Соответствие MaxPatrol SIEM требованиям ГОСТ Р 57580.1-2017

Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер

MaxPatrol SIEM дает полную видимость IT-инфраструктуры и выявляет инциденты информационной безопасности.

Для соответствия ГОСТ Р 57580.1-2017 о безопасности финансовых операций банкам необходимы SIEM-системы, поскольку они позволяют реализовать меры процесса «Управление инцидентами защиты информации». В этот процесс входят 33 обязательные технические меры по мониторингу и анализу событий защиты информации, обнаружению инцидентов и реагированию на них.

MaxPatrol SIEM позволяет покрыть еще 75 технических мер ГОСТ. Итого с помощью продукта заказчики могут реализовать 108 мер. В этом документе представлены требования, которые вы сможете покрыть с MaxPatrol SIEM.

Требования к системе защиты информации

Способы реализации мер защиты информации:

- «О» — реализация путем применения организационной меры защиты информации
- «Т» — реализация путем применения технической меры защиты информации
- «Н» — реализация является необязательной.

По желанию финансовой организации, способ «О» может быть реализован с помощью технической меры защиты информации.

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПРОЦЕСС 1 «Обеспечение защиты информации при управлении доступом»				
ПОДПРОЦЕСС «Управление учетными записями и правами субъектов логического доступа»				
УЗП.22	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего привилегированными правами логического доступа, позволяющими осуществить деструктивное воздействие, приводящее к нарушению выполнения бизнес-процессов или технологических процессов финансовой организации	**Н**	**Т**	**Т**

MaxPatrol SIEM — лидирующее отечественное SIEM-решение

Продукт внедрен более чем в 250 финансовых, промышленных, транспортных компаниях, в частном и государственном секторе, в органах власти.

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.23	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для финансовой организации, клиентов и контрагентов	Т	Т	Т
УЗП.24	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом	Т	Т	Т
УЗП.25	Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектов логического доступа	Т	Т	Т
УЗП.26	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению техническими мерами, реализующими многофакторную аутентификацию	Н	Т	Т
УЗП.27	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по изменению параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации	Н	Т	Т
УЗП.28	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами	Т	Т	Т
ПОДПРОЦЕСС «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»				
РД.39	Регистрация выполнения субъектами логического доступа ряда неуспешных последовательных попыток аутентификации	Н	Т	Т
РД.40	Регистрация осуществления субъектами логического доступа идентификации и аутентификации	Т	Т	Т
РД.41	Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС	Т	Т	Т
РД.42	Регистрация запуска программных сервисов, осуществляющих логический доступ	Н	Т	Т

Согласно исследованию IDC, MaxPatrol SIEM входит в тройку лидеров российского рынка SIEM. Другие отечественные SIEM-системы занимают не более 6% рынка.

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.43	Регистрация изменений аутентификационных данных, используемых для осуществления логического доступа	**Н**	**Т**	**Т**
ПОДПРОЦЕСС «Идентификация и учет ресурсов и объектов доступа»				
ИУ.1	Учет созданных, используемых и (или) эксплуатируемых ресурсов доступа	**О**	**Т**	**Т**
ИУ.2	Учет используемых и (или) эксплуатируемых объектов доступа	**О**	**О**	**Т**
ИУ.3	Учет эксплуатируемых общедоступных объектов доступа (в том числе банкоматов, платежных терминалов)	**О**	**О**	**Т**
ИУ.4	Контроль фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректного размещения в сегментах вычислительных сетей финансовой организации	**О**	**Т**	**Т**
ИУ.5	Контроль выполнения операций по созданию, удалению и резервному копированию ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин)	**Н**	**Т**	**Т**
ИУ.6	Контроль фактического состава эксплуатируемых объектов доступа и их корректного размещения в сегментах вычислительных сетей финансовой организации	**Н**	**О**	**Т**
ИУ.7	Регистрация событий защиты информации, связанных с созданием, копированием, в том числе резервным, и (или) удалением ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин)	**Н**	**Т**	**Т**
ИУ.8	Регистрация событий защиты информации, связанных с подключением (регистрацией) объектов доступа в вычислительных сетях финансовой организации	**Н**	**Н**	**Т**
ПРОЦЕСС 2 «Обеспечение защиты вычислительных сетей»				
ПОДПРОЦЕСС «Сегментация и межсетевое экранирование вычислительных сетей»				
СМЭ.21	Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей финансовой организации	**Т**	**Т**	**Т**

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПОДПРОЦЕСС «Выявления вторжений и сетевых атак»				
ВСА.1	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации	Н	Н	Т
ВСА.2	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между вычислительными сетями финансовой организации и сетью Интернет	Н	Т	Т
ВСА.3	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет	Н	Н	Т
ВСА.4	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным логическим доступом к ресурсам доступа, размещенным в вычислительных сетях финансовой организации, подключенных к сети Интернет	Н	Т	Т
ВСА.5	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным удаленным доступом	Н	Т	Т
ВСА.6	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным логическим доступом к ресурсам доступа, размещенным во внутренних вычислительных сетях финансовой организации	Н	Н	Т
ВСА.7	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным доступом к аутентификационным данным легальных субъектов доступа	Н	Н	Т
ПОДПРОЦЕСС «Защита беспроводных сетей»				
ЗБС.7	Реализация и контроль информационного взаимодействия внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3 настоящей таблицы, в соответствии с установленными правилами и протоколами сетевого взаимодействия	Н	Т	Т

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗБС.10	Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3 таблицы 20	Н	Т	Т
ПРОЦЕСС 3 «Контроль целостности и защищенности информационной инфраструктуры»				
ЦЗИ.12	Контроль размещения и своевременного обновления на серверном и сетевом оборудовании ПО средств и систем защиты информации, прикладного ПО, ПО АС, системного ПО и сигнатурных баз средств защиты информации, в том числе с целью устранения выявленных уязвимостей защиты информации	О	О	Т
ЦЗИ.13	Контроль размещения и своевременного обновления на АРМ пользователей и эксплуатационного персонала ПО средств и систем защиты информации, прикладного ПО, ПО АС и системного ПО, в том числе с целью устранения выявленных уязвимостей защиты информации	О	О	Т
ЦЗИ.20	Контроль состава разрешенного для использования ПО АРМ пользователей и эксплуатационного персонала	О	Т	Т
ЦЗИ.22	Контроль состава ПО серверного оборудования	Н	О	Т
ЦЗИ.23	Контроль состава ПО АРМ пользователей и эксплуатационного персонала, запускаемого при загрузке операционной системы	Н	Т	Т
ЦЗИ.28	Регистрация установки, обновления и (или) удаления ПО АС, ПО средств и систем защиты информации, системного ПО на серверном и сетевом оборудовании	Н	Т	Т
ЦЗИ.29	Регистрация установки, обновления и (или) удаления прикладного ПО, ПО АС, ПО средств и систем защиты информации, системного ПО на АРМ пользователей и эксплуатационного персонала	Н	Т	Т
ЦЗИ.30	Регистрация запуска программных сервисов	Н	Н	Т
ЦЗИ.31	Регистрация результатов выполнения операций по контролю состава ПО серверного оборудования, АРМ пользователей и эксплуатационного персонала	Н	Н	Т
ЦЗИ.32	Регистрация результатов выполнения операций по контролю состава ПО АРМ пользователей и эксплуатационного персонала	Н	Т	Т

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЦЗИ.33	Регистрация результатов выполнения операций по контролю состава ПО, запускаемого при загрузке операционной системы АРМ пользователей и эксплуатационного персонала	**Н**	**Т**	**Т**
ПРОЦЕСС 4 «Защита от вредоносного кода»				
ЗВК.11	Контроль отключения и своевременного обновления средств защиты от вредоносного кода	**Т**	**Т**	**Т**
ЗВК.22	Регистрация операций по проведению проверок на отсутствие вредоносного кода	**Т**	**Т**	**Т**
ЗВК.23	Регистрация фактов выявления вредоносного кода	**Т**	**Т**	**Т**
ЗВК.24	Регистрация неконтролируемого использования технологии мобильного кода <*>	**Т**	**Т**	**Т**
ЗВК.25	Регистрация сбоев в функционировании средств защиты от вредоносного кода	**Т**	**Т**	**Т**
ЗВК.26	Регистрация сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода	**Т**	**Т**	**Т**
ЗВК.27	Регистрация отключения средств защиты от вредоносного кода	**Т**	**Т**	**Т**
ЗВК.28	Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода	**Т**	**Т**	**Т**
ПРОЦЕСС 5 «Предотвращение утечек информации»				
ПУИ.28	Регистрация использования разблокированных портов ввода-вывода информации СВТ	**Н**	**Т**	**Т**
ПУИ.29	Регистрация операций, связанных с осуществлением доступа работниками финансовой организации к ресурсам сети Интернет	**Н**	**Т**	**Т**
ПУИ.30	Регистрация фактов вывода информации на печать	**Н**	**Т**	**Т**

Для реализации процесса 6 необходима SIEM-система

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПРОЦЕСС 6 «Управление инцидентами защиты информации»				
ПОДПРОЦЕСС «Мониторинг и анализ событий защиты информации»				
МАС.1	Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации	Т	Т	Т
МАС.2	Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевым оборудованием, в том числе активным сетевым оборудованием, маршрутизаторами, коммутаторами	Н	Т	Т
МАС.3	Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевыми приложениями и сервисами	Н	Т	Т
МАС.4	Организация мониторинга данных регистрации о событиях защиты информации, формируемых системным ПО, операционными системами, СУБД	Н	Т	Т
МАС.5	Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями	Т	Т	Т
МАС.6	Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов	Т	Т	Т
МАС.7	Организация мониторинга данных регистрации о событиях защиты информации, формируемых средствами (системами) контроля и управления доступом	Н	Н	Т
МАС.8	Централизованный сбор данных регистрации о событиях защиты информации, формируемых объектами информатизации, определенных мерами МАС.1 - МАС.7 таблицы 33	Н	Т	Т
МАС.9	Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации	Т	Т	Т
МАС.10	Контроль формирования данных регистрации о событиях защиты информации объектов информатизации, определенных мерами МАС.1 - МАС.7 таблицы 33	О	Т	Т

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
МАС.11	Реализация защиты данных регистрации о событиях защиты информации от раскрытия и модификации, двухсторонней аутентификации при передаче данных регистрации с использованием сети Интернет	Н	Т	Т
МАС.12	Обеспечение гарантированной доставки данных регистрации о событиях защиты информации при их централизованном сборе	Н	Т	Т
МАС.13	Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации	Т	Т	Т
МАС.14	Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечение целостности и доступности хранимых данных регистрации	Т	Т	Т
МАС.15	Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет	Т	Т	Н
МАС.16	Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение пяти лет	Н	Н	Т
МАС.17	Обеспечение возможности выполнения операции нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации	Н	Т	Т
МАС.18	Обеспечение возможности выявления и анализа событий защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД <*>	Т	Т	Т
МАС.19	Обеспечение возможности определения состава действий и (или) операций конкретного субъекта доступа	Т	Т	Т
МАС.20	Обеспечение возможности определения состава действий и (или) операций субъектов доступа при осуществлении логического доступа к конкретному ресурсу доступа	Т	Т	Т
МАС.21	Регистрация нарушений и сбоев в формировании и сборе данных о событиях защиты информации	Н	Т	Т
МАС.22	Регистрация доступа к хранимым данным о событиях защиты информации	Т	Т	Т

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
МАС.23	Регистрация операций, связанных с изменением правил нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации	Н	Т	Т
ПОДПРОЦЕСС «Обнаружение инцидентов защиты информации и реагирование на них»				
РИ.1	Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации	О	Т	Т
РИ.2	Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов финансовой организации	О	Т	Т
РИ.3	Классификация инцидентов защиты информации с учетом степени их влияния (критичности) на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов финансовой организации	О	О	Т
РИ.5	Установление и применение единых правил регистрации и классификации инцидентов защиты информации в части состава и содержания атрибутов, описывающих инцидент защиты информации, и их возможных значений	О	Т	Т
РИ.10	Своевременное (оперативное) оповещение членов ГРИЗИ о выявленных инцидентах защиты информации	Н	Т	Т
РИ.15	Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации	Т	Т	Т
РИ.16	Разграничение доступа членов ГРИЗИ к информации об инцидентах защиты информации в соответствии с определенным распределением ролей, связанных с реагированием на инциденты защиты информации	Н	Т	Т
РИ.17	Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет	Т	Т	Н
РИ.18	Обеспечение возможности доступа к информации об инцидентах защиты информации в течение пяти лет	Н	Н	Т
РИ.19	Регистрация доступа к информации об инцидентах защиты информации	Т	Т	Т

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ПРОЦЕСС 7 «Защита среды виртуализации»				
ЗСВ.32	Регистрация операций, связанных с запуском (остановкой) виртуальных машин	Т	Т	Т
ЗСВ.33	Регистрация операций, связанных с изменением параметров настроек виртуальных сетевых сегментов, реализованных средствами гипервизора	Н	Т	Т
ЗСВ.34	Регистрация операций, связанных с созданием и удалением виртуальных машин	Т	Т	Т
ЗСВ.35	Регистрация операций, связанных с созданием, изменением, копированием, удалением базовых образов виртуальных машин	Т	Т	Т
ЗСВ.36	Регистрация операций, связанных с копированием текущих образов виртуальных машин	Т	Т	Т
ЗСВ.37	Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации	Т	Т	Т
ЗСВ.38	Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации	Т	Т	Т
ЗСВ.39	Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации	Т	Т	Т
ЗСВ.40	Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам	Т	Т	Т
ЗСВ.41	Регистрация операций, связанных с запуском (остановкой) ПО серверных компонент виртуализации	Н	Н	Т
ЗСВ.42	Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации	Т	Т	Т
ЗСВ.43	Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин	Т	Т	Т

Требования к организации и управлению защитой информации

MaxPatrol SIEM сертифицирован ФСТЭК и Минобороны России и входит в реестр отечественного ПО.

Направление 2
«Реализация процесса системы защиты информации»

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РЗИ.11	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 4 класса	**Н**	**Н**	**Т**
РЗИ.12	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 5 класса	**Н**	**Т**	**Н**
РЗИ.13	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса	**Т**	**Н**	**Н**

300 источников поддерживаются.

Среди них популярные системы российских вендоров — «1С», «Кода безопасности», «Лаборатории Касперского», InfoWatch.

Направление 3
«Контроль процесса системы защиты информации»

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
КЗИ.2	Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий: • контроль фактического размещения технических мер защиты информации в информационной инфраструктуре финансовой организации; • контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации	**О**	**О**	**Т**
КЗИ.4	Периодический контроль (тестирование) полноты реализации технических мер защиты информации	**О**	**Т**	**Т**
КЗИ.9	Регистрация операций по установке и (или) обновлению ПО технических средств защиты информации	**Н**	**Т**	**Т**
КЗИ.10	Регистрация операций по обновлению сигнатурных баз технических средств защиты информации (в случае их использования)	**Н**	**Т**	**Т**

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
КЗИ.11	Регистрация операций по изменению параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации	**н**	**т**	**т**
КЗИ.12	Регистрация сбоев (отказов) технических мер защиты информации	**н**	**т**	**т**

Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЖЦ.22	Регистрация внесения изменений в АС, включая обновление прикладного ПО	**н**	**о**	**о**
ЖЦ.23	Регистрация операций по изменению параметров настроек технических мер системы защиты информации АС	**о**	**т**	**т**

Для небольших инфраструктур существуют объединенные лицензии **MaxPatrol SIEM All-in-One**. Есть три варианта лицензии: до 250, 500 и 1000 узлов.

Специально для кредитных организаций есть лицензия на 100 сетевых узлов за 2,2 млн рублей.

Подробнее

Отзывы банков

Ольга Казанская,
председатель правления
банка «Оранжевый»

Банк «Оранжевый»

«С внедрением решения MaxPatrol SIEM мы получили эффективный инструмент анализа в режиме реального времени всех событий безопасности, исходящих от множества сетевых устройств и приложений. Это позволило сотрудникам отдела информационной безопасности оперативно реагировать на любые события ИБ до наступления существенного ущерба. Время обработки событий также значительно сократилось».

Игорь Чумаковский,
Председатель Правления
АО «КБ «Солидарность»

АО «КБ «Солидарность»

«С помощью MaxPatrol SIEM существенно повысилась скорость обработки инцидентов информационной безопасности».

Другие отзывы партнеров и заказчиков смотрите на странице MaxPatrol SIEM на сайте ptsecurity.com.

Вступайте в комьюнити MaxPatrol SIEM

Наши эксперты, партнеры и заказчики ответят на вопросы, посоветуют полезные ссылки и будут держать в курсе новостей продукта:
t.me/MPSIEMChat

Как пропилотировать MaxPatrol SIEM

Результаты 23 пилотов MaxPatrol SIEM

Мы собрали в отчете популярные задачи пилотных внедрений, топ подключенных источников и выявленных инцидентов ИБ:

ptsecurity.com/ru-ru/research/analytics/incidents-siem-2020/

1 неделя	4 недели	2 недели	1 неделя
Подписание NDA, заполнение анкеты об инфраструктуре, подготовка источников событий ИБ	Разворачивание SIEM на пилотном сегменте, подключение источников и настройка правил	Пилотирование, экспертный мониторинг специалистами PT Expert Security Center (по договоренности)	Отчет по итогам пилота

ПОПРОБОВАТЬ

Проведите пилотное внедрение

Оцените возможности MaxPatrol SIEM на вашей инфраструктуре — заполните заявку на сайте и начните выявлять актуальные угрозы с помощью экспертизы Positive Technologies.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays