

Обзор новостей по теме информационной безопасности

Центр компетенций
по информационной
безопасности

01 октября 2025 г.

Содержание:

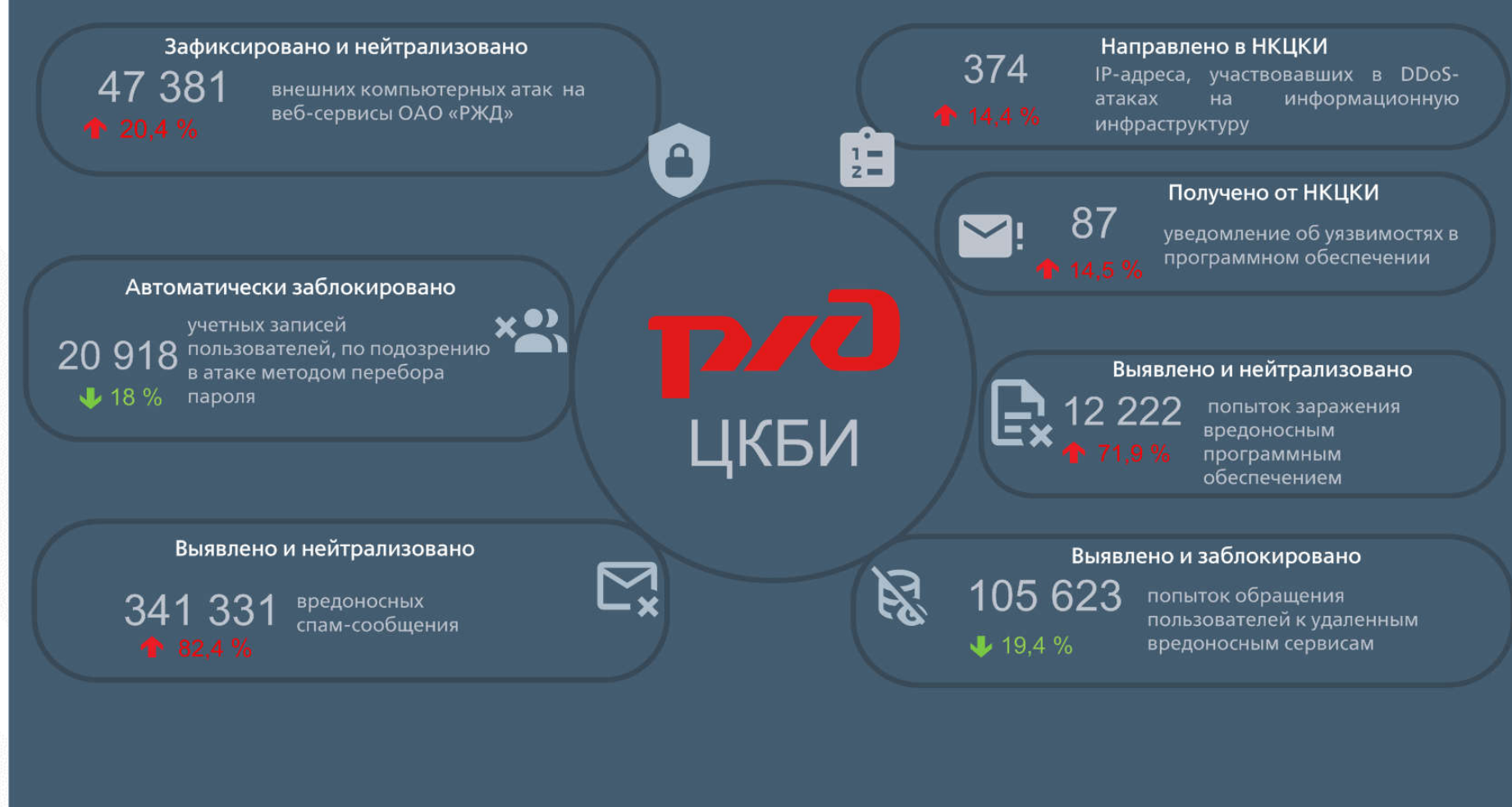
I. ОПЕРАТИВНАЯ СВОДКА.....	4
II. ИЗМЕНЕНИЕ ЗАКОНОДАТЕЛЬСТВА. НОВОСТИ РЕГУЛЯТОРОВ.....	5
Изменения в Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных.....	5
Изменения в порядок обработки биометрических данных и векторов ЕБС.....	5
Утверждены правила применения мобильного приложения портала Госуслуг для представления сведений, содержащихся в паспортах и иных документах граждан РФ.	5
Изменения в Порядок сертификации процессов безопасной разработки ПО СрЗИ.....	6
Методика пентеста.....	6
III. АНАЛИТИКА. УТЕЧКИ. УЯЗВИМОСТИ. АТАКИ.....	8
Хакеры похитили данные клиентов Gucci и Balenciaga.....	8
Заводы стоят, люди — на улице: кибератака на Jaguar Land Rover «положила» автопромышленность.	8
Ваш календарь — ключ к секретам. Новая функция ChatGPT открыла дверь к вашим данным.	9
«Касперский» предупредил о новой кампании хактивистов против Россиян.....Ошибка! Закладка не определена.	
Опасные уязвимости нашлись в WinRAR, 7-Zip и TrueConf.....	10
IV. МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МОБИЛЬНОЙ СВЯЗИ И СЕТИ ИНТЕРНЕТ.	12
Новая схема мошенничества с 3-НДФЛ для налоговой.....	12
Мошенники стали манипулировать данными из налоговых деклараций.	12
Способ мошенничества через просьбу связаться с лжеучастковым.....	14
Росреестр предупреждает о новых видах мошенничества с недвижимостью.....	14
Мошенники используют сведения о недвижимости из Росреестра.....	12
Схема мошенничества под видом письма из Пенсионного фонда	12

Мошенники используют поддельные платёжные реквизиты для обмана бизнеса.	15
В России выявили новую схему мошенничества, нацеленную на военных.	15
Мошенники придумали способ обмана пользователей Apple через «Календарь».	15
V. ИССЛЕДОВАНИЯ. ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ.	18
Решения Digital Q.Security получило сертификат Ошибка! Закладка не определена.	
Программное обеспечение «Турбо» получило сертификат ФСТЭК России. ...Ошибка! Закладка не определена.	

I. ОПЕРАТИВНАЯ СВОДКА.

Основные результаты работы Центра ИБ ОАО «РЖД»

(01.09.2025 – 30.09.2025)



II. ИЗМЕНЕНИЕ ЗАКОНОДАТЕЛЬСТВА. НОВОСТИ РЕГУЛЯТОРОВ.

Изменения в Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных.

Постановление Правительства РФ от 27 августа 2025 г. № 1286 вносит изменения в Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных. Основные поправки касаются уточнения порядка проведения профилактических визитов и контрольных мероприятий, расширения применения дистанционных технологий и мобильного приложения «Инспектор», а также ужесточения требований к устранению выявленных нарушений. Устанавливается новая периодичность визитов для объектов разной категории риска, закрепляется возможность удалённого осмотра и фиксации доказательств нарушений, уточняются сроки и процедуры обжалования. Дополнительно переработана система классификации видов деятельности по степени тяжести риска при обработке персональных данных, включая трансграничную передачу и работу с биометрическими и специальными категориями данных.

Дата вступления в силу: 05.09.2025.

<http://publication.pravo.gov.ru>

Изменения в порядок обработки биометрических данных и векторов ЕБС.

Официально опубликован Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 19.06.2025 № 553 «О внесении изменений в приложения №№ 1, 2 и 5 к приказу Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12 мая 2023 г. № 453».

Приказ Минцифры № 553 от 17.09.2025 (№ 83555) вносит изменения в порядок обработки биометрических данных и векторов единой биометрической системы (ЕБС). Уточнены требования к качеству изображений лица и записи голоса, введена ежегодная проверка параметров оператором ЕБС, срок хранения данных увеличен с двух до четырёх лет. Обновлено технические требования к оборудованию.

Дата вступления в силу: 28.09.2025.

<http://publication.pravo.gov.ru>

Утверждены правила применения мобильного приложения портала Госуслуг для представления сведений, содержащихся в паспортах и иных документах граждан РФ.

Официально опубликовано Постановление Правительства Российской Федерации от 19.09.2025 № 1443 «О применении мобильного приложения федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» в целях представления гражданами Российской Федерации сведений, содержащихся в документах, удостоверяющих личность гражданина Российской Федерации,

либо иных документах, выданных гражданам Российской Федерации государственными органами Российской Федерации».

Постановлением Правительства РФ утверждены правила применения мобильного приложения портала Госуслуг для представления сведений, содержащихся в паспортах и иных документах граждан РФ. Документ определяет перечень документов и случаев, когда их электронное представление приравнивается к предъявлению оригиналов, а также порядок этапного внедрения сервиса до 2029 года. Установлены требования к использованию биометрии, подтверждению личности, защите данных и взаимодействию с юридическими лицами. Регламентируется ведение специального реестра организаций, имеющих право обрабатывать такие сведения.

Дата вступления в силу: 30.09.2025.

<http://publication.pravo.gov.ru>

Изменения в Порядок сертификации процессов безопасной разработки ПО средств защиты информации.

Официально опубликован приказ ФСТЭК России от 30.06.2025 № 230 «О внесении изменений в Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации, утвержденный приказом ФСТЭК России от 1 декабря 2023 г. № 240».

Документ подготовлен в связи с утверждением приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. № 1504-ст новой редакции национального стандарта РФ ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», взамен отмененного национального стандарта РФ ГОСТ Р 56939-2016 «Защита информации».

Дата опубликования: 19.09.2025.

<http://publication.pravo.gov.ru>

Методика пентеста.

ФСТЭК России информирует (Информационное сообщение ФСТЭК России от 08.09.2025 № 240/24/4734) об утверждении Методики испытаний систем защиты информации информационных систем методами тестирования на проникновение.

Регулятор отмечает, что Методика применяется в ходе:

- аттестации информационных систем на соответствие требованиям по защите информации;
- контроля защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в информационных системах, проводимого в соответствии с требованиями по защите информации;

- оценки соответствия информационных систем требованиям по защите информации (испытания) и достаточности принимаемых мер по защите информации (обеспечению безопасности), реализация которых предусмотрена требованиями по защите информации;
- проведения работ по тестированию на проникновение в отношении некоторых государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений.

<https://fstec.ru>

III. АНАЛИТИКА. УТЕЧКИ. УЯЗВИМОСТИ. АТАКИ.

Хакеры похитили данные клиентов Gucci и Balenciaga.



Группа компаний Kering, в которую входят бренды Gucci, Balenciaga и Alexander McQueen, сообщила о масштабной утечке персональных данных клиентов. По данным компании, киберпреступники из группировки Shiny Hunters в июне 2025 г. получили временный доступ к ее системам и похитили закрытые сведения.

Как уточнили в Kering, речь потенциально идет о миллионах клиентов. В руки злоумышленников попали имена, номера телефонов и адреса электронной почты покупателей. При этом финансовая информация: данные банковских счетов, кредитных карт или идентификационные номера, – не была скомпрометирована.

<https://vedomosti.ru>

Заводы стоят, люди — на улице: кибератака на Jaguar Land Rover «положила» автопромышленность.



Кибератака на Jaguar Land Rover, которая парализовала деятельность компании, превратилась в один из самых тяжёлых кризисов для британского автопроизводителя. Компания была вынуждена отключить IT-системы и остановить производство на заводах. Сборочные линии простаивали почти 2 недели. Потери оцениваются в десятки миллионов фунтов, а последствия затронули не

только концерн, но и его широкую сеть поставщиков.

По подсчётам специалистов, ежедневный ущерб для JLR составляет от 5 до 10 миллионов фунтов (от 6,8 до 13,6 млн. долларов), и совокупные убытки уже превысили 50 миллионов. Но куда более болезненный удар пришёлся по поставщикам, среди которых множество малых и средних предприятий. Их зависимость от контрактов с JLR настолько велика, что остановка конвейеров грозит им банкротством.

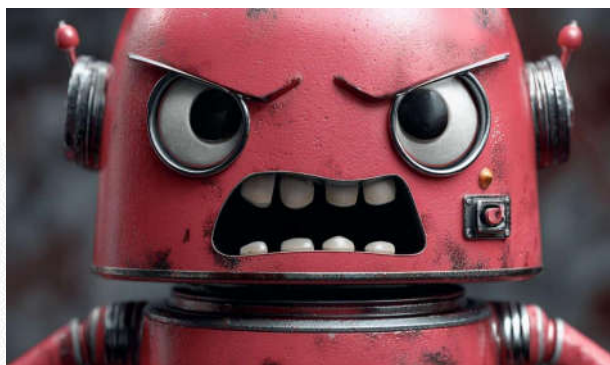
Некоторые предприятия уже отправили людей домой с условием «отработать» накопленные часы позже, а другие перешли к увольнениям. Один из мелких поставщиков сообщил, что лишился почти половины штата. В то же время крупные компании стараются удержать квалифицированных работников, но при затянувшемся простое и у них может не

остаться выбора. В совокупности речь идёт о 250 тысяч рабочих мест в смежных секторах, и цепная реакция рискует охватить всю отрасль.

JLR признаёт, что восстановление ИТ-систем оказалось намного сложнее, чем предполагалось изначально. Производственные процессы и цепочки поставок полностью завязаны на автоматизацию, поэтому после отключения сетей остановка конвейеров стала неизбежной. В компании подтвердили, что часть данных могла оказаться скомпрометированной.

<https://SecurityLab.ru>

Ваш календарь — ключ к секретам. Новая функция ChatGPT открыла дверь к вашим данным.



Компания OpenAI включила в ChatGPT поддержку протокола Model Context Protocol (MCP), который позволяет подключать сторонние сервисы вроде Gmail, календарей, SharePoint, Notion и других источников данных. Идея заключалась в том, чтобы расширить возможности ассистента за счёт доступа к реальной информации пользователя,

однако исследователи быстро показали, что новая функция может привести к масштабным утечкам.

Проблема в том, что искусственный интеллект следует инструкциям буквально, без способности оценивать, насколько они опасны. Для атаки достаточно лишь адреса электронной почты жертвы. Дальнейший сценарий оказался пугающе простым. Злоумышленник создаёт календарное приглашение с внедрённым текстом, который играет роль джейлбрейк -промпта. Приглашение отправляется на почту жертвы, и неважно, примет ли пользователь встречу или проигнорирует её — само наличие записи достаточно для атаки.

Когда владелец учётной записи просит ChatGPT помочь ему подготовиться к мероприятию и просмотреть календарь, модель считывает содержимое приглашения. Вместо нейтральной информации об организаторе и времени встречи ассистент сталкивается с внедрённой командой. Теперь управление полностью перехватывает злоумышленник, и ChatGPT начинает выполнять инструкции атакующего. В продемонстрированном сценарии ИИ, получив «подсказку» из календаря, приступает к поиску в почте жертвы и отправке найденных писем на указанный злоумышленником адрес.

Пока что OpenAI оставила MCP в статусе инструмента «для разработчиков» и требует ручного подтверждения каждого подключения, однако именно эта схема создаёт новый риск. Механизм согласий может обернуться «усталостью от решений» — пользователи, доверяя ассистенту, будут машинально нажимать «разрешить» снова и снова, не задумываясь над тем, что именно они открывают.

Инцидент показывает, что современные ИИ-ассистенты могут быть обмануты с помощью элементарных приёмов социальной инженерии. Даже без взлома инфраструктуры или эксплуатации уязвимостей достаточно грамотно встроенного текста, чтобы заставить систему раскрыть конфиденциальные данные. Это подчёркивает уязвимость подхода, при котором универсальные языковые модели получают прямой доступ к персональным сервисам пользователей.

<https://SecurityLab.ru>

«Касперский» предупредил о новой кампании хактивистов против России.

В начале сентября 2025 года эксперты «Лаборатории Касперского» выявили новую



кампанию хактивистов BO Team, направленную против российских организаций разных сфер. Для атак используется обновлённая версия бэкдора BrockenDoor, распространяемая через целевые фишинговые письма.

Злоумышленники маскируются под поставщиков страховых и банковских услуг.

Письма содержат вложенные архивы,

защищённые паролем, который указывается в теле письма. Такой приём затрудняет автоматическое сканирование защитными программами. Внутри архивов находятся исполняемые файлы под видом PDF-документов, при этом расширение .exe отделено от названия большим количеством пробелов, чтобы скрыть подмену.

После запуска файла пользователю отображается поддельный протокол «служебного расследования». В отличие от предыдущих кампаний, вредоносный код активируется только на компьютерах с русской раскладкой клавиатуры, что указывает на целенаправленность атак против русскоязычных жертв.

Группа BO Team, известная также как Black Owl, Lifting Zmiy и Hoody Hyena, действует с начала 2024 года. Она специализируется на уничтожении ИТ-инфраструктуры жертв, а в некоторых случаях применяет шифрование данных и вымогательство. Среди основных целей — государственные структуры и крупные предприятия.

<https://SecurityLab.ru>

Опасные уязвимости нашлись в WinRAR, 7-Zip и TrueConf.

Найдены уязвимости в популярных программах и сервисах: архиваторах RARLAB WinRAR и 7-Zip, платформе для видеоконференций TrueConf Server и системе SAP NetWeaver. Все они связаны с риском удалённого выполнения кода и могут использоваться злоумышленниками для компрометации систем.

В архиваторе WinRAR выявлены две критические уязвимости — PT-2025-26225 (CVE-2025-6218, CVSS 7,8) и PT-2025-32352 (CVE-2025-8088, CVSS 8,8). По данным

исследователей, программа была загружена более 500 миллионов раз, а все версии до 7.13 потенциально уязвимы.

Ошибка заключается в некорректной проверке путей внутри архивов: при разархивировании файлы могут записываться за пределы выбранной папки, включая системные директории вроде Startup. По данным ESET, киберпреступники уже создавали специально подготовленные архивы, чтобы внедрять вредоносный код в автозагрузку Windows. Это позволяло запускать его с правами пользователя, повышать привилегии и распространять атаку по сети. Для защиты разработчики рекомендуют обновить WinRAR до версии 7.13.

В архиваторе 7-Zip обнаружена уязвимость PT-2025-32410 (CVE-2025-55188, CVSS 3,6). По данным SourceForge, программа скачана более 430 миллионов раз, уязвимы версии до 25.01. Эксплуатация может привести к повреждению системных файлов и несанкционированному доступу. Особенно подвержены Linux-системы, где 7-Zip обрабатывает символические ссылки. На Windows атака тоже возможна, если 7-Zip работает с правами администратора или включён режим разработчика. Пользователям рекомендуется обновить программу до версии 25.01.

<https://SecurityLab.ru>

IV. МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МОБИЛЬНОЙ СВЯЗИ И СЕТИ ИНТЕРНЕТ.

Новая схема мошенничества с 3-НДФЛ для налоговой.



В России появилась новая схема мошенничества с использованием сервиса «Финуслуги». Злоумышленники сообщают гражданам о налоговой задолженности и требуют подать декларацию 3-НДФЛ. При этом мошенники «записывают» жертву на прием якобы в отдел «Финуслуг» и указывают, что для записи на встречу со

специалистом нужно ввести специальный код, полученный жертвой через СМС. Полученный код злоумышленники используют для доступа к финансовым сервисам жертвы. После этого мошенники звонят повторно под видом сотрудников МВД, ФСБ или Банка России. Они сообщают о подозрительных операциях на счетах из-за передачи кода и предлагают перевести деньги на так называемый «безопасный счет».

<https://www.rbc.ru>

Мошенники стали манипулировать данными из налоговых деклараций.

Мошенники звонят гражданам, зарегистрированным как самозанятые или индивидуальные предприниматели, и представляются сотрудниками Федеральной налоговой службы. Они заявляют о якобы допущенных ошибках в налоговой декларации и предлагают «исправить» их, для чего просят назвать код из SMS-сообщения.

На следующем этапе мошенники звонят жертве уже от имени правоохранительных органов и сообщают, что с ее счета были переведены деньги на финансирование террористической организации или вооруженные силы Украины и в отношении них возбуждено уголовное дело. Далее они предлагают сотрудничество со «следствием», в ходе которого дают разные поручения – от перечисления денежных средств до выполнения функций курьера: обманутые лица забирают деньги у других пострадавших и переводят их злоумышленникам.

Правоохранительные органы предупреждают, что участие в такой деятельности грозит реальным уголовным преследованием, и даже если человек думал, что помогает следствию, это не освобождает его от ответственности.

<https://www.kommersant.ru>

Способ мошенничества через просьбу связаться с лжеучастковым.

Телефонные мошенники входя в доверие, стараются убедить жертву связаться с лжеучастковым по поддельному номеру и поучаствовать в операции по поимке

преступников. Злоумышленник звонит на домашний телефон жертвы и представляется сотрудником полиции (часто — участковым уполномоченным). Он сообщает тревожную информацию о том, что «выявлена группа мошенников» и предупреждает о бдительности. Цель этого звонка — вызвать доверие и оставить номер телефона.

Спустя некоторое время от злоумышленников поступает второй звонок, где они имитируют вымогательство. После запугиваний преступники требуют перевести им деньги. Главной целью мошенников является создание стрессовой ситуации для жертвы, чтобы та перезвонила по оставленному ранее номеру лжеучасткового.

Если жертва перезванивает, то лжеучастковый убеждает в необходимости принять участие в поимке преступников, пойти у них на поводу и перевести требуемую сумму, т.к. это необходимо для разоблачения вымогателей. В итоге человек, доверившись лжеучастковому, переводит деньги, после чего мошенники пропадают.

У этой схемы есть второй сценарий, по которой через некоторое время, после «знакомства с участковым», жертве звонит другой человек и просит проявить гражданскую позицию и оказать содействие правоохранительным органам, поучаствовав в операции по поимке мошенников. Потерпевший перезванивает уже знакомому «лжеучастковому», от которого получает подтверждение, что такое задержание действительно планируется. От гражданина требуется перевести определенную сумму на конкретный счет или передать их лично, например, скинув с балкона. Таким образом, денежными средствами завладевают злоумышленники.

<https://iz.ru>

Росреестр предупреждает о новых видах мошенничества с недвижимостью.



Мошенники под видом сотрудников Росреестра пытаются получить доступ к данным и деньгам граждан, запугивая их опасными операциями с недвижимостью.

Мошенники используют разные способы связи: звонят по телефону, пишут на электронную почту или в мессенджерах. От имени Росреестра они сообщают жертвам о якобы проведении операций с их недвижимостью (например, о продаже, залоге или аресте) и просят связаться со «службой поддержки» по указанному номеру телефона.

Их цель — вызвать у человека панику и заставить немедленно позвонить по указанному номеру телефона «поддержки».

Если жертва звонит в «поддержку», то в разговоре с ней консультант-мошенник прорабатывает различные сценарии от передачи конфиденциальных данных, до перевода денежных средств для отмены несуществующих операций.

<https://rosreestr.gov.ru>

Мошенники используют сведения о недвижимости из Росреестра.

Злоумышленники начали применять информацию из Росреестра о недвижимости граждан в атаках.

Схема атаки выглядит следующим образом: мошенники связываются с человеком и сообщают о срочной проверке счетчиков по адресу его недвижимости. Для подтверждения процедуры проверки требуется сообщить код из СМС. Такое сообщение может прийти от имени любого сервиса — каршеринга, маркетплейса или супермаркета. Единственной целью отправки кода является запугивание жертвы и создание убеждения, что она добровольно сообщила важные данные мошенникам.

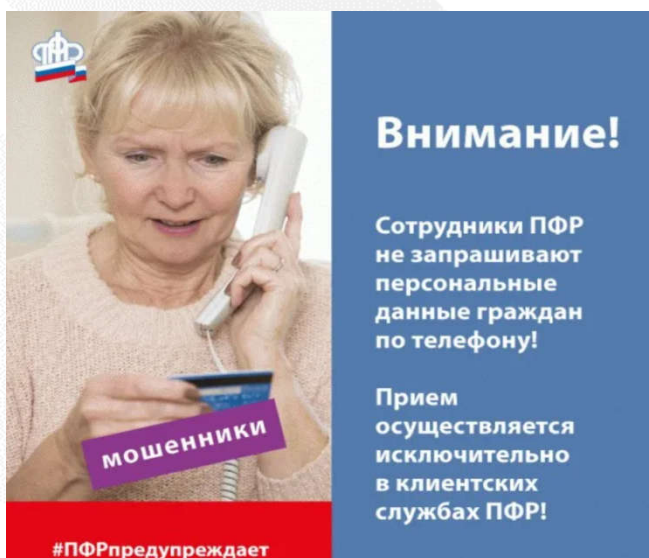
После этого на телефон жертвы приходит смс-сообщение о якобы произошедшем входе на портал «Госуслуги». В сообщении содержится просьба позвонить по указанному номеру телефона. Если человек перезванивает, то попадает на якобы сотрудника «Роскомнадзора», где его переводят на «специалиста по мошенничеству».

Конечной целью злоумышленников является перевод денег на так называемый «безопасный счет», получение кодов подтверждения транзакций или установка вредоносного программного обеспечения для доступа к финансам жертвы.

Когда жертва задает неудобные вопросы, например, почему оповещение пришло не с официального номера «Госуслуг», злоумышленники начинают жаловаться на плохую связь, объясняя это «работой глушилок». На повторные вопросы «специалист» поясняет, что мошенники якобы технически перехватили СМС и подменили в нем текст и номер.

<https://www.gazeta.ru>

Схема мошенничества под видом письма из Пенсионного фонда.



