Информзащита
Системный интегратор

Тенденции + по продуктам и услугам

январь 2024

Оглавление

В фокусе

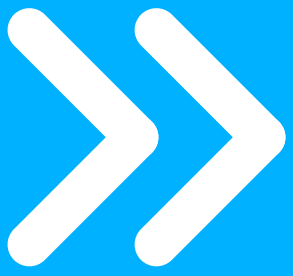
Госдума приняла в первом чтении законопроекты об административной и уголовной ответственности за утечки персональных данных.

На весенней сессии в Госдуме РФ депутаты рассмотрят новые законопроекты, касающиеся информационной безопасности.

На повестке будут стоять вопросы ответственности компаний перед гражданами за утечки персональных данных, легализации белых хакеров и законодательного приравнивания SIM-карт к средствам платежей.

В Госдуме доработают законопроект об отстранении топ-менеджеров российских банков за утечки информации.

Новости компаний



Тенденции по продуктам и услугам

В рамках партнерства с DataSpace Angara Security будет предоставлять услуги коммерческого SOC-центра,

включая мониторинг и управление инцидентами ИБ, реагирование на инциденты и компьютерную криминалистику (DFIRMA), OSINT и защиту бренда, а также интеграцию решений SOC для выстраивания собственных процессов информационной безопасности заказчиков.

DataSpace | Angara Security | SOC

Beeline cloud объявил о запуске платформы Cloud SD-WAN

— специализированного решения для управления сетевой инфраструктурой предприятий. В создании нового облачного сервиса приняла участие «Лаборатория Касперского», а в основу продукта положена платформа Kaspersky SD-WAN.

Beeline | Лаборатория Касперского | Cloud SD-WAN

Компания R-Vision заявила о расширении функциональных возможностей технологии R-Vision SIEM,

чтобы улучшить работу с поступающими событиями кибербезопасности. Версия 1.3 имеет ряд обновлений: разработчик расширил функционал для сбора и обработки событий, интегрировал новые инструменты для работы с контентом и поиском, добавил конструктор отчетов и расширил методы интеграции с внешними системами.

R-Vision | SIEM

Компания "Аладдин" запустила обновленный центр сертификации под Linux - Aladdin Enterprise CA 2.0.

Это российский аналог центра выдачи сертифика¬тов Microsoft Certificate.

Аладдин | Linux | Aladdin Enterprise CA 2.0

Компания Positive Technologies анонсировала выпуск пакета экспертизы для системы глубокого анализа технологического трафика PT ISIM.

В решении расширилась поддержка распределенной системы управления (РСУ) DeltaV компании Emerson. Теперь PT ISIM обнаруживает больше событий кибербезопасности и позволяет эффективнее обеспечивать защиту.

Positive Technologies | PT ISIM

ГК «Солар» заявила о выпуске новой версии шлюза веб-безопасности (SWG) Solar webProxy 4.0.

В обновлении добавлен ряд новых компонентов — агент Solar webProxy, который перенаправляет трафик приложений на веб-прокси, сквозной поиск ресурсов, который упрощает взаимодействие пользователя с системой, а также конструктор условий, который позволяет создавать более сложные правила доступа сотрудников к веб-ресурсам.

Солар | SWG | Solar webProxy 4.0

ГК «Солар» представила новую версию Solar Dozor 7.11.

В обновленной DLP-системе нашла реализацию уникальная на российском рынке возможность контроля информации, которая передаётся через средства ВКС и мессенджеры, позволяющая не допускать утечки данных в процессе их трансляции на экране. Помимо этого, продукт был дополнен некоторыми новыми инструментами, среди которых перехват QR-кодов и интеграционный модуль.

Солар | DLP | Solar Dozor 7.11

Компания «Код Безопасности» сообщила о том, что новая версия продукта Континент 4.1.7.1446 прошла сертификационные испытания ФСТЭК России и поступает в продажу.

Код Безопасности | Континент 4.1.7.1446 | ФСТЭК России

Группа компаний «Гарда» обновила систему обезличивания данных.

Теперь «Гарда Маскирование 1.6» поддерживает работу с базами данных 1С – пользователи 1С ERP смогут передавать конфиденциальные данные в третьи руки с соблюдением всех законодательных норм.

Гарда Маскирование 1.6 | 1С ERP

Эксперты Глобального центра исследований и анализа угроз (GReAT) ЛК создали новый метод обнаружения индикаторов заражения устройств на iOS сложным шпионским ПО, таким как Pegasus, Reign и Predator.

Специалисты разработали ***инструмент для поиска ранее неизвестных следов в Shutdown.log***, чтобы пользователи могли самостоятельно проверить свои устройства iPhone.

Лаборатория Касперского | GReAT | iOS

«Группа Астра» заявила о запуске нового продукта – платформы Astra Automation.

Решение используется для автоматизации ИТ-инфраструктуры, которая построена на базе продуктов Группы и ее партнеров. Дата официального релиза намечена на 15 февраля 2024 года. Astra Automation представляет собой программную платформу, которая позволяет автоматизировать установку и обновление ПО, конфигурирование сетевого оборудования, настройку правил безопасности (в соответствии с требованиями регуляторов либо на основе собственных политик заказчика) и другие рутинные задачи по обслуживанию ИТ-инфраструктуры.

Группа Астра | Astra Automation

В «Лаборатории Касперского» сообщили о выпуске игры — интерактивного симулятора, моделирующего атаки программ-вымогателей

Лаборатория Касперского

За 12 месяцев 2023 года выручка «Кода Безопасности» составила более 9,2 миллиардов рублей. Это на 24% больше результатов предыдущего года.

67,7% продаж компании составляют продукты сетевой безопасности – NGFW «Континент 4» (3,14 млрд рублей) и «Континент 3» (3,1 млрд). 20% принес сегмент защиты конечных точек: «Соболь» – 1,03 млрд, Secret Net Studio – 804 млн. Замыкает тройку средство защиты жизненного цикла виртуальных машин vGate с долей 5,6%, или 518 млн.

+ 24% выручка Кода Безопасности за 2023 год (9,2 млрд)

Континент 4, Континент 3	**67,7%** (6,24 млрд руб)
Соболь, Secret Net Studio	**20%** (1,83 млрд руб)
vGate	**5,6%** (0,5 млрд руб)

Партнерства

Axoft  MTC RED

Axoft займется поставками на территории России платформы для управления безопасной разработкой ПО MTC RED ASOC, системы повышения киберграмотности сотрудников Security Awareness, технологий комплексной защиты контейнерных приложений и ряда других решений MTC RED.

Security Vision  Газинформсервис

Security Vision и «Газинформсервис» подтвердили совместимость защищенной системы управления базами данных (СУБД) Jatoba и автоматизированной платформы кибербезопасности Security Vision в процессе всестороннего тестирования.

UserGate  Innostage

UserGate присвоила Innostage высший партнерский статус Platinum.

Гарда  K2 Кибербезопасность

«Гарда» и «K2 Кибербезопасность» объявили о сотрудничестве. На старте они будут развивать направление по защите и маскированию баз данных. Партнерство компаний позволит заказчикам с помощью решения Гарда DBF усилить защиту конфиденциальной информации, управлять доступом к базам данных, проводить мониторинг и аудит действий пользователей и предотвращать попытки несанкционированного доступа в СУБД. С помощью Гарда Маскирование — выявлять чувствительные данные в информационных системах, обезличивать данные в СУБД, обеспечивать необходимую защиту информации при передаче и пр.

Fortis  Аладдин

Компания Fortis, отечественный дистрибутор высокотехнологичных решений в сфере кибербезопасности, и компания Аладдин подписали дистрибуторское соглашение.

F.A.C.C.T. Бизнес Айти

F.A.C.C.T. и компания «Бизнес Айти» сообщили о запуске совместной MSSP-программы. В ходе партнёрства «Бизнес Айти» выступит оператором решения F.A.C.C.T. Attack Surface Management (ASM), которое позволяет отслеживать у клиентов незащищенные участки инфраструктуры, вероятные уязвимости, теневые цифровые активы и неправильное настроенные элементы сети, которые могут быть применены хакерами в атаках.

Softline КлаудРан

ГК Softline объявила о включении решения для защиты контейнеров и Kubernetes Luntry от вендора «КлаудРан» в Softline Universe. Softline Universe – это активно развивающаяся модель предоставления доступа к экосистеме прикладных интегрированных сервисов, вычислительным ресурсам и инфраструктуре через Интернет.

Softline Стингрей Технолоджиз

ГК Softline объявил о включении в свой портфель вендоров компании «Стингрей Технолоджиз», специализирующейся на информационной безопасности мобильных приложений.

Softline команда

ГК Softline расширила экспертизу и компетенций в области информационной безопасности и облачных технологий за счет присоединения команды специалистов и приобретения портфеля оборудования. Компания получила компетенции в области построения и аттестации комплексных систем информационной безопасности уровня ЦОД, многоуровневых распределенных информационных систем, консалтинга по лицензированию в области информационной безопасности, а также приобрела экспертизу в сфере высоконагруженных инфраструктур. Группа также расширила портфель аппаратного обеспечения, дополнив его комплектом высокопроизводительного отказоустойчивого вычислительного оборудования, пригодного для заказчиков федерального уровня.

MaxPatrol EDR внесен в единый реестр отечественного ПО.

Компания **«ИнфоТеКС»** заявила о получении сертификата ФСБ России № СФ/124-4702 от 28.12.2023,

который удостоверяет, что ViPNet CSP версии 4.4.8 соответствует требованиям к средствам криптозащиты информации классов КС1, КС2 и КС3, требованиям к средствам ЭЦП, которые утверждены приказом ФСБ России от 27.12. 2011 г. № 796, установленным для классов КС1, КС2 и КС3, и может применяться для криптозащиты информации, не содержащей информации, составляющих гостайну. Сертификат действителен до 28.12.2026.

Компания **Step Logic** сообщила, что технологическая платформа для автоматизации анализа данных и расследования инцидентов Security Data Lake включена в Реестр российского ПО

(реестровая запись №20657 от 25.12.2023) по классу «02.08 Средства мониторинга и управления». Программный продукт Security Data Lake является собственной разработкой STEP LOGIC для центров кибербезопасности (SOC), объединяющей в себе функции мониторинга событий и выявления инцидентов (SIEM), реагирования и расследования (IRP), а также автоматизации и оркестрации этих процессов (SOAR).

Innostage представил зарубежным партнерам в Саудовской Аравии и Объединенных Арабских Эмиратах проект Межвузовского Центра противодействия киберугрозам.

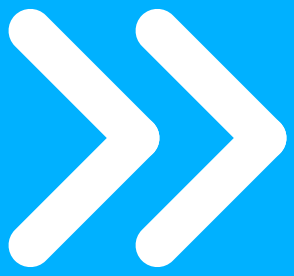
Особый акцент был сделан на том, как с помощью SOC обучать ИБ-специалистов.

Олег Бакшинский назначен на должность операционного директора Angara Security

и возглавит управление ключевыми блоками компании – HR, IT, проектным офисом, финансовым департаментом, административным отделом и направлением маркетинга.

Вероника Гименез (Тараба) возглавила маркетинг Angara Security. Инга Оськина стала директором по персоналу Angara Security.

Ключевые регуляторные инициативы



Тенденции по продуктам и услугам

Персональные данные

Госдума приняла в первом чтении законопроекты об административной и уголовной ответственности за утечки персональных данных.

Поправки в законодательство, в частности, предполагают, что если утечка коснется от 1 тыс. до 10 тыс. субъектов, то штраф для юрлиц составит от 3 до 5 млн руб.; от 10 тыс. до 100 тыс. субъектов - от 5 до 10 млн рублей; более 100 тыс. - от 10 до 15 млн руб. За повторные утечки предлагаются оборотные штрафы - для граждан в размере от 400 тыс. до 600 тыс. руб., для должностных лиц - от 2 млн до 4 млн руб., в отношении юридических лиц предусматривается оборотный штраф - от 0,1% до 3% выручки за календарный год или за часть текущего года, не менее 15 млн рублей и не более 500 млн рублей.

Центральный банк

ЦБ РФ подготовил проект закона, предполагающий десятилетнее отстранение топ-менеджеров крупных финансовых учреждений, страховых компаний, пенсионных фондов и микрофинансовых организаций за серьёзные нарушения в области утечки конфиденциальных данных или банковской тайны.

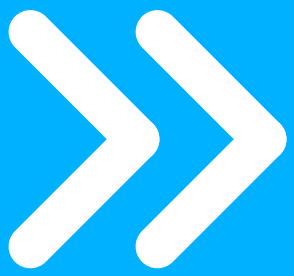
Глава думского комитета по финансовому рынку Анатолий Аксаков заявил, что проект закона будет доработан, в том числе будут пересмотрены сроки отстранения руководящих лиц. Скорректированный проект закона, скорее всего, поступит на рассмотрение в Госдуму РФ в феврале 2024 года. Депутаты постараются принять его в первой половине года, чтобы с второго полугодия он вступил в законную силу.

Безопасная разработка

Национальный стандарт Р 56939 «Защита информации. Разработка безопасного программного обеспечения»

2016 года признан устаревшим и на замену ему разработан проект нового ГОСТа. Документ опубликован на ***сайте ФСТЭК***, его публичное обсуждение продлится до 15 февраля 2024 года.

Тенденции



Тенденции по продуктам и услугам

Инфосистемы Джет

отчет "Итоги года"

Ландшафт угроз и общее количество атак в 2023 году отличаются незначительно.

+ 11 % общего числа **атак** зафиксировано в 2023 году

Наибольшее число наблюдаемых инцидентов связано с заражением вредоносным ПО: как через посещение сайтов с вредоносным контентом, так и через фишинговые атаки. Проблема проникновения злоумышленников через подрядные организации становится особенно острой в 2023 году. Результаты расследований показали, что **причиной каждого пятого инцидента стал взлом ИТ-подрядчика.**

На проектах по мониторингу внешних цифровых рисков у

72 % компаний были найдены **критические уязвимости на периметре**

для которых существуют публичные эксплойты. Подобные уязвимости могут послужить точкой входа злоумышленника в инфраструктуру компании.

Рост спроса на услуги:

+ 30 % запросы на проведение **внешнего тестирования на проникновение** в 2023 году

в **3,2** раза увеличился спрос на решения для управления привилегированным доступом **(PIM/PAM)** за последние годы

в **2,5** раза увеличилось количество обращений от организаций на проведение **расследований и оказание экспертных консультаций** в 2023 году

в **2** раза увеличилось спрос на проведение **киберучений** в крупных компаниях за 2023 год

В основном за этой услугой обращались компании из сфер телекома, финансов и промышленности. Рост спроса на киберучения подтверждают эксперты Positive Technologies и ГК «Солар». В 2023 г. количество проведенных ГК «Солар» коммерческих учений выросло в 5 раз относительно 2022 г. В 2024 г. ГК «Солар» прогнозирует рост еще в 3 раза.

Лаборатория Касперского

По данным исследования «Лаборатории Касперского», многие российские компании готовы инвестировать в направление информационной безопасности в ближайшие год-полтора, чтобы повысить уровень своей защищённости от киберугроз.

43 % респондентов сообщили, что в планах — инвестировать в **ПО для обнаружения угроз**

Более трети компаний планируют выделять бюджет на обучение персонала:

39 % на тренинги для специалистов по кибербезопасности

32 % на тренинги по киберграмотности для сотрудников неспециализированных подразделений

Среди других планируемых мер

36 % внедрение ПО для **защиты конечных устройств**

27 % внедрение **облачных решений SaaS**

21 % **наём дополнительных специалистов** в области информационной безопасности

+ 47 % количество кибератак на пользователей **мобильных устройств** в России в 2023 г.

в 5 раз увеличилось количество **фишинговых и скам ссылок** в доменной зоне .RU, которые заблокировала ЛК в 2023 году

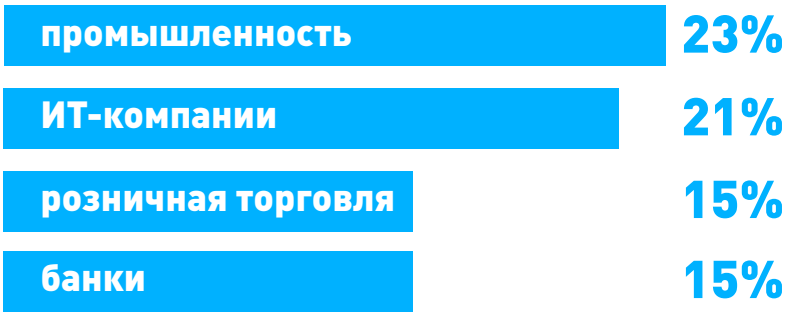
МТС RED SOC

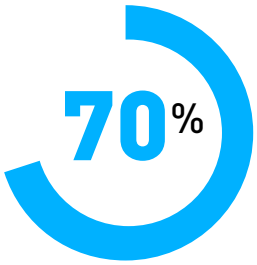
+ 43 % атак выявлено за 2023 год
(более 50 000 инцидентов ИБ)

При этом отмечается сокращение доли критичных инцидентов.

2022 год - **40-45%**	2023 год - **25%**

Больше всего высококритичных инцидентов было зафиксировано





Самыми распространенными методами атак
в 2023 году стали
сетевые атаки, попытки обхода технических средств защиты и заражения вредоносным ПО.
Эти вектора составили совокупно около 70% от общего числа инцидентов информационной безопасности в российских компаниях.

Код Безопасности

в **10-15** раз выросло количество **мошеннических рассылок** сотрудникам компаний от лица руководителей с октября по настоящее время

BI.ZONE CESP

68% целевых атак на российские компании начинается с **электронного письма**

+ 70% доля **фишинговых писем** в 2023 году

Главной мишенью стала **сфера транспорта и логистики**. Эта же отрасль — лидер по темпам роста фишинговых атак.

в **2,4** раза увеличилось доля **писем с вредоносными вложениями** за 2023 год

Абсолютным лидером стал **промышленный сектор**: в этой сфере процент писем с ВПО почти в 6 раз превышает средний показатель.

Страховые фирмы, которые развивают направление покрытий ущерба организаций от последствий хакерских атак, в 2023 году смогли получить на 80% больше премий, чем в 2022 году, достигнув показателей в 1,3 млрд рублей.

В подобных страховых продуктах, как заявили в ПСБ, на данный момент в России в большей степени заинтересованы крупные финансовые учреждения и промышленные предприятия, в большинстве своём, представляющие топливно-энергетический комплекс и металлургию. В пакеты, которые предлагаются страховыми компаниями, также может входить кибераудит.

В течение 2023 года система фильтрации **DDoS-Guard** зафиксировала 2,26 млн кибератак, направленных против различных российских организаций.

Это число на 80% превышает показатели 2022 года и на 1224% больше, чем в 2021 году. Специалисты отметили изменение тактики злоумышленников: они сосредоточили внимание на региональных поддоменах, а также на различных технических сервисах целевых организаций. Кроме того, в 2023 году сохранялся тренд на использование IoT-устройств в ботнетах.

Информзащита
Системный интегратор

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Сервисный центр

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru

IZ:SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru