

17 декабря 2025 г.

# Вебинар 23. Реагирование на информацию об уязвимостях

Виталий Александрович Пиков, руководитель направления обучения по РБПО,  
преподаватель НОУ ДПО «УЦБИ «МАСКОМ».

## **ДИСКЛЕЙМЕР / DISKLAIMER**

• Данное выступление содержит материалы, которые могут быть неприемлемы, неуместны или оскорбительны для некоторых зрителей. Просмотр данного выступления рекомендуется только лицам старше 18 лет в соответствии с законодательством. Некоторые высказывания, сказанные в ходе выступления, предназначены исключительно для юмористических целей и не несут в себе намерения оскорбить или унижить кого-либо. Все сценарии, персонажи и ситуации являются вымышленными и не имеют отношения к реальным событиям или личностям. Юмористический контент данного выступления может содержать ненормативную лексику, сексуальные сцены, насилие, кровь, резкие и/или громкие звуки, а также световые вспышки или другие элементы, которые могут вызвать дискомфорт или неприязнь при просмотре. Все действия были выполнены профессиональными актерами и исполнителями с использованием спецэффектов и безопасного оборудования. Не пытайтесь повторить или воссоздать какие-либо сцены из выступления. Автор не несет ответственности за любые возможные негативные последствия, вызванные просмотром данного выступления, и рекомендует обратиться за помощью к квалифицированным специалистам в случае возникновения психологических или эмоциональных проблем в результате просмотра.

• Данное выступление не рекомендуется к просмотру лицам младше 18 лет, а некоторые высказывания, сказанные в ходе выступления, предназначены исключительно для юмористических целей и не используются для распространения информации с целью опорочить людей по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, не содержит призывов к осуществлению террористической и экстремистской деятельности, участию в массовых мероприятиях, проводимых с нарушением установленного порядка, не демонстрирует неуважение к обществу, государству, официальным государственным символам Российской Федерации, конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации.

• Мнения, озвученные в данном выступлении, являются оценочными суждениями и в соответствии с принципами свободы слова, выраженными в ст. 10 европейской конвенции по правам человека, свободны к распространению и не являются призывом к совершению противоправных действий. Выступление может содержать информацию, просмотр которой в соответствии с Федеральным Законом Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», доступен только для лиц старше 18 лет.



**ПИКОВ**  
**Виталий**  
**Александрович**

**Общий стаж работы:** более 26 лет.

**Стаж преподавательской работы:** более 10 лет.

**Образование:** высшее, Тамбовский военный авиационный инженерный институт по специальности «Автоматизированные системы обработки информации и управления».

Заслуженный доцент Российского нового университета, преподаватель высшей школы.

В 2017 году прошёл профессиональную переподготовку в МГТУ им. Н. Э. Баумана по направлению подготовки «Информационная безопасность».

В 2019 году прошёл профессиональную переподготовку по программе «Противодействие иностранным техническим разведкам».

В 2020 году прошёл профессиональную переподготовку по программе «Педагогика профессионального обучения, профессионального образования и дополнительного профессионального образования».

В 2021 году прошёл профессиональную переподготовку по дополнительной профессиональной программе «ТЗИ».

В 2022 году прошёл профессиональную переподготовку по программе «Практическая психология».

**Microsoft Certifications Earned: MCT, MCPs, MCSA, MCTS.**

**Автор более 40 научных публикаций.**

Постоянный участник, спикер, эксперт на мероприятиях по информационной безопасности: Positive Hack Days Fest 2, Национальный форум информационной безопасности «Инфофорум», Международный военно-технический форум «АРМИЯ», Международная выставка InfoSecurity Russia, Международная научная конференция «Цивилизация знаний: российские реалии» (РосНОУ) и некоторых других.

Имею награды и звания Минобороны России.

**Авторизованный преподаватель по продуктам «Группы Астра» с правом проведения курсов по ОС Astra Linux Special Edition 1.8**

Читаю курсы, провожу занятия в области информационной безопасности, защиты информации и информационных технологий.



# Можно ли сделать систему без уязвимостей?

Три аксиомы Шуры-Буры:

**Аксиома первая.** Каждая программа содержит ошибку.

**Аксиома вторая.** Если программа не содержит ошибок, то неверен примененный метод.

**Аксиома третья.** Если программа на самом деле полностью и абсолютно правильна, она никому не нужна.

Факторы влияющие на наличие уязвимостей:

- Для сложных систем за частую невозможно за приемлемое время доказать отсутствие уязвимостей «нулевого дня» (0 day).
- Количество известных уязвимостей системы со временем растет.
- В конфигурации системы могут появляются уязвимости при вводе системы и при ее эксплуатации.
- Человеческий фактор.



**Абсолютной безопасности  
не существует...  
Всё взламывается...**

**Рано или поздно.**

**По стоимости, времени или мотивации атакующего.**



**~~Абсолютной безопасности  
не существует...  
Всё взламывается...~~**



**~~Рано или поздно.  
По стоимости, времени или мотивации атакующего.~~**

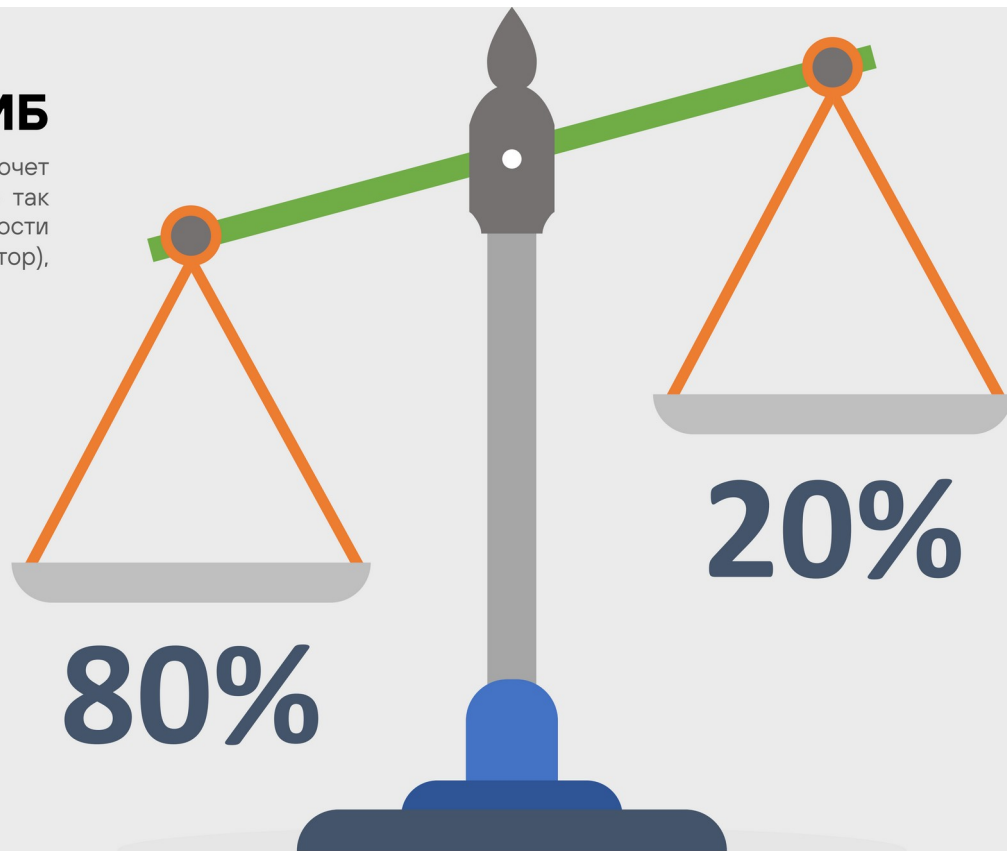
**Но мы, всё же, попробуем  
что-то с этим сделать!!!**



# Нормативка по ИБ – это неизбежное зло, но и его можно повернуть во благо!\*

## Результативная ИБ

Пентесты (потому что так хочет регулятор), мониторинг (потому что так хочет регулятор), оценка защищенности (потому что так хочет регулятор), реагирование (если успеем)...



## Бумажная ИБ

17/21/31/31/235/239 приказы ФСТЭК  
ФЗ-152/149/187/161  
683/757/747/719/779/787-П  
367/368/369/196/281/282 приказы ФСБ

Training Lab

## Максимизация ценности в интегрированных сценариях PoC

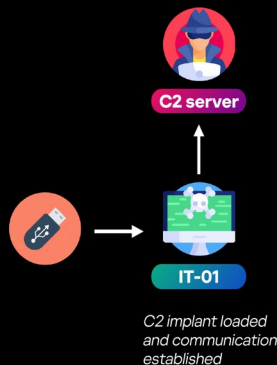
АНТОН ТИХОНОВ  
Solutions Expert, Advanced Threat Protection

**kaspersky** bring on  
the future



Phase 1: Malicious USB Attack

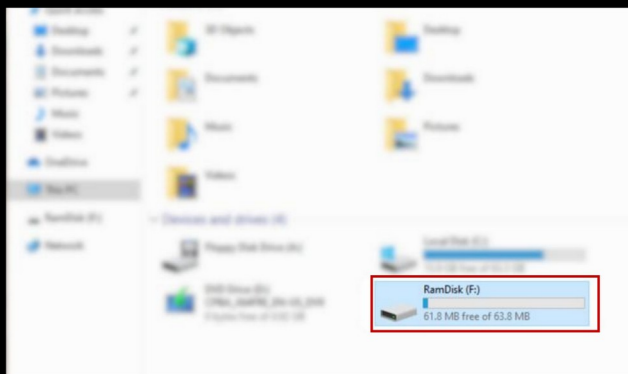
3



- A USB device with a dropper is connected to the target system (IT-01)
- The dropper runs, launching the attack chain
- The system initiates a connection to a malicious C&C server
- The attacker's toolset is downloaded to the compromised machine

Phase 1: Malicious USB Attack

4



Executing  
**admin\_guide.exe**  
dropper from a  
USB Drive (F:)

Phase 1: Running a Dropper (admin\_guide.exe) from a USB Drive

KUMA

5

### Alerts

Search...

<input type="checkbox"/>	Name	Status	Affected asset categories
<input type="checkbox"/>	Suspicious endpoint activity detected by EDR	New	Main/Categorized assets/Address space Main/Categorized assets/Test
<input type="checkbox"/>	Removable Media Process Execution	New	Uncategorized
<input type="checkbox"/>	Suspicious network behaviour detected	New	Uncategorized
<input type="checkbox"/>	Malicious file download	New	Uncategorized

The console displayed a list of alerts generated by KUMA SIEM



## Custom SIEM Rules: A Practical How-To

KUMA 7

**Task:** Detect execution of malicious binaries directly from removable media

+ Add Duplicate Delete Tags Show dependencies Link to correlator Exclusion list Search...		
<input type="checkbox"/> Name	Kind	Description
<input type="checkbox"/> Removable Media Process Execution	standard	Connecting a USB device and executing a binary from it may indicate the use of a rogue USB device or infected removable media
<input type="checkbox"/> A new process has been created	simple	The rule monitors the creation of new processes on endpoints (silent)
<input type="checkbox"/> A new external device connected	simple	The rule detects when a new external device, such as a USB storage device, is connected to a system.

**Trigger:** A USB storage device is connected to a system

**Follow-up Condition:** Process creation observed from the connected USB drive

## Custom SIEM Rules: A Practical How-To

KUMA 8

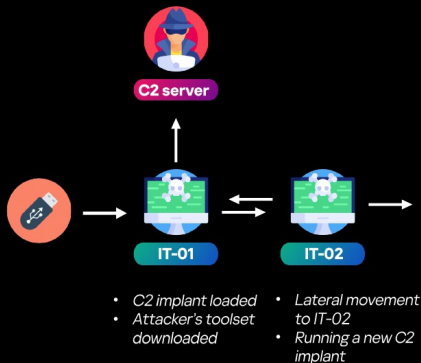
Name	A new external device connected	+	Name	A new process has been created
StartTime	2025-03-21 12:35:55:219		StartTime	2025-03-21 12:35:58:499
EndTime	2025-03-21 12:35:55:219		EndTime	2025-03-21 12:35:58:499
DeviceEventClassID	6416		DeviceEventClassID	4688
DeviceHostName	IT-01		DeviceHostName	IT-01
DeviceProduct	Windows		DeviceProduct	Windows
DeviceTimeZone	+03:00		DeviceTimeZone	+03:00
DeviceVendor	SanDisk Cruzer Blade USB Device		DeviceVendor	Kaspersky
DeviceCustomString4	Security		SourceProcessName	F:\admin_guide.exe
DeviceCustomString5	A new external device was recognized by the System		DeviceCustomString5	A new process has been created
CorrelationRule	A new external device connected		CorrelationRule	A new process has been created
Service	[OOTB] Correlator		Service	[OOTB] Correlator
BaseEventCount	1		BaseEventCount	1
ExternalID	A new device connected		ExternalID	A new process has been created

Event 1: USB Connected

Event 2: Executable launched

## Phase 3: Reconnaissance Activities

25



- Host & network reconnaissance (Nmap+LLM)
- Discovering secrets related to nearby **SRV-09** host on the compromised machine

## Detecting Public LLM API Usage in SIEM: A Practical How-To

26

```

LLM Result
{
  "id": "chatcmpl-8a8a7b4d0b94d3b885e2a23f3ed3ae",
  "choices": [
    {
      "message": {
        "content": "Nmap Scan Results Analysis

Open Ports: **[n]l.
Port 53/tcp - Domain Service**
State: Open
Protocol: TCP
Version: 9.20.2
Vulnerability: The open DNS service on this port may expose the
system to potential DNS amplification attacks or DNS spoofing.
Port 5432/tcp - PostgreSQL Database Service
State: Open
Protocol: TCP
Version: 16.0 - 16.2
Vulnerability: The PostgreSQL database service is exposed to the network,
which may allow unauthorized access or exploitation of known vulnerabilities in the
specific version range (16.0 - 16.2). It is recommended to ensure that the database
service is properly configured, and any necessary security patches are applied.

}
},
  "created": 1743170412,
  "model": "meta-llama/Meta-Llama-3-1-70B-Instruct"
}
  
```

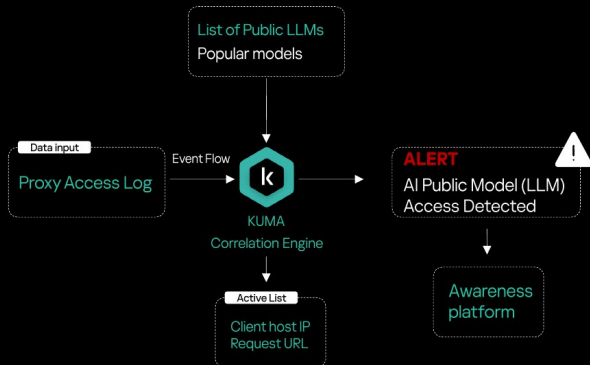
Nmap Scan → LLM Analysis → Actor Use

Why it matters?

- Automated reconnaissance
- Rapid exploitation of CVEs
- Speeds threat actor kill chain

## Custom SIEM Rules: A Practical How-To

27



## Phase 3: Detecting Public LLM API Usage in SIEM

KUMA 28

Timestamp	2025-03-19 14:57:30:559
Name	AI Public Model (LLM) Access Detected
StartTime	2025-03-19 14:57:29:226
EndTime	2025-03-19 14:57:29:226
DeviceProduct	KUMA
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
SourceHostName	aplstudio.nebius.com
DestinationAddress	195.242.11.3
CorrelationRule	AI Public Model (LLM) Access Detected
Service	[OOB] Correlator

Attackers are increasingly misuse public LLMs for malware creation, phishing, and evasion.

Usage of the **Nebius AI** interface has been detected

**РБПО** – это сокр. от «Разработка безопасного программного обеспечения» (РБПО).

## ГОСТ Р 56939-2024

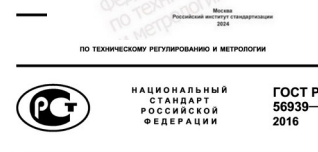
«**3.1 безопасное программное обеспечение:** Программное обеспечение, разработанное в ходе реализации совокупности процессов (мер), **направленных на предотвращение появления и устранение недостатков программы**».

## ГОСТ Р 56939-2016

«**3.2 безопасное программное обеспечение:** Программное обеспечение, разработанное с использованием совокупности мер, **направленных на предотвращение появления и устранение уязвимостей программы**».

## ГОСТ Р 56939-2024

«**3.8 недостаток программы:** Любое несоответствие программы заданным требованиям или любая ошибка, допущенная в ходе проектирования или реализации программы, которая в случае её неисправления может являться причиной невозможности выполнения требуемых функциональных возможностей или уязвимости программы».



Защита информации  
РАЗРАБОТКА БЕЗОПАСНОГО  
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
Общие требования  
Издание официальное





## Сертификация процессов разработки безопасного программного обеспечения



### Порядок сертификации процессов разработки безопасного программного обеспечения средств защиты информации

утвержден приказом ФСТЭК России  
от 1 декабря 2023 г. № 240

#### Что проверяется?

- ✓ Проверка документации
- ✓ Анализ инструментов и инфраструктуры разработки
- ✓ Проверка квалификации специалистов
- ✓ Проверка реализации изготовителем процессов РБПО
- ✓ Проверка реализации изготовителем процедур поддержки безопасности программного обеспечения

#### Что дает наличие сертификата?

- Разработчик может самостоятельно проводить испытания, связанные с изменениями средств защиты информации

#### На что выдается сертификат?

- Сертификат соответствия выдается организации в отношении заданной области деятельности

#### Органы по сертификации:

ИСП РАН



Количество заявок на сертификацию: 18

Количество решений: 14

Количество сертификатов: 7

#### Организации имеющие сертификат:

SBER TECH  
kaspersky



positive  
technologies

РусБИТех-Астра

PosgresPro

infotecs

09.12.2025 Зал "Молекула"

## Результаты деятельности системы сертификации ФСТЭК России

3

Выдано более **5000** сертификатов  
соответствия на средства защиты  
информации

За прошедший год сертифицировано **110** средств защиты  
информации от несанкционированного доступа

В 2025 году произведено более **3 200 000** экземпляров  
сертифицированных средств защиты информации,  
применяемых в информационных системах органов  
государственной власти и на субъектами критической  
информационной инфраструктуры

В настоящее время производится **508** типов  
сертифицированных средств защиты информации

### Основные типы средств защиты информации

Операционные системы (26 сертификатов)

Системы управления базами данных (23 сертификата)

Средства доверенной загрузки (24 сертификата)

Средства антивирусной защиты (29 сертификатов)

Межсетевые экраны (59 сертификатов)

Системы обнаружения вторжений (49 сертификатов)

Средства виртуализации (22 сертификата)

Средства контейнеризации (12 сертификатов)

Средства контроля съемных машинных носителей информации  
(22 сертификата)

Системы управления событиями безопасности (12 сертификатов)

## Заимствованные программные компоненты с открытым исходным кодом в средствах защиты информации



**Порядок испытаний  
и поддержки безопасности  
средств защиты информации,  
в состав которых входят  
заимствованные программные  
компоненты с открытым  
исходным кодом**

письмо ФСТЭК России  
от 26 сентября 2024 г. № 240/24/4436

Более **90%** сертифицированных средств защиты информации созданы  
с использованием заимствованных программных компонентов

**Выдан 91 план испытаний  
на средства защиты информации**

### Типовые недостатки выявленные при рассмотрении SBOM

Неверно определены заимствованные  
программные компоненты, относящиеся к  
поверхности атаки

Неправильно представлено описание полей  
объектов в части источников получения и  
внешних ссылок

В перечень включаются только заимствованные  
компоненты, относящиеся к поверхности атаки  
и реализующие функции безопасности  
информации



## КАРТА РОССИЙСКОГО РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 2024

ЗАЩИТА ИНФРАСТРУКТУРЫ

Безопасность каналов и выделенных сетей

Защита АСУ ТП

Безопасность частных сетей (VPN)

Безопасность мобильных устройств

Безопасность беспроводных сетей (Wi-Fi)

Безопасность удаленного доступа к ресурсам (VPN, Cloud)

Безопасность облачных сервисов (SaaS, PaaS, IaaS)

Безопасность мобильных устройств

Безопасность беспроводных сетей (Wi-Fi)

Безопасность удаленного доступа к ресурсам (VPN, Cloud)

Безопасность облачных сервисов (SaaS, PaaS, IaaS)

МОНИТОРИНГ, ИССЛЕДОВАНИЕ, АНАЛИЗ

Центры мониторинга и расследования инцидентов (CSIRT)

Платформы для мониторинга ИБ-инцидентов (SIEM, SOAR)

Системы анализа безопасности, Средств безопасности (DevSecOps)

Системы управления инцидентами информационной безопасности (SIEM)

Платформы для расследования инцидентов (SIEM, SOAR)

Системы анализа безопасности, Средств безопасности (DevSecOps)

Системы управления инцидентами информационной безопасности (SIEM)

ЗАЩИТА ДАННЫХ

Системы классификации информации (КИИ, КИС, КИС-М)

Системы классификации информации (КИИ, КИС, КИС-М)

Системы классификации информации (КИИ, КИС, КИС-М)

Системы классификации информации (КИИ, КИС, КИС-М)

Системы классификации информации (КИИ, КИС, КИС-М)

Системы классификации информации (КИИ, КИС, КИС-М)

Системы классификации информации (КИИ, КИС, КИС-М)

Системы классификации информации (КИИ, КИС, КИС-М)

УСЛУГИ И СЕРВИСЫ

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

УСЛУГИ И СЕРВИСЫ

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

УСЛУГИ И СЕРВИСЫ

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности

Интеграция, сопровождение и ведение в области информационной безопасности



Продолжим рассуждать про:

**...уязвимости,**

**...хакеров,**

**...атаки.**

В соответствии ISO/IEC 27000:2014 «**Уязвимость** — это слабость актива или управления, эксплуатация которой приведёт к реализации одной или нескольких угроз».

**Уязвимость** – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использован для реализации угроз безопасности информации [**ГОСТ Р 56545–2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»**].

**Уязвимость программного обеспечения** — ошибка в программном обеспечении, способная напрямую быть использована хакером для получения доступа к системе или сети [CWE (Common Weakness Enumeration) — общий перечень дефектов (недостатков) безопасности [Электронный ресурс] URL: <http://cwe.mitre.org>].

В соответствии с **ГОСТ Р 56546–2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»** принята «классификация уязвимостей информационных систем, исходя из области происхождения уязвимостей, типов недостатков информационных систем и мест возникновения (проявления) уязвимостей информационных систем».

В соответствии со стандартом «в основе классификации уязвимостей информационных систем используются следующие классификационные признаки:

- область происхождения уязвимости;
- типы недостатков информационных систем;
- место возникновения (проявления) уязвимости информационных систем».

В соответствии с пунктом 5.1 стандарта «**уязвимости информационных систем по области происхождения**» подразделяются на следующие классы:

- уязвимости кода;
- уязвимости конфигурации;
- уязвимости архитектуры;
- организационные уязвимости;
- многофакторные уязвимости».

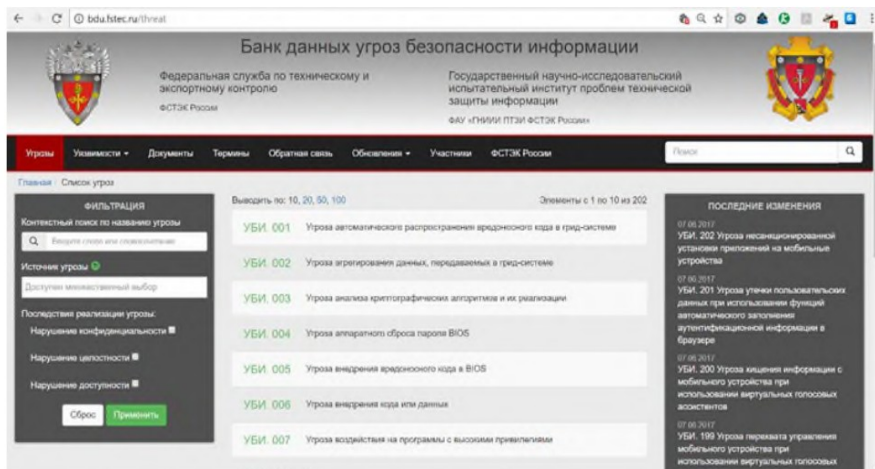


А согласно требованиям пункта 5.2 «уязвимости информационных систем по типам недостатков информационных систем подразделяются на:

- недостатки, связанные с неправильной настройкой параметров программного обеспечения;**
- недостатки, связанные с неполнотой проверки вводимых (входных) данных;**
- недостатки, связанные с возможностью прослеживания пути доступа к каталогам;**
- недостатки, связанные с возможностью перехода по ссылкам;**
- недостатки, связанные с возможностью внедрения команд ОС;**
- недостатки, связанные с межсайтовым скриптингом (выполнением сценариев);**
- недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки;**
- недостатки, связанные с внедрением произвольного кода;**
- недостатки, связанные с переполнением буфера памяти;**
- недостатки, связанные с неконтролируемой форматной строкой;**
- недостатки, связанные с вычислениями;**
- недостатки, приводящие к утечке/раскрытию информации ограниченного доступа;**
- недостатки, связанные с управлением полномочиями (учетными данными);**
- недостатки, связанные с управлением разрешениями, привилегиями и доступом;**
- недостатки, связанные с аутентификацией;**
- недостатки, связанные с криптографическими преобразованиями (недостатки шифрования);**
- недостатки, связанные с подменой межсайтовых запросов;**
- недостатки, приводящие к «состоянию гонки»;**
- недостатки, связанные с управлением ресурсами;**
- иные типы недостатков».**

В соответствии с пунктом 5.3 стандарта «уязвимости информационных систем по месту возникновения (проявления) подразделяются на:

- **уязвимости в общесистемном (общем) программном обеспечении;**
- **уязвимости в прикладном программном обеспечении;**
- **уязвимости в специальном программном обеспечении;**
- **уязвимости в технических средствах;**
- **уязвимости в портативных технических средствах;**
- **уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании;**
- **уязвимости в средствах защиты информации».**



Опубликованы в банке данных угроз ФСТЭК России, NIST NVD и т.п.

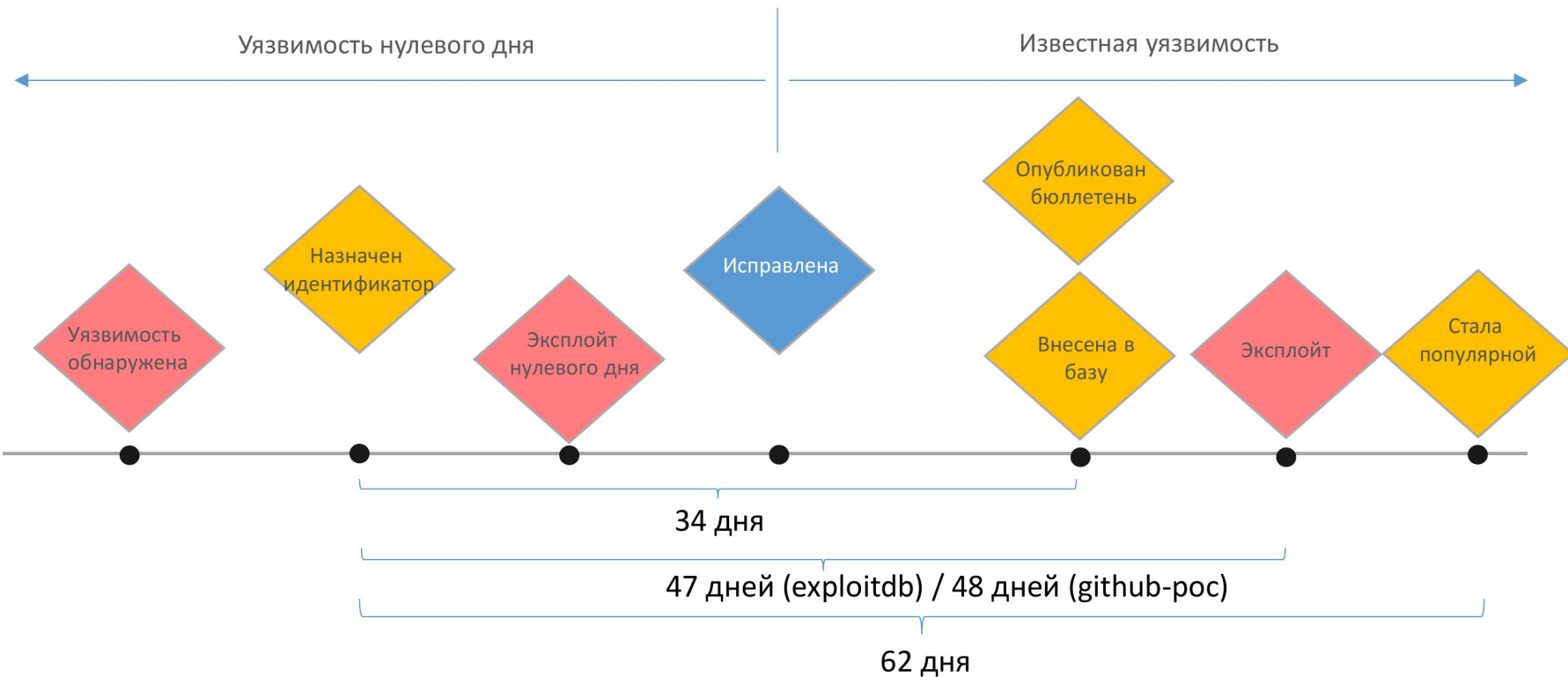
Нулевого дня (zero day)

Впервые выявленная уязвимость (Unpublished vulnerability) уязвимость, выявленная впервые и неопубликованная в общедоступных источниках.  
<https://bdu.fstec.ru/ubi/terms/terms/view/id/11>

**Уязвимость нулевого дня\*** — это недостаток программного обеспечения, для которого официальное исправление или обновление для системы безопасности не выпущено. Поставщик программного обеспечения может знать или не знать об уязвимости, и нет общедоступной информации об этом риске. Уязвимости нулевого дня часто имеют высокий уровень серьезности и активно эксплуатируются.

Управление уязвимостями будет отображать только уязвимости нулевого дня, о которых у него есть сведения.

<https://learn.microsoft.com/ru-ru/microsoft-365/security/defender-vulnerability-management/tvm-zero-day-vulnerabilities?view=o365-worldwide>



**Примечание:**  
Данные за 2023 год  
Медианные значения



Можно сказать, что **все наши действия** по обеспечению безопасности значимого объекта критической информационной инфраструктуры Российской Федерации направлены на:

- **исключение появления уязвимостей (уязвимость кода) при создании систем, ПО — РБПО** и прочее;
- **устранение уже имеющихся (уязвимости кода, уязвимости архитектуры)** — VM, зам. по ИБ, подразделение по ИБ, ОРД;
- **недопущение появления новых (организационные уязвимости, многофакторные уязвимости)**— VM, зам. по ИБ, подразделение по ИБ, ОРД.



- **Common Vulnerability Scoring System (CVSS)** — это открытый стандарт, используемый для расчета количественной оценки степени опасности, разработанный Национальным консультативным советом по инфраструктуре США.
- Текущая версия стандарта — Common Vulnerability Scoring System version 4.0.
- При расчете учитываются такие факторы, как наличие эксплойта, возможность удаленной эксплуатации, необходимость авторизации, возможные последствия.
- Калькуляторы для расчета CVSS 2/3/3.1:  
<https://bdu.fstec.ru/calc>

# Определение степени опасности уязвимости

## ■ CVSSv2:

- Низкая (Low) – 0.0 – 3.9
- Средняя (Medium) – 4.0 – 6.9
- Высокая (High) – 7.0 – 10.0

## ■ CVSSv3:

- Не определен (None) – 0.0
- Низкая (Low) – 0.1 – 3.9
- Средняя (Medium) – 4.0 – 6.9
- Высокая (High) 7.0 – 8.9
- Критическая (Critical) – 9.0 – 10.0



- **Низкая** – получение информации о системе.
- **Средняя** – получение информации о системе, которая будет полезна для проведения дальнейшей атаки, либо уязвимость, которую очень сложно проэксплуатировать.
- **Высокая и критическая** – получение административного доступа, либо запуск произвольного кода.

Главная · Калькулятор CVSS V3.1

Вектор CVSS v3: (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:H)

Базовые метрики
10

Базовая оценка (BS): 10

Вектор атаки (AV):

Сетевой (N)	Смежная сеть (A)	Локальный (L)	Физический (P)
-------------	------------------	---------------	----------------

Влияние на другие компоненты системы (S):

Не оказывает (U)	Оказывает (C)
------------------	---------------

Сложность атаки (AC):

Высокая (H)	Низкая (L)
-------------	------------

Влияние на конфиденциальность (C):

Не оказывает (N)	Низкое (L)	Высокое (H)
------------------	------------	-------------

Уровень привилегий (PR):

Высокий (H)	Низкий (L)	Не требуется (N)
-------------	------------	------------------

Влияние на целостность (I):

Не оказывает (N)	Низкое (L)	Высокое (H)
------------------	------------	-------------

Взаимодействие с пользователем (UI):

Требуется (R)	Не требуется (N)
---------------	------------------

Влияние на доступность (A):

Не оказывает (N)	Низкое (L)	Высокое (H)
------------------	------------	-------------

Временные метрики

Контекстные метрики

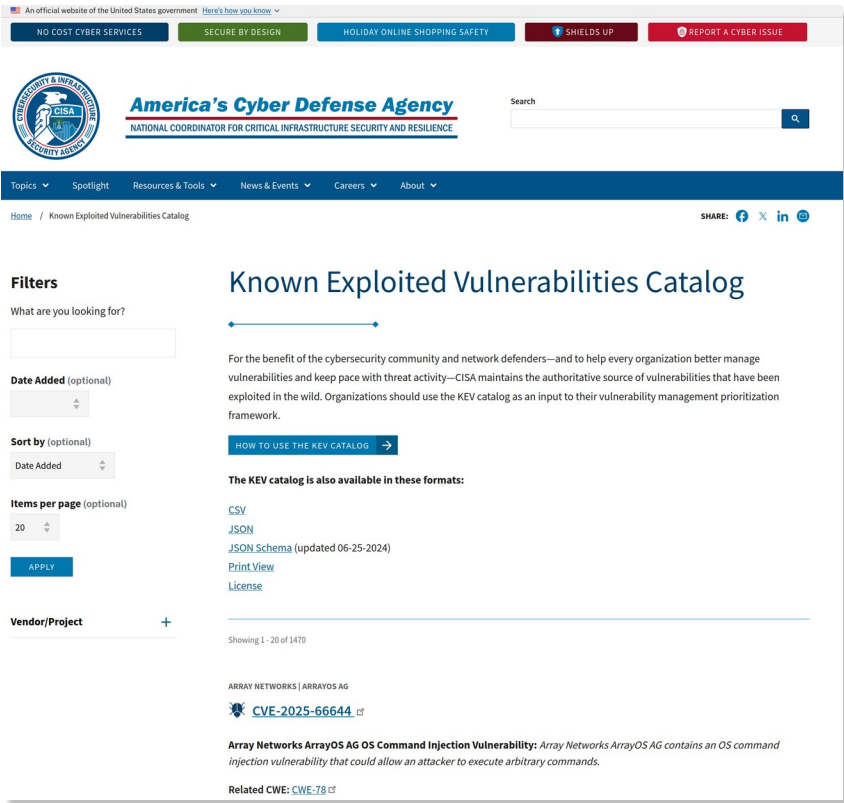
- **EPSS** предоставляет возможности для эффективного управления уязвимостями на основе данных. Основана основана на данных и использует текущую информацию об угрозах из CVE и реальные данные об эксплойтах.

- **Модель EPSS** выдает оценку вероятности от 0 до 1 (от 0 до 100 %), где чем выше оценка, тем больше вероятность того, что уязвимость будет использована.

### **Как работает модель EPSS?**

1. Сбор информации об уязвимостях из различных источников.
2. Сбор информации об ежедневной активности по эксплуатации.
3. Обучение модели: выявление взаимосвязей между информацией об уязвимостях и активностью по эксплуатации.
4. Измерение производительности модели и повторение 3 шага для оптимизации модели.
5. Ежедневное обновление информации об уязвимостях (шаг 1) и использование модели (шаг 3) для получения ежедневных оценок вероятности эксплуатации в течение следующих 30 дней для каждого опубликованного CVE.





Official website of the United States government. Here's how you know.

NO COST CYBER SERVICES | SECURE BY DESIGN | HOLIDAY ONLINE SHOPPING SAFETY | SHIELDS UP | REPORT A CYBER ISSUE

**America's Cyber Defense Agency**  
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / Known Exploited Vulnerabilities Catalog

SHARE: | | |

## Known Exploited Vulnerabilities Catalog

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

**Filters**

What are you looking for?

Date Added (optional)

Sort by (optional)

Date Added

Items per page (optional)

20

APPLY

Vendor/Project

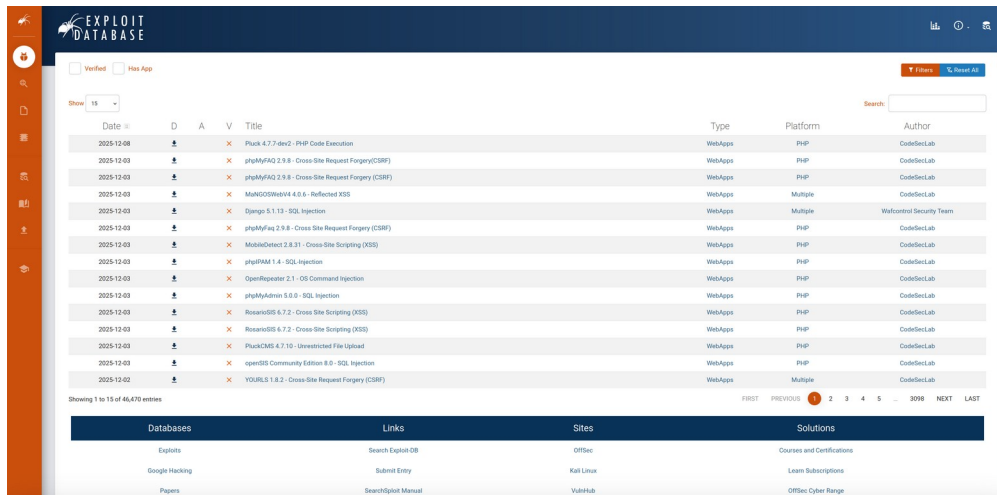
Showing 1 - 20 of 1470

ARRAY NETWORKS | ARRAYOS AG

**CVE-2025-66644**

**Array Networks ArrayOS AG OS Command Injection Vulnerability:** Array Networks ArrayOS AG contains an OS command injection vulnerability that could allow an attacker to execute arbitrary commands.

Related CWE: [CWE-78](#)



EXPLOIT DATABASE

Verified | Has App

Show: 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2025-12-08			X	Pluck 4.7.7.dn2 - PHP Code Execution	WebApps	PHP	CodeSecLab
2025-12-03			X	phpMyFAQ 2.9.8 - Cross-Site Request Forgery (CSRF)	WebApps	PHP	CodeSecLab
2025-12-03			X	phpMyFAQ 2.9.8 - Cross-Site Request Forgery (CSRF)	WebApps	PHP	CodeSecLab
2025-12-03			X	MANGOSWEAT 4.0.6 - Reflected XSS	WebApps	Multiple	CodeSecLab
2025-12-03			X	Omniqs 5.1.13 - SQL Injection	WebApps	Multiple	WafControl Security Team
2025-12-03			X	phpMyFAQ 2.9.8 - Cross-Site Request Forgery (CSRF)	WebApps	PHP	CodeSecLab
2025-12-03			X	MadonDetox 3.8.31 - Cross-Site Scripting (XSS)	WebApps	PHP	CodeSecLab
2025-12-03			X	phpFMM 1.4 - SQL Injection	WebApps	PHP	CodeSecLab
2025-12-03			X	OpenRepeater 2.1 - OS Command Injection	WebApps	PHP	CodeSecLab
2025-12-03			X	phpMyAdmin 5.0.0 - SQL Injection	WebApps	PHP	CodeSecLab
2025-12-03			X	ResearchOS 6.7.2 - Cross-Site Scripting (XSS)	WebApps	PHP	CodeSecLab
2025-12-03			X	ResearchOS 6.7.2 - Cross-Site Scripting (XSS)	WebApps	PHP	CodeSecLab
2025-12-03			X	PluckCMS 4.7.10 - Unauthenticated File Upload	WebApps	PHP	CodeSecLab
2025-12-03			X	openOS Community Edition 8.0 - SQL Injection	WebApps	PHP	CodeSecLab
2025-12-02			X	YOURLS 1.8.2 - Cross-Site Request Forgery (CSRF)	WebApps	Multiple	CodeSecLab

Showing 1 to 15 of 46,470 entries

FIRST PREVIOUS 1 2 3 4 5 ... 3086 NEXT LAST

Databases	Links	Sites	Solutions
Exploits	Search Exploit DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	Search/Submit Manual	VulnHub	OffSec Cyber Range

★

ЗАДАЧИ

Активы

Задачи

Отчеты

Карты сети

Инструменты

Администрирование

Проект\_01

▼

Ru

admin

Главная / Список задач / Поиск уязвимостей / Уязвимое ПО / libqt4-opengl /

Информация по найденной уязвимости

Средний

CVE-2009-3272

Информация об уязвимости

Описание

Уязвимость потребления стека в WebKit.dll в WebKit в Apple Safari 3.2.3 и, возможно, в других версиях до 4.1.2, позволяет удаленным злоумышленникам вызывать отказ в обслуживании (сбой приложения) с помощью кода JavaScript, который вызывает eval в длинной строке, состоящей из последовательностей/.

CVE	CVE-2009-3272
БДУ	—
CVSS2 вектор	AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS2 балл	5
CVSS3 вектор	—
CVSS3 балл	—

Информация по уязвимому ПО

Название	libqt4-opengl
Связанные названия	libqt4-opengl, qt4-x11
Версия	4:4.8.7+dfsg-20astra3

Рекомендации

Конфигурация

Эксплоиты

exploitdb

<https://www.exploit-db.com/exploits/9606>

- **БДУ ФСТЭК России**: <https://bdu.fstec.ru/>
- NIST NVD: <https://nvd.nist.gov/>
- Chinese National Vulnerability Database (CNNVD):  
<https://www.cnvd.org.cn/>
- **Debian** GNU/Linux Security Bug Tracker  
<https://security-tracker.debian.org/tracker/>
- **Ubuntu** CVE Tracker  
<https://people.canonical.com/~ubuntu-security/cve/>
- **RHEL/CentOS** Security Data  
<https://www.redhat.com/security/data/metrics/>
- **Каталог уязвимостей Сканер-ВС**: <https://vulnerabilities.etecs.ru/>

## НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Web-call: call.gov.ru  
E-mail: info@ncc.gov.ru

РАЗВЕДЫВАТЕЛЬНАЯ АКЦИЯ АМЕРИКАНСКИХ СПЕЦСЛУЖБ  
С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ ФИРМЫ  
APPLE



ALRT-20230601.1 | 1 июня 2023 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Описание угрозы

Центры удаленного управления ВПО

addatamarket.net  
ans7tv.net  
anstv.net  
backuprabbit.com  
businessvideonews.com  
tagclick-cdn.com  
cloudsponcer.com  
datamarketplace.net  
mobilegamerstats.com  
snoweeanalytics.com  
tagclick-cdn.com  
topographyupdates.com  
unlimitedteacup.com  
virtuallaughing.com  
web-trackers.com  
growthtransport.com

Федеральной службой безопасности Российской Федерации совместно с Федеральной службой охраны Российской Федерации вскрыта разведывательная акция американских спецслужб, проведенная с использованием мобильных устройств фирмы Apple (США).

В ходе обеспечения безопасности российской телекоммуникационной инфраструктуры выявлены аномалии, характерные только для пользователей мобильных телефонов Apple и обусловленные работой ранее неизвестного вредоносного программного обеспечения (ВПО), использующего предусмотренные производителем программные уязвимости.

Установлено, что заражению подверглись несколько тысяч телефонных аппаратов этой марки. При этом кроме отечественных абонентов выявлены факты заражения зарубежных номеров и абонентов, использующих sim-карты, зарегистрированные на диппредставительства и посольства в России, включая страны блока НАТО и постсоветского пространства, а также Израиль, САР и КНР.

Заражение ВПО происходит по следующему алгоритму:

- Целевое iOS-устройство получает сообщение iMessage со специальным вложением, содержащим эксплойт
- Без какого-либо взаимодействия с пользователем эксплойт из сообщения вызывает выполнение вредоносного кода
- В ходе выполнения кода устанавливается соединение с сервером управления и происходит последовательная загрузка нескольких модулей вредоносной программы, включая дополнительные эксплойты для повышения привилегий
- После успешной отработки всех вредоносных компонентов загружается конечная вредоносная нагрузка
- Сообщение и вложение с эксплойтом удаляются в процессе заражения
- В результате злоумышленники могут получить несанкционированный доступ к информации о пользователе и системе, а также возможность выполнить произвольный код на уязвимом устройстве

С описанием методов выявления признаков функционирования ВПО на устройствах компании Apple можно ознакомиться в отчете компании «Лаборатория Касперского» по следующей ссылке:

<https://securelist.ru/operation-triangulation/107470/>

# СПАСИБО БОЛЬШОЕ ЗА ВНИМАНИЕ! ПРИХОДИТЕ К НАМ УЧИТЬСЯ!



@MASCOM\_UC

ПОДПИСЫВАЙТЕСЬ  
НА ОФИЦИАЛЬНЫЙ ТЕЛЕГРАМ-КАНАЛ!



<https://mascom-uc.ru/>



@UNDERLINESECURITY



Сделай свой проект  
чистым и безопасным  
вместе с PVS-Studio



**VOKRUG\_RBPO25**



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



**VOKRUG\_RBPO25**



**Учебные курсы  
по обеспечению безопасности  
значимых объектов КИИ  
Российской Федерации**

**Учебные курсы: «ПМ 5», «М 3.7»,**

## Информационная безопасность. Безопасность значимых объектов критической информационной инфраструктуры

С 01 января 2021 г. вступили в силу требования Приказа ФСТЭК России 2017 г. №235 к уровню подготовки специалистов подразделений обеспечения безопасности значимых объектов КИИ: Работники структурного подразделения по безопасности, специалисты по безопасности должны соответствовать следующим требованиям:

- наличие у руководителя структурного подразделения по безопасности высшего профессионального образования по направлению подготовки в области ИБ или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по направлению «Информационная безопасность»;
- прохождение не реже одного раза в 3 года обучения по программам повышения квалификации по направлению «Информационная безопасность».

По окончании обучения слушатели получают Диплом о профессиональной переподготовке.

**ВНИМАНИЕ!**  
ДАТЫ НА КУРС ОБСУЖДАЮТСЯ ИНДИВИДУАЛЬНО ПРИ ЗАКЛЮЧЕНИИ ДОГОВОРА!

В соответствии с Указом Президента РФ 2022 г. №250 и Постановлением Правительства РФ 2022 г. №1272, организации, являющиеся субъектами КИИ, обязаны «возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты». Указанное должностное лицо «должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки

Стоимость:  
Очное обучение **130 000 Р**  
Длительность: **502 ч**  
Форма обучения очно-заочная



Открытый курс

По окончании обучения вы получаете:



Необходимые документы:  
при отсутствии – прохождение курса невозможно

- Копия СНИЛС и диплома о высшем профессиональном образовании.



Согласовано с ФСТЭК России

# Серия учебных курсов по направлению «Обеспечение безопасности ЗО КИИ Российской Федерации»

## Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

С 01 января 2021 г. вступают в силу требования ФСТЭК к уровню подготовки специалистов подразделений по безопасности значимых объектов КИИ (см. изменения в Приказ ФСТЭК от 2017 г. №235):

- Руководитель подразделения (в зависимости от базового образования) должен иметь документ о профессиональной переподготовке по направлению «Информационная безопасность». Предлагаем к изучению курс ПМ 2 «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»;
- Работники подразделения (в зависимости от базового образования) должны иметь документ о повышении квалификации по направлению «Информационная безопасность».

По окончании обучения слушатели получают Удостоверение о повышении квалификации.

С 01 января 2021 г. вступают в силу требования ФСТЭК к уровню подготовки специалистов подразделений по безопасности значимых объектов КИИ (см. изменения в Приказ ФСТЭК от 2017 г. №235):

Руководитель подразделения (в зависимости от базового образования) должен иметь документ о профессиональной переподготовке по направлению «Информационная безопасность». Предлагаем к изучению курс ПМ 2 «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну». Работники подразделения (в зависимости от базового образования) должны иметь документ о повышении квалификации по направлению «Информационная безопасность».

Предлагаем к изучению курс М 3.7 «Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».

Стоимость:  
Очное обучение **53 000 Р**  
Длительность: **108 часов**  
Форма обучения очная очно-заочная дистанционная



Открытый курс

По окончании обучения вы получаете:



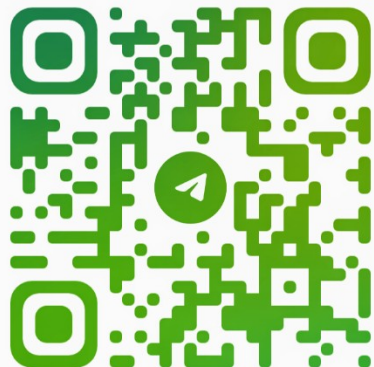
Необходимые документы:  
при отсутствии – прохождение курса невозможно

- Копия СНИЛС и диплома о высшем профессиональном образовании.



Согласовано с ФСТЭК России

# ПОДПИСЫВАЙТЕСЬ НА ОФИЦИАЛЬНЫЙ ТЕЛЕГРАМ-КАНАЛ!



@MASCOM\_UC



<https://mascom-uc.ru/>



@UNDERLINESECURITY



**Учебные курсы  
по процессам разработки  
безопасного программного обеспечения**

**Серия учебных курсов: «М БРПО...»**

---



# Серия учебных курсов по направлению «Безопасная разработка программного обеспечения»



## Специалист по процессам разработки безопасного программного обеспечения

Программа курса направлена на подготовку полноценного специалиста, обладающего всеми необходимыми компетенциями для ведения профессиональной деятельности, имеющего глубокие теоретические знания и практические навыки по направлению разработки безопасного программного обеспечения с учётом актуальной нормативной правовой базы.

**М БРПО-Спец**



02.09.2024-27.09.2024  
30.09.2024-25.10.2024



Пиков Виталий  
Александрович

Время  
200 часов / 20 дней



## Внедрение процессов разработки безопасного программного обеспечения в организации (для руководителей и ответственных)

Программа курса охватывает всё необходимое для руководителей предприятий и ответственных за процессы БРПО для получения знаний теоретических основ и приобретения практических навыков внедрения процессов разработки безопасного программного обеспечения (ГОСТ Р 56939–2016) на предприятии с учётом требований актуальной нормативной правовой базы.

**М БРПО-01**



03.09.2024-06.09.2024  
01.10.2024-04.10.2024



Пиков Виталий  
Александрович

Время  
40 часов / 4 дня



## Внедрение процессов разработки безопасного программного обеспечения для специалистов по информационной безопасности

Программа курса охватывает всё необходимое для получения знаний у специалистов по информационной безопасности теоретических основ актуальной отечественной и зарубежной нормативной правовой базы по направлению разработки безопасного программного обеспечения, а также приобретения практических навыков внедрения процессов разработки безопасного программного обеспечения (ГОСТ Р 56939–2016) в организации.

**М БРПО-02**



02.09.2024-06.09.2024  
30.09.2024-04.10.2024



Пиков Виталий  
Александрович

Время  
50 часов / 5 дней



## Сертификационные испытания с учётом требований по разработке безопасного программного обеспечения для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации

Программа курса охватывает всё необходимое для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации для получения знаний теоретических основ актуальной отечественной и зарубежной нормативной правовой базы по направлению сертификации программного обеспечения, проведению сертификационных испытаний и по разработке безопасного программного обеспечения, а также для приобретения практических навыков проведения сертификационных испытаний по требованиям доверия согласно требованиям приказа ФСТЭК России от 2 июня 2020 г. № 76 и по требованиям к сертификации средств защиты информации в Министерстве обороны Российской Федерации.

**М БРПО-03**



03.09.2024-23.09.2024  
01.10.2024-21.10.2024



Пиков Виталий  
Александрович

Время  
140 часов / 14 дней



## Формирование практических навыков по разработке безопасного программного обеспечения для разработчиков и программистов

Программа курса будет полезна разработчикам программного обеспечения, программистам и их руководителям для получения знаний теоретических основ актуальной отечественной и зарубежной нормативной правовой базы, а также для приобретения обширных практических навыков по разработке безопасного программного обеспечения, проведения сертификационных испытаний программных продуктов и внедрения процессов разработки безопасного программного обеспечения в организации.

**М БРПО-04**



03.09.2024-23.09.2024  
01.10.2024-21.10.2024



Пиков Виталий  
Александрович

Время  
140 часов / 14 дней



## Методология подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России

Программа курса охватывает всё необходимое для подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России, внедрения процессов разработки безопасного программного обеспечения на предприятии с учётом актуальной нормативной правовой базы.

**М БРПО-05**

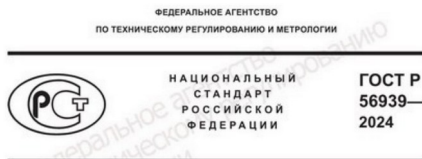


03.09.2024-05.09.2024  
01.10.2024-03.10.2024



Пиков Виталий  
Александрович

Время  
30 часов / 3 дня



Защита информации  
РАЗРАБОТКА БЕЗОПАСНОГО  
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

рологии

ГОСТ Р  
56939—  
2016

Москва  
Российский институт стандартизации  
2024

РАЗРАБОТКА БЕЗОПАСНОГО  
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Москва  
Стандартинформ  
2016



Москва

Об утверждении национального стандарта  
Российской Федерации

В соответствии со статьей 24 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации» и в целях:

1. Утвердить национальный стандарт Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» с датой введения в действие 20 декабря 2024 г.

Выдан ГОСТ Р 56939-2016.

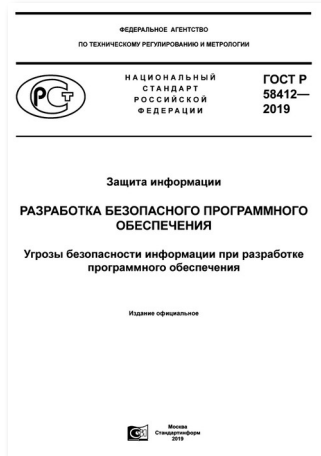
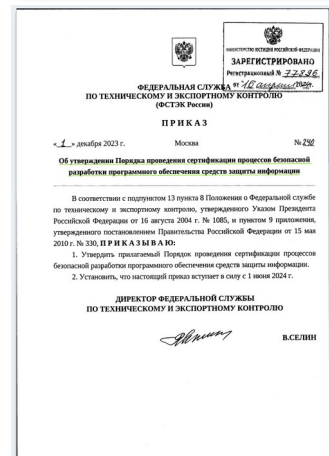
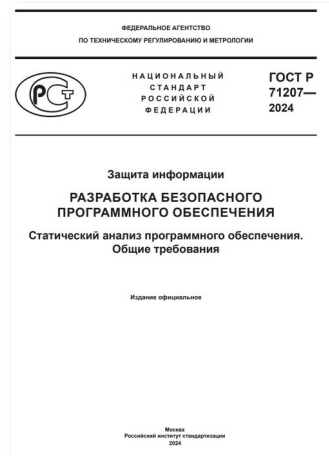
2. Управлению стандартизации обеспечить размещение информации об утвержденном настоящим приказом стандарте на официальном сайте Ростстандарта в информационно-телекоммуникационной сети «Интернет» (далее – официальный сайт) с учетом законодательства о стандартизации.

3. Федеральному государственному бюджетному учреждению «Российский институт стандартизации» разместить утвержденный настоящим приказом стандарт на официальном сайте в установленном порядке.

4. Закрепить утвержденный настоящим приказом стандарт за техническим комитетом по стандартизации № 362 «Защита информации» (ТК 362).

Руководитель

А.П.Шаев



Порядок проведения сертификации процессов безопасной разработки  
программного обеспечения средств защиты информации

1. Сертификация процессов проектирования и производства программного обеспечения (далее – процессы безопасной разработки программного обеспечения) средств защиты информации, содержащих сведения, составляющие государственную тайну или сведения с ограниченным доступом, осуществляется в соответствии с законодательством Российской Федерации, действующим на территории Российской Федерации, осуществляются на соответствие требованиям национального стандарта Российской Федерации ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 63-ст (далее – требования по безопасной разработке).

2. Сертификация процессов безопасной разработки программного обеспечения (далее – сертификация) осуществляется на основании договора, заключаемого изготовителем средств защиты информации (далее – изготовитель) с органом по сертификации.

3. Изготовитель при инициации сертификации процессов безопасной разработки программного обеспечения избирает для проведения сертификации аккредитованный ФСТЭК России орган по сертификации, согласованный с ним органом по сертификации.

4. Для получения сертификата соответствия изготовитель представляет в ФСТЭК России заявку на сертификацию (далее – заявка).

5. Заявка включает:

а) полное и сокращенное (при наличии) наименование изготовителя, его организационно-правовую форму;

б) адрес для корреспонденции изготовителя;

в) фамилию, имя и отчество (при наличии) лица, ответственного за сертификацию;

г) наименование, дата, номер и наименование средства защиты информации, утвержденного изготовителем.

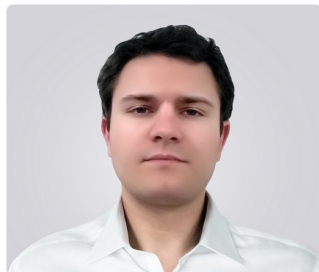
г) наименование, дата, номер и наименование средства защиты информации, утвержденного изготовителем.

В ногу со временем!!!

## Кто научит? - УЦ МАСКОМ !

### Задействовано более 10 лучших преподавателей

**Недогарок Антон Александрович**



Общий стаж работы:

Стаж преподавательской работы: более 11 лет

**Образование:** высшее, МГТУ им. Н.Э. Баумана, специальность - инженер. В 2021 г и 2022 г прошел повышение квалификации в АНО ДПО "Корпоративный университет Сбербанка" по программе "Летняя цифровая школа. Трек "Кибербезопасность".

Читает курсы по "Анализу и реверс-инжинирингу программного обеспечения", "Методы и средства криптографической защиты информации" и "Разработка и эксплуатация защищённых автоматизированных систем" в Московском Политехническом университете с 2016 г.

**Буянов Сергей Васильевич**



Общий стаж работы: более 35 лет

Стаж преподавательской работы: более 25 лет

**Образование:** высшее, кандидат технических наук, Московский авиационный институт по специальности «Вычислительные машины, системы, комплексы и сети». В 2021-24 годах прошёл профессиональную переподготовку в Новосибирском, Томском, Орловском университетах, в МГТУ им. Н. Э. Баумана.

Преподаёт и участвует в курсах: Верификация и валидация вычислительных систем, Компьютерная алгебра, Корпоративные информационные системы, Системы искусственного интеллекта, Проектирование и архитектура вычислительных систем, Научно-исследовательская деятельность.

**Большунов Валерий Владимирович**



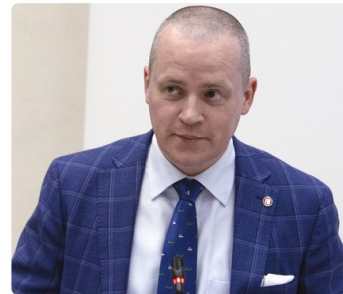
Общий стаж работы: более 22 лет

Стаж преподавательской работы: стаж наставничества/консультаций/обучения коллег - более 15 лет

**Образование:** высшее, с отличием Тамбовский военный авиационный инженерный институт по специальности «Автоматизированные системы обработки информации и управления». В 2017 году прошёл повышение квалификации в ДПО «УЦ ЦБИ» по направлению подготовки: «Техническая защита конфиденциальной информации, Информационная безопасность», «Организация и проведение работ по оценке (подтверждению) соответствия, Информационная безопасность», «Аттестация объектов информатизации по требованиям безопасности информации. Защита от несанкционированного доступа, Информационная безопасность».

Ведет занятия на учебных курсах по направлению разработки безопасного программного обеспечения.

**Пиков Виталий Александрович**



Общий стаж работы: более 26 лет

Стаж преподавательской работы: более 10 лет

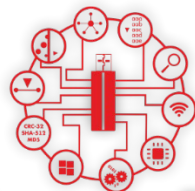
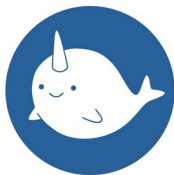


УЧЕБНЫЙ ЦЕНТР  
БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
Год основания: 1998

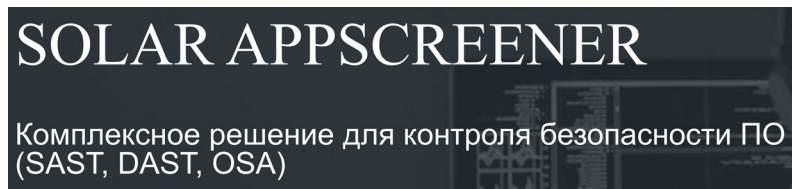








**Сканер-ВС**  
анализ защищённости



Ведутся дальнейшие переговоры с отечественными партнёрами-разработчиками решений для РБПО по вопросу предоставления программных инструментов для наших учебных курсов

**Курсы предназначены:**

- для руководителей и ответственных за организацию разработки безопасного программного обеспечения в организации;
- для специалистов по информационной безопасности;
- для архитекторов, разработчиков программного обеспечения и программистов;
- для экспертов органов по сертификации (испытательных лабораторий) различных систем сертификации средств защиты информации (ФСТЭК России, Минобороны России);
- для организаций, лицензиатов ФСТЭК России и Минобороны России, создающие средства защиты информации.

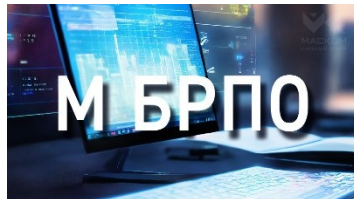




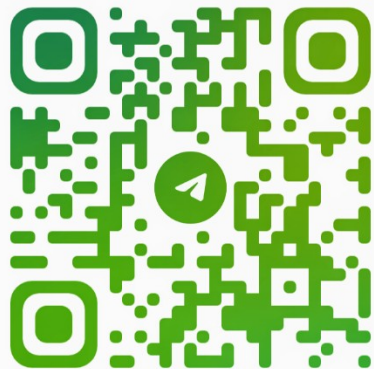
Программы курсов направлены на подготовку полноценного специалиста, обладающего всеми необходимыми компетенциями для ведения профессиональной деятельности и имеющего глубокие теоретические знания и практические навыки по направлению разработки безопасного программного обеспечения с учётом актуальной нормативной правовой базы (ГОСТ Р 56939–2024/2016, методологий SSDLC и DevSecOps).

**Успешно прошедшие обучение смогут самостоятельно разработать для своей организации:**

- ✓ дорожную карту (алгоритм) подготовки предприятия к сертификации процессов безопасной разработки программного обеспечения средств защиты информации в соответствии с требованиями ФСТЭК России;
- ✓ дорожную карту (алгоритм) внедрения БРПО на предприятии;
- ✓ проект Руководства БРПО предприятия;
- ✓ проекты документов предприятия в соответствии с ГОСТ Р 56939–2024/2016.



# ПОДПИСЫВАЙТЕСЬ НА ОФИЦИАЛЬНЫЙ ТЕЛЕГРАМ-КАНАЛ!



@MASCOM\_UC



<https://mascom-uc.ru/>



@UNDERLINESECURITY