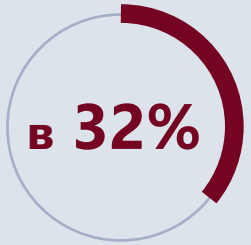
Утечка:
известные уязвимости, конфигурации по умолчанию

ТРЕНДОВЫЕ УГРОЗЫ – ЧТО НАС ЖДЕТ В 2026

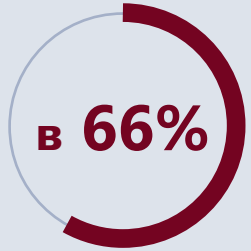
атак используется социальная инженерия, фишинг



атак – это утечка корпоративных УЗ



атак эксплуатируются известные уязвимости



атак используется вредоносное ПО

Ключевой тренд – использование ИИ:

- Еще больше правдоподобия при фишинговых атаках (вишинг, дипфейк, фейкбосс)
- Автоматизация сбора информации в процессе OSINT
- Генерация релевантных паролей
- Ускорение выявления и эксплуатации уязвимостей

Иные тренды:

- Рост государственных кибероопераций, «хактивистов» и сотрудничества хакерских группировок на фоне геополитической ситуации
- Поставщики и цепочка поставок - как основной вектор атаки
- Интеграция ИИ в корпоративные системы создает новые векторы проникновения в инфраструктуру
- Вайб-кодинг - приведет к появлению большого количества функционального, но небезопасного кода

- ✓ Тестирование на проникновение
- ✓ Требования регулятора
- ✓ Обучение персонала
- ✓ Зрелость процессов КБ
- ✓ Контроль средств защиты
- ✓ Харденинг

...

ПРОБЛЕМАТИКА

Иллюзия защищенности

Компания уверена в собственном «киберздоровье», пока не случается острое состояние (инцидент), наносящее ущерб жизненно важным функциям бизнеса

Отсутствие системной диагностики

Фрагментарные проверки безопасности не дают полной картины возможных патологий

Пандемия киберугроз

Злоумышленники раз за разом эксплуатируют одни и те же векторы, используя слабость базового иммунитета

Необходим подход, обеспечивающий комплексную диагностику и план киберлечения: Киберчекап

ЧТО ВХОДИТ В КИБЕРЧЕКАП

Чекап системы менеджмента КБ

Проверка ключевых процессов кибербезопасности

Комплаенс чекап

Проверка соответствия применимым требованиям регуляторов (ФСТЭК России, ФСБ России, РКН, ЦБ РФ)

Технический чекап

Проверка настроек безопасности критичных областей и аудит учетных записей

Чекап периметра

Внешнее тестирование на проникновение

Чекап персонала

Проведение фишинговой рассылки для работников

Чекап бренда

Защита бренда в интернете и обнаружение внешних цифровых угроз


Чекап бренда
Чекап системы менеджмента КБ
Чекап персонала
Комплаенс чекап
Технический чекап
Чекап периметра

Чекап системы менеджмента КБ

Проверка ключевых процессов кибербезопасности

- Сроки: от 2 недель

1. Обследование ключевых процессов кибербезопасности:

База
- управление доступом
- управление уязвимостями
- защита конечных точек
- сетевая безопасность
- управление инцидентами КБ
- восстановление после инцидентов

Опция
- обеспечение безопасности при взаимодействии с третьими сторонами
- управление жизненным циклом ИТ-активов
- управление рисками КБ
- безопасность ИИ-систем
- повышение осведомленности в области КБ
- безопасная разработка ПО
- *другое*

2. Выявление недопустимых для бизнеса событий кибербезопасности и определение приоритетов защиты

3. Разработка приоритизированного плана развития КБ

- ✓ Оценка зрелости процессов и мер обеспечения КБ в соответствии с общепризнанными международными практиками (ISO/IEC 27001, CIS18 и пр.)
- ✓ Выявление «слабых мест» в системе менеджмента КБ
- ✓ Приоритизация мероприятий КБ с учетом профиля рисков

1. Аудит безопасности базовых инфраструктурных сервисов
(AD DC, AD CS WSUS и пр.)

2. Аудит настроек безопасности на границе сети:
- правил межсетевого экранирования на периметре
- безопасности конфигураций сетевого оборудования
- правил удаленного доступа

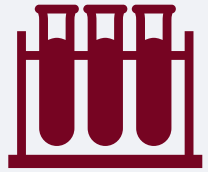
3. Аудит привилегированных и пользовательских учетных записей службы каталогов

4. Аудит настроек и политик средства защиты от вредоносного ПО
- аудит серверной части: настройки, политики, отчеты
- аудит клиентской части: задачи, статусы управляемых устройств проверка покрытия

5. Выдача рекомендаций по реализации Quick Wins

Технический чекап

Проверка настроек безопасности и аудит учетных записей



- Сроки: ~ 2 недели

- ✓ Технический аудит критичных областей инфраструктуры
- ✓ Контроль выполнения базового минимума требований кибербезопасности
- ✓ Понятный план «Quick Wins» в части обеспечения технической безопасности

1. Проверка соответствия применимым регуляторным требованиям
   - ПДн (152-ФЗ)
   - КИИ (187-ФЗ)
   - 250 указ Президента РФ
   - 117 приказ ФСТЭК России
   - ГОСТ Р 57580

   Опция

2. Проверка договоров с подрядчиками в части требований КБ

   Опция

3. Формирование набора рекомендаций по достижению соответствия применимым регуляторным требованиям

Комплаенс чекап

Проверка соответствия применимым требованиям регуляторов

- Сроки: ~ 2 недели

- ✓ Проверка полноты и корректности исполнения регуляторных требований
- ✓ Снижение комплаенс-риска и вероятности регуляторных штрафов
- ✓ Уверенность в соблюдении законодательства в области КБ и повышение доверия клиентов и партнеров

1. Согласование целевой группы работников, сроков и тем для рассылки
2. Проведение фишинговой рассылки для работников
3. Выявление наиболее уязвимого персонала и формирование рекомендаций по дальнейшему обучению

Далее:

4. Использование платформы обучения и проведение регулярных мероприятий по повышению осведомленности в области кибербезопасности

Выстраивание киберкультуры

Чекап персонала

Проведение фишинговой рассылки для работников

- Сроки: ~ 2 недели

✓ Проверка навыков КБ работников в реальной жизни

✓ Определение направлений для дальнейшей работы:

- приоритетных тем для обучения
- приоритетных работников/групп работников

1. Сбор информации о Компании и ее цифровых активах

2. Выявление цифровых угроз для бренда Компании в общедоступных источниках

3. Анализ и верификация обнаруженных угроз с помощью команды экспертов

4. Формирование отчета, содержащего выявленные цифровые угрозы по разным направлениям

Чекап бренда

CYBERDEF – защита бренда в интернете и обнаружение внешних цифровых угроз

- Сроки: ~ 2 недели

Ключевые разделы по аномалиям:

- ✓ домены - выявление фишинговых ресурсов
- ✓ услуги - выявление объявлений о нелегальных услугах, затрагивающих интересы Заказчика
- ✓ утечки - выявление в сети Интернет информации ограниченного доступа
- ✓ бренд - выявление неправомерного использования товарного знака
- ✓ менеджмент - выявление поддельных профилей топ-менеджмента

Чекап периметра

Тестирование на проникновение

1. Согласование границ работ, обсуждение допущений к проводимым работам, получение доступов
2. Определение методики выполнения работ
3. Анализ защищенности сетевого периметра
4. Формирование отчета с описанием наиболее критичных уязвимостей, а так же оценкой уровня защищённости тестируемых объектов:
   - описание выявленных уязвимостей, места их обнаружения, уровни критичности
   - описание метода обнаружения и эксплуатации уязвимости
   - рекомендации по устранению найденных проблем

- Сроки: ~ 1 месяц

✓ Оценка защищенности инфраструктуры сертифицированными экспертами

✓ Понятный план «Quick Wins» в части обеспечения безопасности опубликованных приложений

ЧТО УЖЕ СЛУЧИЛОСЬ?

Чекап бренда

КАК ДЕЛА СЕЙЧАС?

Чекап системы менеджмента КБ

Комплаенс чекап

Технический чекап

Чекап периметра

Чекап персонала

ЧТО ДЕЛАТЬ В БУДУЩЕМ?

План развития:

- Quick Wins
- Комплексное развитие КБ

ПЛАН КИБЕРЛЕЧЕНИЯ

Результаты Киберчекапа:

- ✓ Несовершенства ключевых процессов КБ
- ✓ Несоответствия требованиям регуляторов
- ✓ Аномалии настроек безопасности на границе сети
- ✓ Аномалии службы каталогов
- ✓ Критичные уязвимости на периметре, веб-ресурсах
- ✓ Уязвимости персонала
- ✓ Внешние цифровые угрозы для бренда

Стратегия развития КБ

рекомендации по реализации гигиенического минимума КБ и мероприятий комплексного долгосрочного развития КБ с учетом недопустимых событий и трендовых рисков КБ

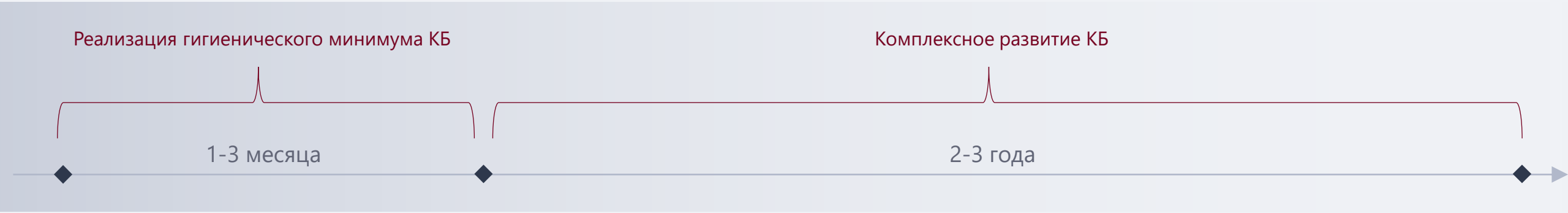
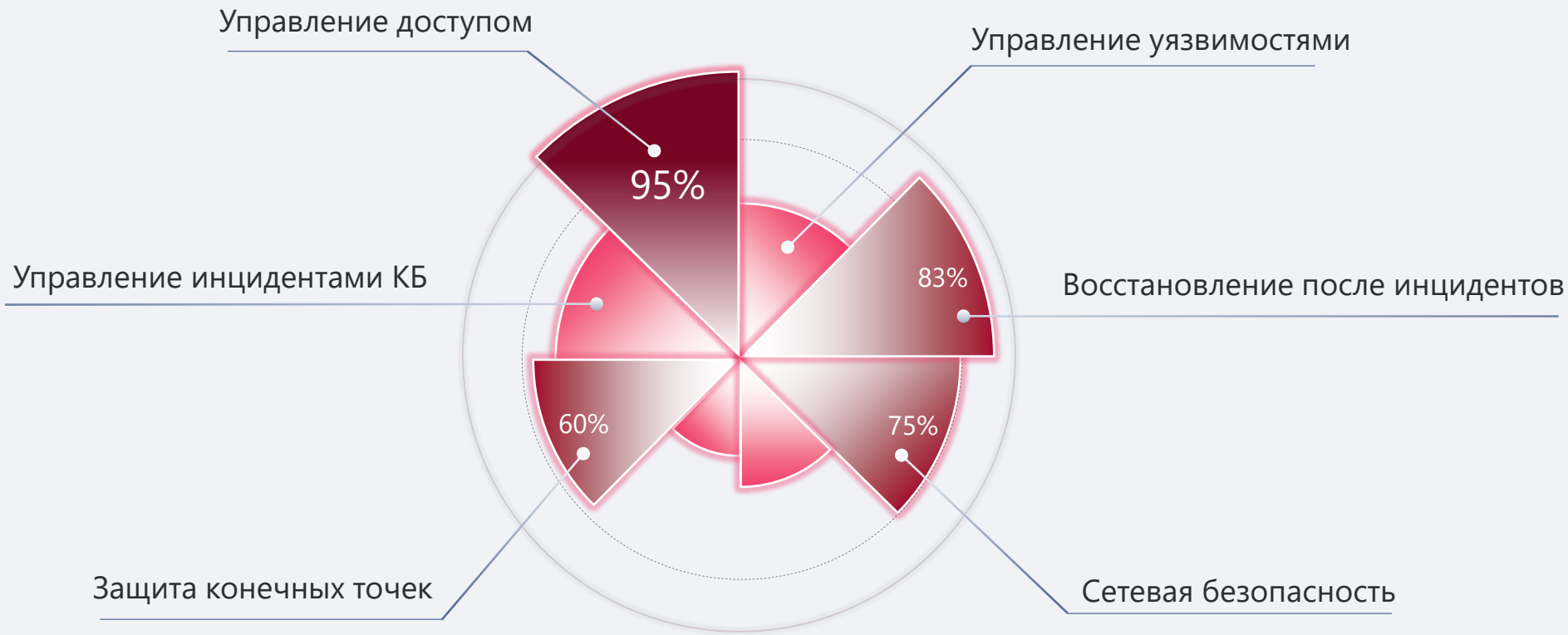


ДИАГРАММА ЗРЕЛОСТИ ПРОЦЕССОВ КИБЕРБЕЗОПАСНОСТИ

Пример

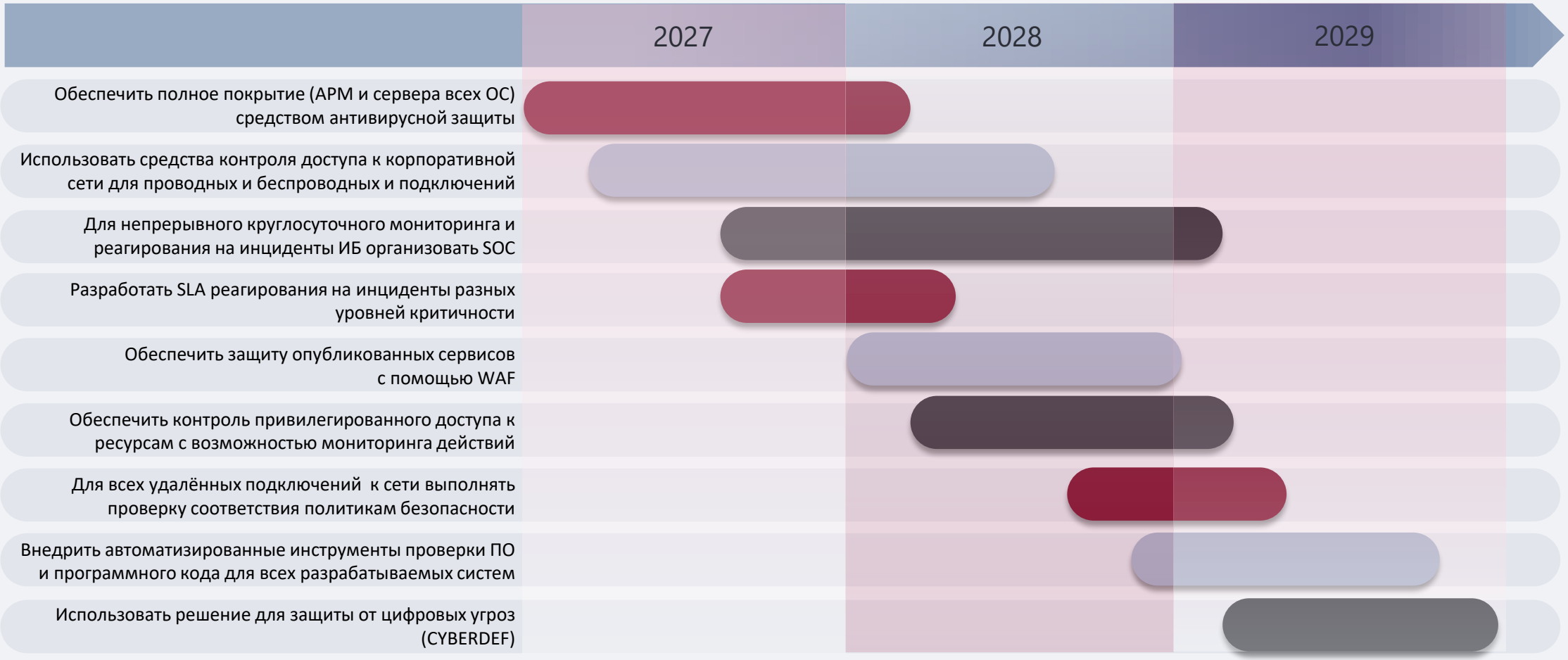


ПРОГРЕСС РОСТА УРОВНЯ ЗРЕЛОСТИ КИБЕРБЕЗОПАСНОСТИ

Пример

ДОРОЖНАЯ КАРТА РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ

Пример



ОСТАВЛЯЕМ КАК ЕСТЬ

Принимаем риски:

- Подрыв репутации
- Финансовый ущерб
- Регуляторные штрафы
- Остановка производства

СТРАТЕГИЧЕСКИЙ ПОДХОД

- Сформирована стратегия долгосрочного развития КБ с учетом целей бизнеса
- Проводится регулярный киберчекап
- Снижена вероятность недопустимых событий
- Выполнены базовые меры КБ

Есть вопросы?

Для дополнительной консультации или уточнения деталей проекта вы можете связаться с персональным аккаунт-менеджером Softline или с руководителем Центра компетенций по консалтингу ИБ Юлией Смолиной

Y.Smolina@softline.com