

Информация с канала, входящего в группу информационных ресурсов РБПО-сообщества ФСТЭК России и ИСП РАН

https://t.me/sdl_community

Ответ Дмитрия Владимировича Пономарёва (НТЦ-ФОБОС, ИСП РАН, модератор SDL-сообщества РФ) на тему «рыб» шаблонов и тд.

Привет!

Нагрузка высокая, но пока что удается её держать! Надеюсь у тебя также всё штатно-положительно 😊

1. "Информация с официального телеграм-канала ИСП РАН и ФСТЭК России по теме РБПО (так называемое SDL-сообщество РФ)"

Более корректно будет написать: "Информация с канала, входящего в группу информационных ресурсов РБПО-сообщества ФСТЭК России и ИСП РАН". Я везде в прессе такую формулировку использую.

2. Формально мне добавить действительно нечего - на текущий момент ничего похожего на единые "православные" регламенты не существует и "в сентябре" их точно не появится. Но к Q1-Q2 2026 ситуация может измениться, если например ФСТЭК поставит такую задачу ИСПу. Это я не про инсайды какие-то пишу, а про то, что сейчас всё стремительно развивается - и в принципе за полгода может многое поменяться. Главное - действительно никаких документальных стандартов оформления сейчас нет.

3. Настоятельно стоит рекомендовать посмотреть первоисточник - выступление Ивана Шаркова на Kaspersky Certification Day (2025). Также я всем рекомендую смотреть первые 4 доклада с АРПП прошедшего - ссылка также в community - Гефнер, Падарян, Подшибякин, Быханова. Елена как раз затрагивает вопросы регламентов, то, на что мы сами сейчас опираемся.

Как то так...

Отрывок с обсуждения темы в (https://t.me/sdl_community)

Nikolai Panfilov

Коллеги, всем добрый день!

Работаю в сфере телекома и IT, разрабатываем хард и софт. Наш AppSec ушёл с должности, где занимался темой Разработки Безопасного Программного Обеспечения, и я как техпис подхватил задачу по текстовой (нетехнической) части написания регламентов. Сейчас ищу «живые» документы по РБПО в соответствии с ГОСТ Р 56939–2024 — хочется научиться на примерах и сделать сразу хорошо, так как опыта работы с ГОСТами совсем не имею.

Если политика вашей компании позволяет делиться такой информацией, можете показать, как у вас составлены такие регламенты?

Алексей П.

В открытом доступе таких документов нет.

Как вариант нанять лабораторию, чтобы "проконсультировала" или брать методику ФСТЭК и пытаться от нее отталкиваться опять же, консультируясь с испытательной лабораторией.

Дмитрий Владимирович Пономарёв

Николай, добрый день.

В настоящий момент времени на дискуссии нет, равно как и нет времени полноценно объяснять, почему внедрение и развитие практик РБПО в компании, при всем уважении к профессии технического писателя, должен начинать не "технический писатель в компании, из которой ушел видимо единственный AppSec, но руководитель поставил задачу 'натянуться на ГОСТ', и решили начать с бумажной безопасности (и ей же возможно и закончить)".

Примерная аналогия - небольшая частная клиника, из которой уволился единственный врач, но санитары/медбратья отправляют администратора клиники где-нибудь накачать красивых регламентов, чтобы как-нибудь что-нибудь, начнем с этого, потом пациенты подтянутся...

Ваш пост вчера я удалил именно по этой причине - чтобы сделать эту работу хорошо вас, как компанию, не спасет никакая хорошая рыба регламентов. Мы видели уже не одну компанию, в которой всё РБПО, это тех.

писатель / аналитик, который сделал красивых бумаг "по форме", но при первом же взгляде не них сразу видно, что это выхолощенная форма, без сути, содержания и реальных процессов в бэке.

Требований к оформлению регламентов нет. Входы, выходы, действующие лица, основные тезисы из ГОСТ - этого достаточно. "Бумага" может быть любой, были бы процессы и люди, их выполняющие.

Настоятельно рекомендую посмотреть выступление Ивана Шаркова с Касперски Серт Дэй, чтобы понять, на чем именно делается фокус как при внедрении, так и при развитии РБПО-практик, и при последующей их проверке.

Не будет людей, инструментов, техники, процессов - а главное, политической воли руководителя на всё это тратиться - никакие регламенты вам не помогут. Будут - как именно писать не принципиально (опять-таки смотрите доклад Шаркова, там про регламенты есть, а заодно и доклад Быхановой на АРПП - вчера выложили).

July 30

Nikolai Panfilov ★

Reply

Коллеги, всем добрый день!

Работаю в сфере телекома и IT, разрабатываем хард и софт. Наш AppSec ушёл с должности, где занимался темой Разработки Безопасного Программного Обеспечения, и я как техпис подхватил задачу по текстовой (не-технической) части написания регламентов. Сейчас ищу «живые» документы по РБПО в соответствии с ГОСТ Р 56939-2024 — хочется научиться на примерах и сделать сразу хорошо, так как опыта работы с ГОСТами совсем не имею.

Если политика вашей компании позволяет делиться такой информацией, можете показать, как у вас составлены такие регламенты?

← 3 10:48

Алексей П

Nikolai Panfilov

Коллеги, всем добрый день! Работаю в сфере телекома и IT,...

В открытом доступе таких документов нет.

Как вариант нанять лабораторию, чтобы "проконсультировала" или брать методику ФСТЭК и пытаться от нее отталкиваться опять же консультируясь с испытательной лабораторией.

АП

10:55

July 31

Дмитрий Владимирович Пономарёв

Николай, добрый день.

В настоящий момент времени на дискуссии нет, равно как и нет времени полноценно объяснять, почему внедрение и развитие практик РБПО в компании, **при всем уважении к профессии технического писателя**, должен начинать не *"технический писатель в компании, из которой ушел видимо единственный AppSec, но руководитель поставил задачу 'натянуться на ГОСТ', и решили начать с бумажной безопасности (и ей же возможно и закончить)"*.

Примерная аналогия - небольшая частная клиника, из которой уволился единственный врач, но санитары/медбраты отправляют администратора клиники где-нибудь накачать красивых регламентов, чтобы *как-нибудь что-нибудь, начнем с этого, потом пациенты подтянутся...*

Ваш пост вчера я удалил именно по этой причине - чтобы сделать эту работу хорошо вас, как компанию, не спасет никакая хорошая рыба регламентов. Мы видели уже не одну компанию, в которой всё РБПО, это тех. писатель / аналитик, который сделал красивых бумаг "по форме", но при первом же взгляде не них сразу видно, что это выхолощенная форма, без сути, содержания и реальных процессов в бэке.

Требований к оформлению регламентов нет. Входы, выходы, действующие лица, основные тезисы из ГОСТ - этого достаточно. "Бумага" может быть любой, были бы процессы и люди, их выполняющие.

Настоятельно рекомендую посмотреть выступление Ивана Шаркова с Касперски Серт Дэй, чтобы понять, на чем именно делается фокус как при внедрении, так и при развитии РБПО-

ПолуОтпуск
До 03.авг

Настоятельно рекомендую посмотреть выступление Ивана Шаркова с Касперски Серт Дэй, чтобы понять, на чем именно делается фокус как при внедрении, так и при развитии РБПО-практик, и при последующей их проверке.

Не будет людей, инструментов, техники, процессов - а главное, политической воли руководителя на всё это тратиться - никакие регламенты вам не помогут. Будут - как именно писать не принципиально (опять таки смотрите доклад Шаркова, там про регламенты есть, а заодно и доклад Быхановой на АРПП - вчера выложили).

ПолуОтпуск
До 03.авг

2:40



Nikolai Panfilov ★

То есть я правильно понимаю, что каждый пишет что-то своё, и понятия «правильно написанный регламент» не существует? Потому что в ГОСТ Р 56939-2024 такие размытые формулировки, что туда можно что угодно подогнать.

2:41



Алексей П

Почему не существует? Как и что писать в регламенты знают лаборатории и органы по сертификации, которые этим занимаются, знает отдел по сертификации ФСТЭК. Я писал, что осилить "с нуля" не занимаясь сертификацией предварительно нелегко, но при грамотной консультации знающих специалистов реально.

Регламенты будут полезны и соответствовать ГОСТ 56939, если будут учитывать специфику именно вашей организации, начиная от количества и должностей работников и заканчивая используемыми средствами тестирования и языками программирования.

2:42

АП



Коллеги, доброго дня.

В сообщество вливаются новые участники, список чатов/каналов сообщества стал достаточно обширным и не все знают про существующие ресурсы. Представляется полезным раз в полгода публиковать список ресурсов сообщества с их краткой аннотацией.

Ресурсы под эгидой Центра компетенций ФСТЭК России и ИСП РАН:

@sdl_inform (https://t.me/sdl_inform) - канал, не ставьте его в Mute, сообщения там появляются в среднем одно в неделю. Основные, наиболее значимые для сообщества оповещения о встречах и иных мероприятиях.

@sdl_static (https://t.me/sdl_static) - чат, посвященный вопросам компиляторики и статического анализа (в первую очередь безопасный компилятор/Svace/Svacer, но не только).

@sdl_dynamic (https://t.me/sdl_dynamic) - чат, посвященный вопросам динамического анализа (в первую очередь Crusher/Sydr/Casr/Блесна/Natch, но не только).

@sdl_community (https://t.me/sdl_community) - чат, посвященный вопросам объединения сил и средства сообщества в вопросах анализ ядра Линукс и критичных компонентов, доверенной загрузки и т. п., а также мероприятиям и некоторым (согласованным) новостям от регулятора.

[NEW] @sdl_ (https://t.me/sdl_flood)arch - чат, посвященный вопросам качественной и безопасной разработки, не укладывающимся в темы указанных выше чатов. В частности здесь обсуждаются вопросы композиционного анализа и ППК, вопросы контейнеров и кубернетес, общий вопросы моделирования и архитектуры

[NEW - ранее flood] @sdl_ (https://t.me/sdl_flood)holywar - чат, холивары на тему безопасной и качественно разработки. Сюда переносятся холивары по любым темам из остальных чатов, чтобы не засорять эфир и поддерживать низкий SNR (Signal-Noise Ratio).

Дружественные тематические ресурсы:

@sydr_fuzz (https://t.me/sydr_fuzz) - чат, поддержка пользователей фаззера Sydr.

@ispras_natch (https://t.me/ispras_natch) - чат, поддержка пользователей системы определения поверхности атаки Natch.

@sdl_for_upstream_ru (https://t.me/sdl_for_upstream_ru) и @sdl_for_upstream (https://t.me/sdl_for_upstream) - чат и канал, оповещения о принятых апстримом багах и уязвимостях, найденных участниками сообщества.

@ispras_friends (https://t.me/ispras_friends) - чат неформального общения друзей и единомышленников РБПО-сообщества ФСТЭК России и ИСП РАН.

@SDL_Community_SPb (https://t.me/SDL_Community_SPb) - чат, локальный чат Питерской ветки нашего сообщества, созданный в мае с целью координировать локальные встречи в СПб (ближайшая будет 12-го августа, 27-го июля объявим подробности).

Некоторые правила ресурсов «под эгидой»:

1. Не стесняйтесь задавать вопросы - чаты изначально созданы именно как просветительский ресурс под эгидой регулятора, в этом их основная миссия. И, традиционно, нам нужны мотивированные и грамотные контрибьюторы :)

2. Чаты не предназначены для обсуждения особенностей трактовки регуляторных документов (Положения, Требования, Методики и т. п.) и их правоприменительной практики, за исключением особых случаев, как правило непосредственно инспирированных регулятором, например: https://t.me/sdl_community/2218.

3. Чаты не предназначены для форвардинга сообщений маркетинговой направленности, особенно в отношении различных "поделок". Описание вашего личного, подтверждаемого и воспроизводимого в потенциальных публичных соревнованиях опыта использования тех или иных инструментов/методик, приветствуется.

[NEW] 3.1. Некоторое исключение делается для значимых и кросс-верифицированных участников нашего сообщества (вы и так знаете о ком речь, если в сообществе давно. Модератор знает их точно, и авторитаризм никто не отменял) в случае ответов на вопросы в чате. Но в любом случае злоупотребление данной возможностью будет пресекаться вне зависимости от любой дружбы.

4. Избегайте флуда, в том числе личных эмоциональных позиций, флейма, глубокомысленных комментариев по вопросам, в которых вы слабо разбираетесь и т. п. Все люди взрослые, банхаммер не дремлет :) Исключение - чат друзей @ispras_friends.