DevSecOps в управлении рисками ИБ

Шмаков Илья Станиславович
AppSec Teamlead & ISO
ГК ЛАНИТ

WHOA!

Салют 👋,
Более 8 лет в сфере ИБ продуктовой разработке.
Специализируюсь на защищённости CI/CD, DevSecOps, Risk Analysis.

- Являюсь лидером сообщества FinDevSecOps для fintech рынка РФ
- Преподаю курс по DevSecOps для Security Champion
- Подготовил первый в РФ хакатон по DevSecOps
- Спроектировал AML концепт на базе Multisig с учетом эскроу-схемы подписи в OpenVZ
- Проектировал архитектуру СБП, процессинговой платформы, POS-терминалов и т.д.
- Проектирую и внедряю сервисы защищенности поставок, а также AppSec Toolchain
- Опыт работы в fintech более 4-ех лет (НФО, Банки, УпрКомп, СпецДеп, Деп)

Почему классно быть в DevSecOps?

DevSecOps (Development, Security & Operations) – разработка ПО, направлена на устранение сработок УЯЗ, из-за которых могут возникнуть киберпреступления, отказы в обслуживании, утечки и другое.

В направлении рассматривается как команда подходит к разработке, какие недостатки архитектуры, частоту ошибок при тестировании и строятся критерии качества ИБ. В конечном счете всё направлено на обеспечение безопасности и защиты продукта в разработке, включая мониторинг.

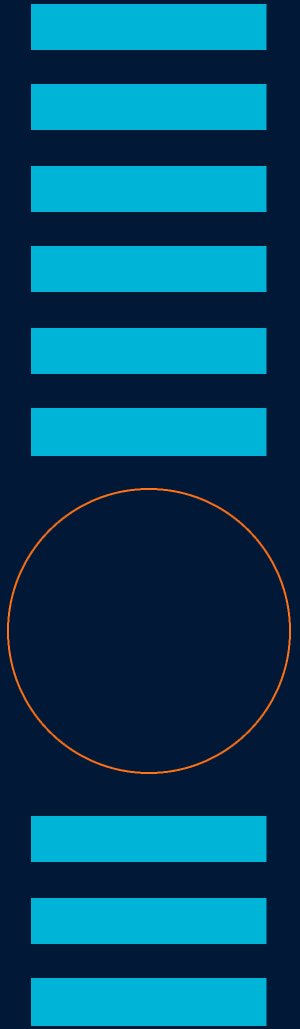
Тезисы DevSecOps

- **DevSecOps** повышает уровень безопасности поставок, - для команд это отсутствие влияния на Time-To-Market, оптимизация, устранение уязвимостей, снижение рисков ИБ,

- **Quality Gate** - контроль безопасного непрерывного процесса поставки изменений с устранением уязвимостей,
Основная цель - защита продуктов, мониторинг поставок, снижение вероятности возникновения инцидента и прямого/ побочного «урона»,

- **Смысл Quality Gate** в превентивном контроле Pipeline, Shift-Left подходе, автоматизации проверок тестирования ИБ,

- **Критерии Quality Gate** снижают риски ИБ, имеющиеся уязвимости и обеспечивают безопасность поставок в продукционную среду не блокируя бизнес.



«Начинается»

Skill matrix

Компетенции и интересные темы
для тебя и твоего роста

Sic Parvis Magna

Т-профиль

Область знаний

Охват экспертной оценки

Hard скиллы

Применимость навыков и областей знаний для бизнеса

Область навыков

Возможность адаптироваться и углубиться в предметную область

Soft скиллы

комплекс умений, связанных с личностными качествами человека

Компетенции

feat Денис Макрушин CPO продуктовой разработки ИБ в ЯД

01

Risk Analysis

В разделе рассматривается риск анализ и проектное управление в котором необходимо правильное взаимодействие, коммуникация

Что угрожает информационной безопасности?

- Наступление недопустимого события
- Нарушение работоспособности структурных подразделений
- Нарушение технологических процессов
- Срыв своевременного решения задач ИБ
- Отсутствие мер и средств защиты информации
- Не декларированные возможности
- Недостатки архитектуры и технических решений
- Отсутствие оценки рисков ИБ
- Низкая приоритезация исполнения мер ИБ
- Отказ от реализации практик ИБ и т.д.

Виды ответственности за правонарушения в сфере информационной безопасности

Уголовная ответственность – за наиболее важные, охраняемые уголовным законом интересы в сфере информации

Административная ответственность – назначается органом или должностным лицом, наделенным соответствующими полномочиями в виде административного наказания лицу, совершившему правонарушение.

Гражданская ответственность – договорная и внедоговорная (из причинения вреда) ответственность, связанная с имущественными интересами.

Дисциплинарная ответственность – возникает при нарушениях в сфере информационной безопасности при осуществлении ими рудовых функций.

Риск и угроза ИБ

Риск - это вероятность, возможность возникновения реализации угрозы, которая может эксплуатироваться посредством имеющейся уязвимости, недостатка.

Информационная безопасность оценивает риск ИБ исходя из бизнес-потребности, ценности продукта, услуги и сферы работы.

Для определения риска ИБ необходимо понимать угрозы, приводящие к ущербу деятельности бизнеса.

Угроза ИБ – это потенциально возможное действие /бездействие, событие, которое может привести к нанесению основного, либо побочного ущерба владельцу, - влияющая на конфиденциальность, целостность, доступность.

Угрозы могут быть, как пример: воздействие регуляторных требований на деятельность бизнеса, утечка конфиденциальной информации, приводящей к потерям активов /пассивов, киберпреступление, связанное с потерей финансовых показателей и так далее.

Должная осмотрительность

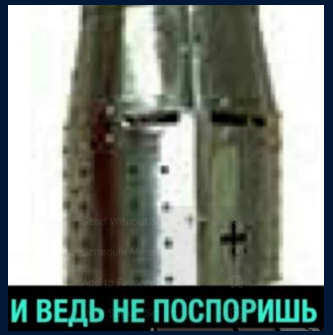
Должная осмотрительность представляет собой комплекс мер, направленных на проверку действительности событий.

Сам термин и формат предполагает действия от НК на проверку контрагентов, но в нашем случае мы рассматриваем взаимодействие с людьми и воздействием человеческого фактора.

То есть это именно то, что отделяет корректную реакцию на действия злоумышленников от поведения под воздействием влияния.

При ее отсутствии могут быть понесены серьёзные последствия для лица и организации, которые в дальнейшем приведут к последствиям, намного менее благоприятным чем первоначальное воздействие.

Методы воздействия на риск



При оценке угроз мы понимаем, какой вытекающий риск ИБ.

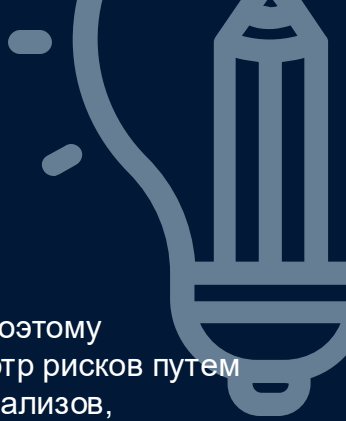
То есть каким образом он реализовывается и, вследствие, мы понимаем методы воздействия, используемые нами.

Для ценности поставляемой услуги, продукта мы учитываем количественные, качественные показатели степени влияния, критичности риска.

Риски ИБ описывают последствия для бизнеса исходя из угрозы и, следовательно, мы оцениваем степень вероятности возникновения инцидента, а далее снижаем мерами противодействия.

- **Отказ**,
- **Принятие**, - можем оценить, понять последствия и мы можем с ним работать из-за более выгодных условий, либо из-за отсутствия альтернативных решений,
- **Минимизация**, - меры, которые предпринимаем для того, чтобы степень критичности риска снизился до приемлемого, либо далее целевого,
- **Делегирование**, - аналог мер, который рассматриваем как снятие с себя ответственности, либо полное устранение воздействия риска на нас путем передачи на аутсорсинг, страхование.

И зачем нам риски?



Благодаря опыту и аналитическому мышлению мы понимаем, как реализует риск, следовательно это позволяет нам развить компетенцию в ИБ.

Понимание риска, угрозы и приведенной классификации предоставляет нам прикладное значение.

Результат реализации – это событие, которое оказывает финансовое, репутационное, регуляторное, судебное последствие как прямо, так и косвенно для владельца, который может быть как нарушение целостности, доступности, конфиденциальности, но последствия могут иметь разную составляющую.

Реализация риска изменчива, поэтому необходимо проводить пересмотр рисков путем проведения дополнительных анализов, как по истечению времени завершения активности, так и в условиях, если эта активность затрагивается смежными инициативами.

При анализе рисков информационной безопасности, следует опираться на активности бизнеса и научиться с ним договариваться о том, что мы можем проработать альтернативными методами, это позволит избежать незапланированных расходов на оборудование, ПО, меры и средства ИБ.

Классификация рисков ИБ

1. Регуляторное несоответствие	• нарушение законодательства в области регулятора (пример: ЦБ), включая отраслевого (пример: ФСТЭК, ЦБ); • нарушение нормативных требований (пример: РКН, НКЦКИ, ФинЦЕРТ); • нарушение частных федеральных законов, нормативно-правовых актов (пример: ПДн по 152 ФЗ) и т. д.
2. Недостатки проектного управления, управления менеджментом	• несоблюдение требований эксплуатации систем; • недостаточный уровень контроля (технического, организационного); • низкий уровень осведомлённости, уведомлений об активностях, коммуникаций и т. д.
3. Киберпреступления, утечки и иные криминальные активности	• утечки конфиденциальной, инсайдерской, ограниченного доступа информации; • киберпреступления, совершённые третьими лицами в отношении информационных систем владельца бизнеса, используемых сервисов, персональных устройств клиентов бизнеса, внешних партнёров; • саботаж, сговор с целью нарушения и получения личной выгоды и т. д.
4. Нехватка или недоступность работников, неспособность обеспечения операционной деятельности бизнеса	• недостаток квалифицированного персонала; • отсутствие вендоров; • геополитический кризис и т. д.
5. Недоступность и сбои поставки, работы продукта, оказания услуг	• несвоевременная реализация защитных мер ИБ; • низкий уровень технического администрирования; • сбои в работе информационных систем.

Степень и уровень критичности риска

При проработке риска мы можем использовать оценку в следующем виде:

- LOW, - не оказывает влияния на бизнес,
- MEDIUM, - средняя величина влияния с которой мы можем работать и на которую мы можем повлиять в моменте времени,
- HIGH, - окажет весомое влияние на деятельность бизнеса,
- CRITICAL, - окажет значительное влияние вплоть до приостановки деятельности бизнеса

Степень критичности рассматриваем от пользовательской истории, которая появляется при изменении, добавлении процесса внутри продукта, услуги.

Анализ событий, данных, условий, которые появляются и влияют на деятельность бизнеса негативно, где мы указываем на это бизнесу описав последствия, которые могут возникнуть для нас.

Что мы можем сделать?

- Установить контекст: определить область оценки, внешние, внутренние факторы,
- Произвести оценку рисков ИБ: анализ, сравнительную оценку выявленных рисков, оценку остаточного риска,
- Принять методы работы с рисками (минимизация, делегирование, принятие, отказ),
- Установить мониторинг, а также последующую оценку пересмотра рисков ИБ,
- Произвести стандартизацию на базе DMAIC.

Зачем нам вникать в это?

Бизнес ориентируется на систему создания ценности услуг Service Value System. То есть это бизнес-решение, которое является обслуживаемым и способным к развитию.

Следовательно, после проверки гипотезы и доказательства, что продукт становится жизнеспособным получается развитие цепочки создания ценности. Вследствие бизнес понимает, как можно его развить, монетизировать.

Shift-Left - встраивание ИБ на стадиях планирования, разработки и концепции дизайна продукта, которая подразумевает разработку технического решения.

Концепция ориентируется на требованиях ИБ, проверку и контроль на стадии формирования жизненного цикла ПО. То есть, при данном методе мы предвидим и оцениваем риски, которые могут повлиять на бюджет, возникновение инцидентов.

Типовые ошибки

55%

45%

Управление, документирование и операции

- Отсутствие приоритизации уязвимостей при разработке
- Компетенции
- «Для нас это не является риском»

STLC, Quality Gate/ Security Gate

- Отсутствие механизмов приравнивания уязвимостей к дефектам кода
- Пороговые критерии качества кода

Основы концепта

Требования ИБ

Понятные, актуальные, конкретные и адаптированные под особенности каждой команды и проекта.

Мотивация

SecAwareness

Обучить команды писать и поддерживать код, разбирать актуальные задачи команд, с примерами безопасной реализации.

DMAIC

Определить, стандартизировать и внедрить – базис предикатора ценности

Имеет 5 взаимосвязанных этапов:

- Определение,
- Измерение,
- Анализ,
- Совершенствование,
- Контроль.

DMAIC

При обеспечении информационной безопасности придерживаемся принципа DMAIC, который помогает постепенно улучшать и оптимизировать процессы разработки, проектирования и поддержания текущего статуса безопасности организации.

Каждый этап имеет суммарный результат, основанный на информации и данных, сгенерированных на предыдущих этапах, и повторяющийся в течение нескольких итераций позволяющий достигать поставленных целей безопасности структурно и последовательно.

DMAIC цикл

Цель Кайзен события

- Найти корневые причины
- Разрешить корневые причины
- Поддерживать непрерывные улучшения
- Предотвратить повторение проблем

Результаты Кайзен события

- Факты о проблеме
- Устранение потерь
- Стандартизация
- Решенная проблема и улучшение

А что если делать правильно?

- Исследование проблемы: определение деталей, которые могут позволить предотвратить возможные дефекты,
- Описание ключевых причин фактами: сбор данных, статистики, - основанная на конкретных обоснованных доказательствах,
- Удовлетворение клиента: где ценность, поставляемая клиенту, приводит к повышению спроса, использования продукта, услуги,
- Аналитика путем определения проблемы через ее поиск, вследствие обнаружения причин появления, а далее устранение,
- Проверка результатов – повторение цикла определения, устранения и оптимизации процесса,
- Стандартизация процесса.

И как же с этим работать?

При формировании требований превентивно повлиять и оценить предполагаемые уязвимости, недостатки, дефекты исходя из риск анализа.

Shift-Left является подходом проверки безопасности на самых ранних стадиях проекта и позволяет повлиять на уязвимости, безопасность, когда продукт формируется по функциональным, не функциональным требованиям.

Смысл в том, что мы интегрируем требования ИБ и оцениваем актуальность мер на ранних стадиях, где сами меры могут делать допущения, а также акценты на наиболее важных и насущных вещах.

Данные допущения, либо ограничения могут быть не учтены менеджерами и специалистами, кто смотрит в сторону наибольшей скорости поставки ценности по Time-to-Market и монетизации.

Эффективность управления рисками УЯЗ

Анализ

Взаимосвязь данных с бизнес-ценностью продукта и устранение УЯЗ

Ценность

Корректировка на ценность конечному пользователю для ИБ, как условия работы с рисками

Критерии качества

Технологический контроль кода и конфигов, недостатков архитектуры

Условия

Учет выполнения мер минимизации уровня High и Critical в препрод (PRE-условия) и/или с последующим контролем (POST-условия)

Инкремент

Управление мажором и минором в поставках

Метрики

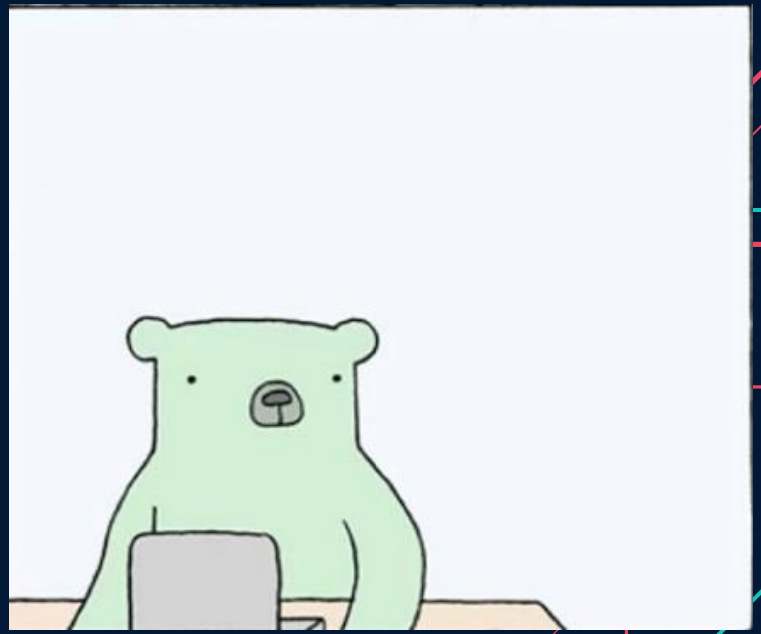
Software Testing LifeCycle

>185,000

Среднее число атак в РФ за 2024 год

“This is a quote, words full of wisdom that someone important said and can make the reader get inspired”

— Someone Famous



02

DevSecOps

В разделе рассматривается риск анализ и проектное управление в котором необходимо правильное взаимодействие, коммуникация

Какие стадии и кто участвует?

6 фаз жизненного цикла разработки приложения

АНАЛИЗ	ДИЗАЙН	РАЗРАБОТКА	ТЕСТИРОВАНИЕ	РАЗВЕРТЫВАНИЕ	ПОДДЕРЖКА
Владелец продукта Менеджер проекта Бизнес-аналитик Технический директор (CTO)	Системный архитектор Дизайнер UX/UI	Front-end-разработчик Back-end-разработчик	Архитектор решений Инженер по качеству (QA) Тестировщик DevOps	Администратор данных DevOps	Пользователи Тестировщики Менеджеры поддержки

DASA DevOps

DevOps Agile Skills Association (DASA) — это сообщество, которое развивает навыки DevOps и Agile.

DASA была основана в апреле 2016 года. Сообщество обеспечивает сертификацию компетенций DevOps.

DASA это про создание команд из T-образного профиля компетенций, обладающих навыками для самостоятельного создания, обслуживания систем.

Области знаний

- DASA позволяет расти и становиться автономнее.
- DASA учитывает развитие акцентируясь на T-профиле с уклоном в безопасность, риски и Compliance, что в свою очередь позволяет нам проще взаимодействовать с командами разработки, бизнеса.
- Появляется возможность беспрепятственного взаимодействия с командами, а также акцентирование внимание на повышение ценности продукта, soft-скиллов и обучения команд со стороны безопасности продукта.

Подход DevSecOps и DASA DevOps

Циклы разработки ПО должны включать меры по информационной безопасности исходя из определений рисков при подготовке продуктов.

Таким образом подход встраивается в культуру команды, тем более мы понимаем, как она работает.

DevSecOps и DASA раскрывает полноту используемых процессов и инструментов внутри команды.

Таким образом мы можем проконтролировать, обеспечить бесперебойность, снизить риски и обезопасить быструю поставку ценности продукта, которая будет исключать уязвимости в коде приравнивания их к дефектам кода, на что и будут обращать внимание команды разработки.

Процесс DevSecOps ориентирован на организацию помощи командам в эффективном устранении рисков ИБ, уязвимостей, недостатков архитектуры и соответствия регуляторным требованиям.

Таким образом информационная безопасность включается в каждый этап разработки ПО посредством Shift-Left.

Проблема в безопасной безопасности?

DevOps направлен на оптимизацию процесса масштабирования продукта и его поддержания, — ускорить выпуск новых версий без потери качества.

DevSecOps рассматривают как замедляющий фактор, который откладывает поставку.

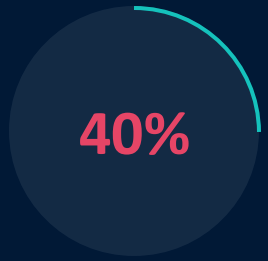
В результате на выходе может быть получена уязвимая поставка, на исправление которой тратится большое количество ресурсов.

Задача DevSecOps осуществить контроль цикла DevOps, не затрагивания TTM.

DevSecOps не вносит фундаментальные изменения в DevOps, но позволяет превентивно предусматривать их и рассматривать в виде допущений/ограничений.

DevSecOps позволяет отойти от проверки готовой поставки на соответствие политикам в пользу внедрения механизмов превентивного контроля кода на УЯЗ.

COMMON MISTAKES



Управление, DocOps

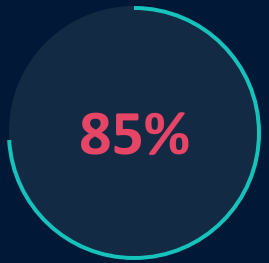
Отсутствие приоритезации и triage при разработке.

Компетенции

STLC, QG/ SG

Отсутствие механизмов приравнивания уязвимостей к дефектам кода.

Пороговый QG



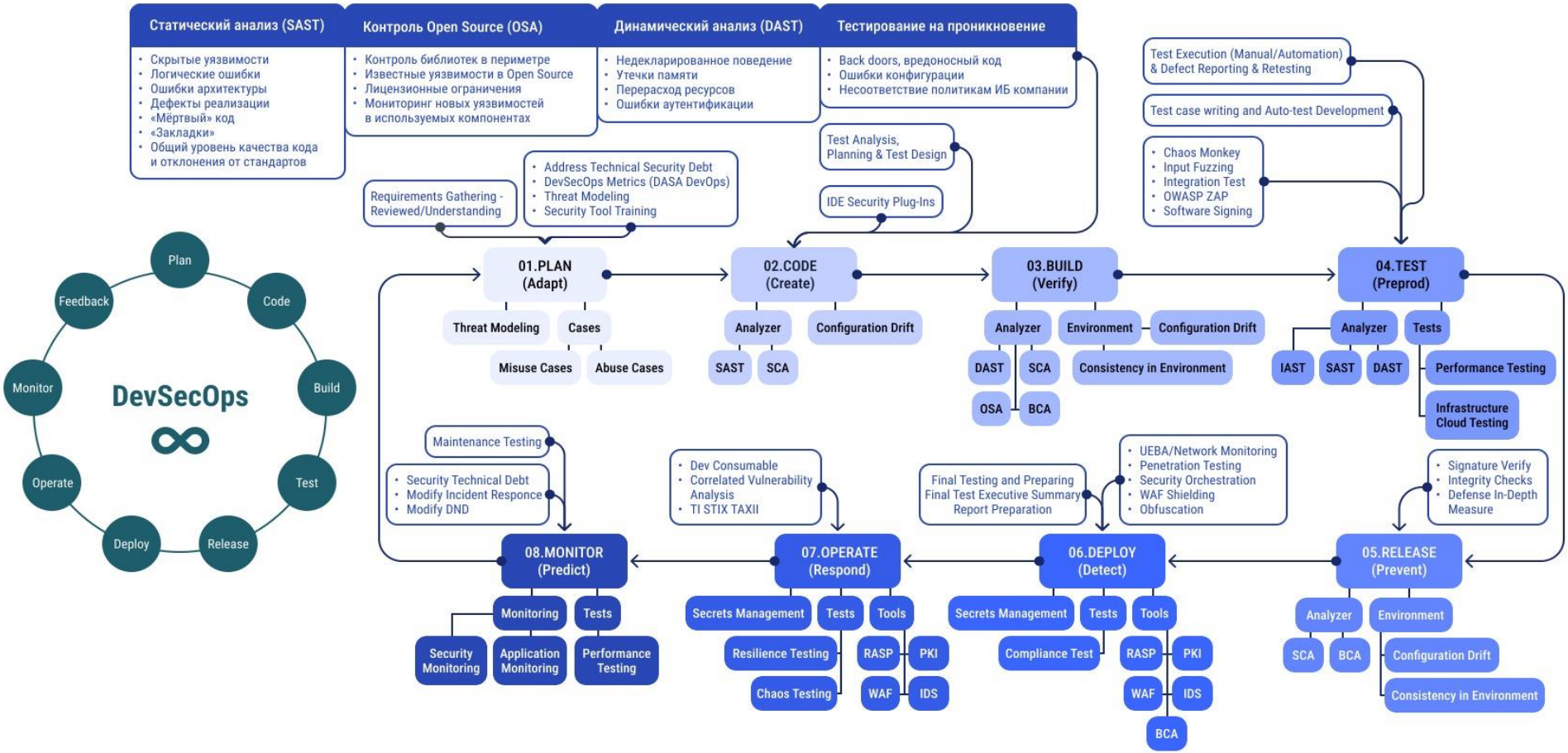
DocOps,

«Для нас это не является риском»

«Нет бюджета»

«Добавим в технический долг»

Secure Software Development Life Cycle (SDLC) / DevSecOps ToolChain



Принципы DevSecOps

Agile

Сотрудничество всех не в рамках SLA для команд разработки, эксплуатации и безопасности.

За безопасность продукта несут ответственность все

SecAwareness

Стандартизация и автоматизация.

Обучение паттернам безопасной разработки и внедрения политик ИБ

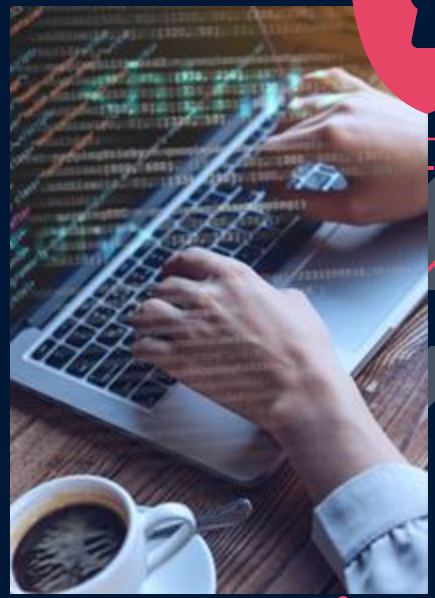
Сопровождение

Измерение, мониторинг, отчетность, реализация.

Метрики, критерии качества, STLC

Почему это важно для бизнеса?

И какой для нас профит?



Зачем «вот это вот всё» нам?

- Для внедрения в команды, понимания бизнеса, понимания механизмов воздействия,
- Для устранения недостатков на стадии проектирования и формирования матрицы бизнес-требований разработки функциональных/не функциональных фичей,
- Внедрения автоматических тестов инструментария Application Security,
- Построения критериев качества прохождения сред разработки (требований ИБ),
- Проверки зависимостей, компонентного анализа, IDE среды разработки и иного,
- Приравнивания уязвимостей к дефектам кода,
- Постоянному мониторингу изменений.

Кейс

- Контрольная среда описывает уровень текущей ситуации на проекте и у продукта
- Текущий уровень риска отображает актуальный статус на сегодняшний день
- Целевой уровень риска указывает к чему мы придем в случае выполнения мер минимизации
- В иных случаях происходит работа с рисками: делегирование, отказ, принятие.

ИБ предлагает принять целевые риски активности с учетом реализации мер ИБ		Текущий уровень в активности	Целевой уровень в активности	Контрольная среда
NC 208	**Нарушение законодательных требований** 187-ФЗ к защите данных ОКИИ, что может привести к административной ответственности со стороны ФСТЭК, вплоть до уголовной (при причинении значимого вреда КИИ).	H	M	
DL 505	**Утечка конфиденциальной информации** в логах совершенная из внешней неконтролируемой среды , что может привести к ущербу репутации, компрометации инфраструктуры и, как следствие, усилению кибер-атак на Банк	H	M	

Как обезопаситься?

В случае раскрытия конфиденциальной информации уровня С2 (инфраструктурные логи) повлекшей за собой киберинцидент на ОКИИ, либо проведении регуляторной проверки, аудита (включая/исключая киберинцидент) возможно выявление несоответствия требований к защите ОКИИ, что приведет к штрафным санкциям для банка, должностных лиц, в том числе уголовная ответственность.

PRE-условия	Ответственный	Статус	Срок
Провести сканирование исходного кода системы мониторинга			
Обезличить инфраструктурные данные, которые передаются в виде нотификаций в телеграмм канал			
Проработать и автоматизировать механизм удаления чувствительных данных из системы мониторинга, telegram-канала раз в неделю			
Интегрировать систему мониторинга с telegram-каналом для передачи инфраструктурных логов через WSO2 MI			

POST-условия	Ответственный	Статус	Срок
Устранить уязвимости по отчету сканирования исходного кода системы мониторинга			
Проработать возможность использования отечественного аналога telegram на других платформах и согласовать с BISO			
Реализовать механизм защиты микросервисов и контейнеризации на OpenShift			
Проработать ролевую матрицу системы мониторинга и согласовать с BISO			
Интегрировать DAM и обеспечить контроль трафика на PROD сервере			
Провести Hardening платформы PostgreSQL в соответствии с CIS Benchmarks			
Обезличить инфраструктурные данные, которые передаются в виде нотификаций в телеграмм канал			

А что будет?

Санкционный риск связанный с штрафами от регуляторов по факту совершенного киберинцидента, где передается информация в НКЦКИ для проведения расследования и вынесения соответствующей ответственности для банка, должностных лиц.

Риск может повлечь за собой проверку на соответствие другим требованиям к защите ОКИИ. В случае выявления аудитом, либо регуляторной проверки ответственность аналогична, отличия в степени тяжести по действующему законодательству.

Ответственность:
УК согласно ст. 274.1 УК РФ, части 3,4,5

- Сроком лишения свободы до 10 лет,
- Запрет на деятельность и занимаемые должности до 5 лет для должных лиц.
- ГК - КоАП РФ Статья 13.12.1. с штрафом до 100 000 рублей на физическое лицо, на юридическое лицо до 500 000 рублей,
- Иные регуляторные штрафные санкции для банка.

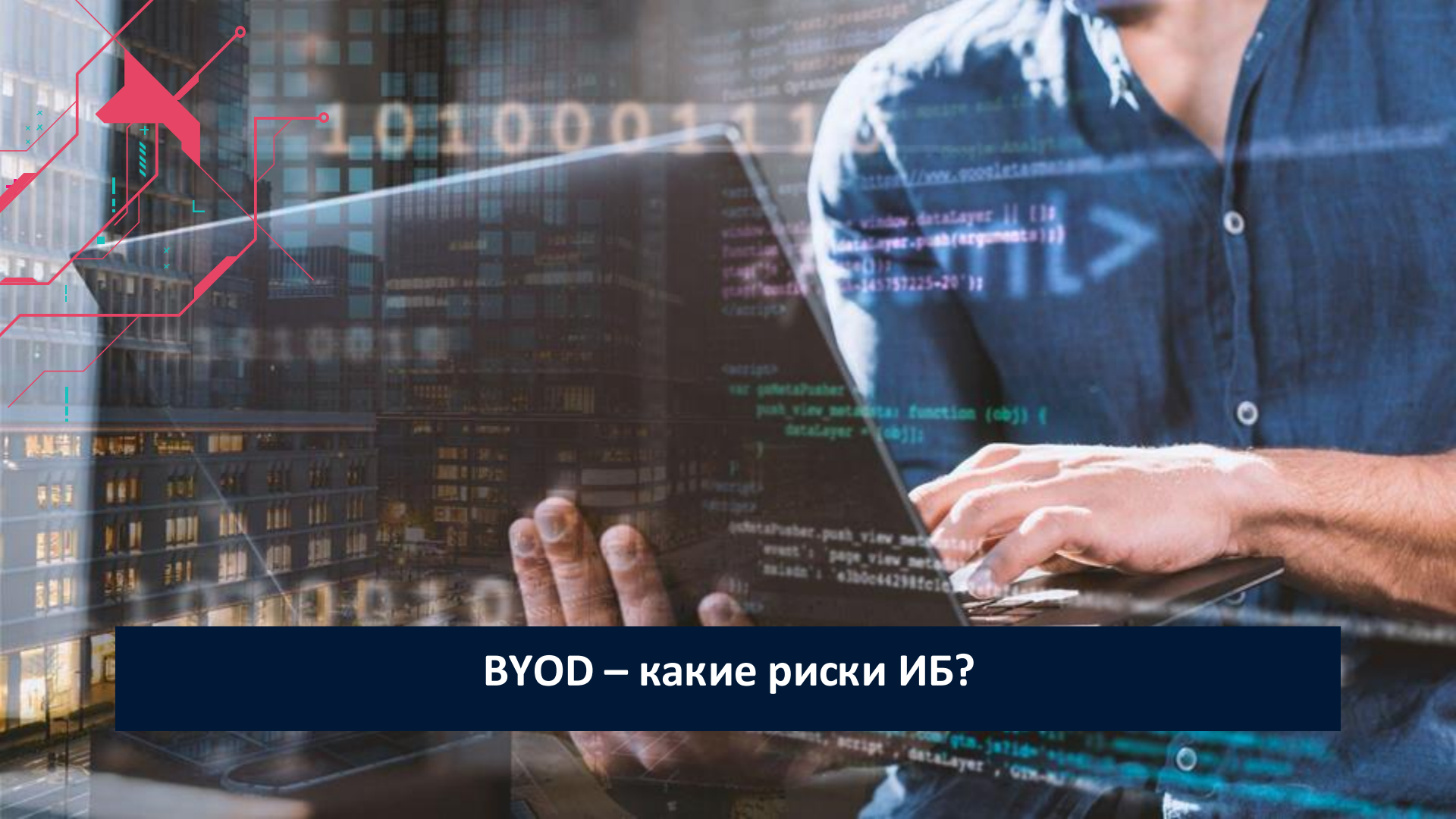
Последовательность: уведомление о устранении (в случае отсутствия киберинцидента), штрафы, привлечение к ответственности согласно УК, ГК РФ.

Основания

Включает в себя нарушение условий кризисных требований (желтый уровень опасности):

- Письмо ФСТЭК 8 от 07.03.2022 №240/84/1189, - запретить возможность размещения защищаемой информации в облачных сервисах, а также ее передачу через мессенджеры, Google Docs и другие сервисы,
- Письмо ФСТЭК 12 от 19.03.2022 №240/80/607, - провести инвентаризацию информационных ресурсов на предмет использования иностранного программного обеспечения, включая облачные решения, мессенджеры, системы управления взаимоотношениями с клиентами (CRM), средства коллективной работы, офисное программное обеспечение, интегрированную среду разработки (IDE). В случае наличия таких решений разработать план по переходу на отечественные аналоги,
- Бюллетень НКЦКИ 19 от 19.03.2022, - организовать инвентаризацию облачных решений и разработать план по переходу на российские аналоги или решения, разворачиваемые локально и неконтролируемые производителем извне. Это касается в том числе и решений, которые используются коммерческими предприятиями: мессенджеры, система управления взаимоотношениями с клиентами (CRM), средства коллективной работы, офисные пакеты, интегрированные среды разработки (IDE) и прочее.

Аналогично: РКН признал Telegram иностранным мессенджерам и не подлежащим к интеграции с банками.



BYOD – какие риски ИБ?

Thanks!

Вопросы?
shmakovis@inbox.ru
shmakovis@lanit.ru
@geminishkv