

# ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

## Вебинар 23. Реагирование на информацию об уязвимостях





# ПРЕДСТАВИМСЯ!

Спикеры и гости вебинара



# ВАЛЕРИЙ ФИЛАТОВ

Irreplaceable **Developer Advocate**

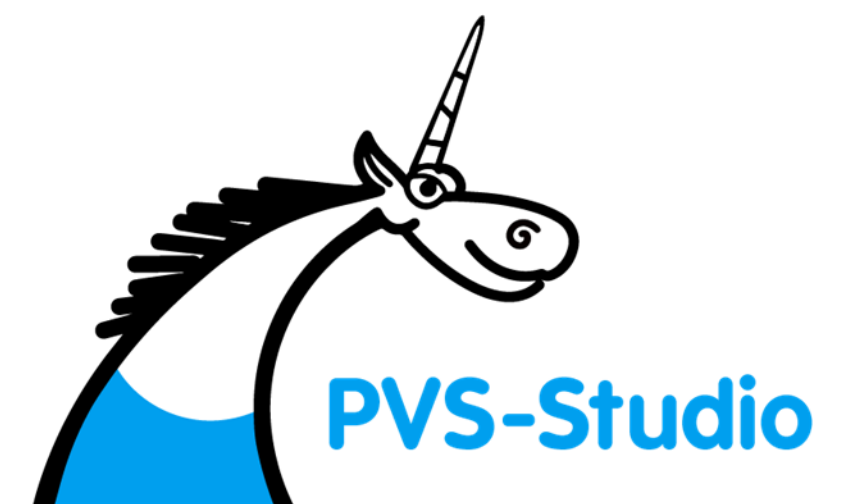
- Разработчик статического анализатора кода PVS-Studio.
- Рассказываю про технологии статического анализа и не только в статьях и на различных мероприятиях.



@feeelin



@feelindex



# ВИТАЛИЙ ПИКОВ

Неповторимый эксперт в области ИТ, ИБ,  
преподаватель

- Стаж преподавательской работы более 10 лет.
- Заслуженный доцент Российского нового университета, преподаватель высшей школы.
- Microsoft Certifications Earned: MCT, MCPS, MCSA, MCTS.
- Автор более 30 научных публикаций.



# ДМИТРИЙ ЧАСТУХИН

Важный **технический директор**

- Эксперт в пентесте и управлении уязвимостями
- Более 15 лет в сфере кибербезопасности
- Спикер на различных конференциях



 **Hexway**



# О ЦИКЛЕ ВЕБИНАРОВ

«Вокруг РБПО за 25 вебинаров»



## ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ: ГОСТ Р 56939-2024

- Организуют УЦ МАСКОМ и ООО «ПВС» (PVS-Studio)
- ГОСТ Р 56939-2024 описывает 25 процессов, необходимых для реализации разработки безопасного ПО, поэтому и 25 вебинаров
- Мы открыты к сотрудничеству по разбору тем, пишите нам!



# #МНОГАБУКАФ

## 5.23 Реагирование на информацию об уязвимостях





## 5.23.1 ЦЕЛИ

Обеспечение выявления и устранения уязвимостей при эксплуатации ПО.



## 5.23.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

- Разработать регламент реагирования на информацию об уязвимостях.



## 5.23.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

- Разработать регламент реагирования на информацию об уязвимостях.
- Осуществлять обработку поступающих запросов от пользователей (через службу технической поддержки, по иным каналам взаимодействия) с последующим анализом ошибок функционирования на предмет наличия уязвимостей (в случае получения таких запросов).

## 5.23.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

- Разработать регламент реагирования на информацию об уязвимостях.
- Осуществлять обработку поступающих запросов от пользователей (через службу технической поддержки, по иным каналам взаимодействия) с последующим анализом ошибок функционирования на предмет наличия уязвимостей (в случае получения таких запросов).
- При обработке поступающих запросов и при последующем анализе использовать средства автоматизации (например, систему управления изменениями, систему отслеживания ошибок, систему управления задачами и т.п.).



## 5.23.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

- Разработать регламент реагирования на информацию об уязвимостях.
- Осуществлять обработку поступающих запросов от пользователей (через службу технической поддержки, по иным каналам взаимодействия) с последующим анализом ошибок функционирования на предмет наличия уязвимостей (в случае получения таких запросов).
- При обработке поступающих запросов и при последующем анализе использовать средства автоматизации (например, систему управления изменениями, систему отслеживания ошибок, систему управления задачами и т.п.).
- Осуществлять анализ информации о найденных уязвимостях в ПО на предмет подтверждения наличия/отсутствия уязвимостей и принимать решение о необходимости их устранения по результатам оценки.

## 5.23.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

- Разработать регламент реагирования на информацию об уязвимостях.
- Осуществлять обработку поступающих запросов от пользователей (через службу технической поддержки, по иным каналам взаимодействия) с последующим анализом ошибок функционирования на предмет наличия уязвимостей (в случае получения таких запросов).
- При обработке поступающих запросов и при последующем анализе использовать средства автоматизации (например, систему управления изменениями, систему отслеживания ошибок, систему управления задачами и т.п.).
- Осуществлять анализ информации о найденных уязвимостях в ПО на предмет подтверждения наличия/отсутствия уязвимостей и принимать решение о необходимости их устранения по результатам оценки.
- Осуществлять оценку актуальности и критичности уязвимости с точки зрения безопасности ПО (в случае получения информации об уязвимости ПО из внешнего источника) и принимать решение о необходимости ее устранения по результатам оценки.



## 5.9.2 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

- Регламент реагирования на информацию об уязвимостях должен содержать обязанности сотрудников и их роли при реагировании на информацию об уязвимостях ПО, правила реагирования на информацию об уязвимостях, правила оценки актуальности и критичности уязвимости с точки зрения безопасности ПО, периодичность проведения поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО.

## 5.9.2 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

- Регламент реагирования на информацию об уязвимостях должен содержать обязанности сотрудников и их роли при реагировании на информацию об уязвимостях ПО, правила реагирования на информацию об уязвимостях, правила оценки актуальности и критичности уязвимости с точки зрения безопасности ПО, периодичность проведения поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО.
- Артефакты реализации требований, подтверждающие получение и обработку запросов от пользователей, должны содержать информацию о запросах пользователей об ошибках (уязвимостях) ПО (дата, время запроса, идентификатор пользователя, статус запроса), результат анализа ошибок функционирования на предмет наличия уязвимостей.



## 5.9.2 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

- Регламент реагирования на информацию об уязвимостях должен содержать обязанности сотрудников и их роли при реагировании на информацию об уязвимостях ПО, правила реагирования на информацию об уязвимостях, правила оценки актуальности и критичности уязвимости с точки зрения безопасности ПО, периодичность проведения поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО.
- Артефакты реализации требований, подтверждающие получение и обработку запросов от пользователей, должны содержать информацию о запросах пользователей об ошибках (уязвимостях) ПО (дата, время запроса, идентификатор пользователя, статус запроса), результат анализа ошибок функционирования на предмет наличия уязвимостей.
- Артефакты реализации требований, подтверждающие выполнение анализа информации о найденных уязвимостях в ПО, должны содержать информацию о результатах тестирования ПО на предмет применимости информации об уязвимости ПО, проект (шаблон) ответа пользователям на запросы пользователей об ошибках (уязвимостях) ПО (о применимости информации о найденных уязвимостях), решение по результатам анализа информации о найденных уязвимостях в ПО.

## 5.9.2 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

- Регламент реагирования на информацию об уязвимостях должен содержать обязанности сотрудников и их роли при реагировании на информацию об уязвимостях ПО, правила реагирования на информацию об уязвимостях, правила оценки актуальности и критичности уязвимости с точки зрения безопасности ПО, периодичность проведения поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО.
- Артефакты реализации требований, подтверждающие получение и обработку запросов от пользователей, должны содержать информацию о запросах пользователей об ошибках (уязвимостях) ПО (дата, время запроса, идентификатор пользователя, статус запроса), результат анализа ошибок функционирования на предмет наличия уязвимостей.
- Артефакты реализации требований, подтверждающие выполнение анализа информации о найденных уязвимостях в ПО, должны содержать информацию о результатах тестирования ПО на предмет применимости информации об уязвимости ПО, проект (шаблон) ответа пользователям на запросы пользователей об ошибках (уязвимостях) ПО (о применимости информации о найденных уязвимостях), решение по результатам анализа информации о найденных уязвимостях в ПО.
- Артефакты реализации требований, подтверждающие выполнение оценки актуальности и критичности уязвимости с точки зрения безопасности, должны содержать следующие сведения, информацию об оценке актуальности уязвимости, информацию об оценке уровня критичности уязвимости ПО, решение по результатам анализа актуальности и критичности уязвимости.

# СЛОВО СПИКЕРАМ!

Переходим к докладам





Сделай свой проект чистым  
и безопасным вместе  
с PVS-Studio



Telegram-канал  
Hexway Vampy ASPM



Community-версия  
Hexway ASOC



Сайт  
Hexway



Получи 10% скидку  
на курсы «М БРПО»  
в Учебном Центре «МАСКОМ»