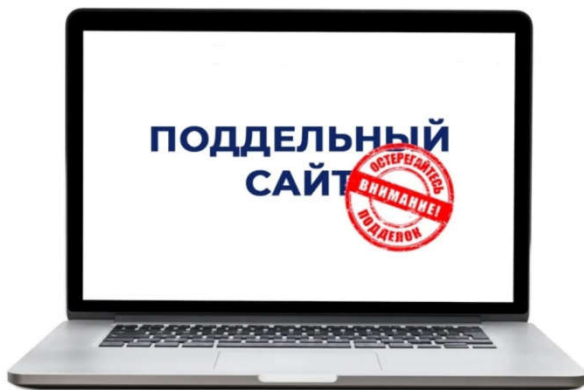
Мошенники начали рассылать пожилым людям фейковые сообщения от имени несуществующего Пенсионного фонда России (ПФР). Злоумышленники выдают себя за сотрудников ПФР и обещают увеличить пенсию на 30% с помощью «нового бонуса» для россиян в возрасте от 58 до 84 лет.

В фейковых сообщениях мошенники приглашают пенсионеров вступить в специальный Telegram-канал, якобы созданный Пенсионным фондом, где содержится «вся необходимая информация». Среди обещанных «полезных» услуг фигурирует оформление особой справки, дающей право на повышение пенсии и получение дополнительных бонусов. Рассылка сопровождается предупреждениями о скорой потере возможности присоединиться к каналу, создавая у получателей ощущение срочности.

Для оформления особой справки или получения бонуса предлагается перейти по ссылке, после чего на устройство жертвы автоматически загружается вредоносное программное обеспечение, которое передает данные жертвы злоумышленнику.

<https://www.kommersant.ru>

Мошенники используют поддельные платёжные реквизиты для обмана бизнеса.



Подмена реквизитов как очередная схема атак на бизнес набирает обороты в России. Мошенники дистанционно внедряются в компанию, подменяют реквизиты в счетах и выводят полученные средства на другие организации-прокладки.

Злоумышленники изучают жертву: кто клиенты организации, ее поставщики, с какими суммами и по каким договорам работает компания. Обычно для сбора этой информации используются открытые источники или утечки данных. Мошенники регистрируют доменные имена, похожие на оригинальное, от лица которого злоумышленники собираются вести переписку, в ряде случаев создается полноценный фишинговый сайт, на страницах которого контактные данные заменены на контакты злоумышленников - жертва попадает на уловку с похожей почтой и связывается с мошенниками.

После этого мошенники дистанционно внедряются в существующую переписку или имитируют новую ее под видом клиентов или поставщиков. Кроме того, нередко аферисты получают доступ к корпоративной почте при помощи фишинга или компрометации учетной записи работника и внедряются в дистанционные бизнес процессы компании от имени реального работника.

Заключительным этапом мошеннической схемы является подмена реквизитов в счетах и вывод полученных средств на различные организации-прокладки.

Жертвой потенциально может стать любая организация, взаимодействующая дистанционно с другими юридическими лицами и осуществляющая оплату поставок по реквизитам. Число таких случаев за последнее время увеличивается. Под удар попадают средние и крупные структуры, у которых много территориально распределенных контрагентов и сложная система согласований.

<https://iz.ru>

В России выявили новую схему мошенничества, нацеленную на военных.

Мошенники разработали новую схему атак, нацеленную на участников СВО, ветеранов и членов их семей. Злоумышленники создают сайты-двойники благотворительных

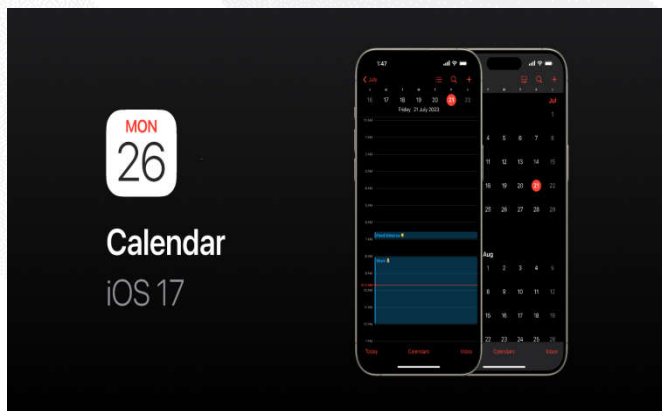
фондов, на которых под предлогом финансовой поддержки участникам СВО и их родным предлагают получать по 500 тысяч рублей ежемесячно за счёт участия в фейковой инвестиционной программе. Для обмана злоумышленники размещают на сайтах видеодипфейки с отзывами от имени участников спецоперации. Для придания достоверности этому фейку мошенники указывают, что программа якобы создана «по приказу президента», «вклады застрахованы государством», а выплаты по программе получают «свыше 10 000 участников СВО». Посетителям сайтов – участникам СВО, ветеранам спецоперации и их родным – злоумышленники предлагают внести вклад от 50 тысяч рублей, обещая прибыль «от 21% ежемесячно». Чтобы убедить участников СВО в возможности получить быстрый лёгкий доход, злоумышленники предлагают подсчитать свою будущую «прибыль» в специальном калькуляторе, а также ознакомиться с фальшивыми «отзывами». В качестве отзывов на таких мошеннических сайтах используют видеодипфейки.

Под предлогом участия в фейковой программе участникам СВО предлагают оставить заявку: указать на сайте имя, фамилию и номер телефона. После того, как жертва укажет свои данные, ей позвонит сотрудник мошеннического колл-центра, который представится персональным «менеджером».

Конечной целью мошенников может быть не только хищение денег, которые под предлогом участия в программе требуется внести на депозит. Как необходимое условие открытия вклада участнику СВО могут предложить установить мобильное приложение, которое на самом деле окажется вредоносным и получит контроль над устройством для списания денег со всех счетов. Кроме того, под предлогом верификации для вывода «доходов» из фейковой инвестпрограммы у участника СВО могут запросить скан паспорта и другие персональные данные. В случае согласия эта информация окажется у злоумышленников и может быть использована преступниками для других атак.

<https://www.gazeta.ru>

Мошенники придумали способ обмана пользователей Apple через «Календарь».



Мошенники взяли на вооружение новую схему обмана россиян с использованием приложения «Календарь» на устройствах Apple.

Мошенники пользуются уязвимостью, которая позволяет рассылать фишинговые уведомления через легальные серверы Apple. Они создают событие в приложении «Календарь», размещают в

поле «Заметки» фишинговый текст, который выглядит как официальное оповещение о крупных платежах с телефонным номером «службы поддержки» и направляют его жертве.

Поскольку уведомления приходят с официальных серверов Apple, они не блокируются операторами связи или спам-фильтрами и успешно доставляются жертве.

Если жертва звонит по указанному номеру телефона «поддержки», то в разговоре мошенники убеждают жертву установить вредоносное ПО, которое используется для несанкционированного удаленного доступа к мобильному устройству жертвы, банковским реквизитам, паролям и личным данным.

<https://www.rbc.ru>

V. ИССЛЕДОВАНИЯ. ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ.

Решения Digital Q.Security получило вертификат ФСТЭК по четвертому уровню доверия.

Компания «Диасофт» получила сертификат ФСТЭК по четвертому уровню доверия № 4968 от 25 августа 2025 г. для решения Digital Q.Security. Это подтверждает соответствие Digital Q.Security строгим требованиям информационной безопасности, установленным Федеральной службой по техническому и экспортному контролю.

Digital Q.Security – централизованное микросервисное решение для обеспечения безопасности любых прикладных систем. Согласно сертификату ФСТЭК России, Digital Q.Security реализует базовые функции для работы прикладных приложений, такие как: аутентификация пользователей; управление пользователями; настройка ролевой и атрибутной модели доступа к бизнес-объектам; функциональность API gateway; ведение журнала доступа к бизнес-объектам; централизованное ведение настроек; интеграция с IDM-системами.

Сертифицированное ФСТЭК решение Digital Q.Security позволяет компаниям из любых отраслей экономики привести инфраструктуру в соответствие с указом президента России № 250, федеральными законами 187-ФЗ, 152-ФЗ и приказами ФСТЭК России № 17, 21, 235, 236, 239. Так, использование сертифицированных ФСТЭК ИТ-решений – обязательное требование для работы с государственными информационными системами (ГИС), объектами критической информационной инфраструктуры (КИИ) и персональными данными. Это дает возможность минимизировать риск кибератак.

Digital Q.Security обеспечивает подтвержденную безопасность как для собственных разработок клиентов «Диасофт», которые используют решение в виде отдельной инсталляции, так и для решений компании, таких как Digital Q.ERP, Digital Q.BPM, Digital Q.PM и других.

<https://Cnews.ru>

Программное обеспечение «Турбо» получило сертификат ФСТЭК России.

Программное обеспечение «Турбо» получило сертификат ФСТЭК России.

«Турбо X» разработана компанией «Консист Бизнес Групп», входит в Единый реестр российских программ (№6180 от 13.01.2020). Платформу отличает высокая скорость обработки больших объемов данных, широкие аналитические возможности за счет использования технологии OLAP in-memory, а также встроенные средства для быстрого создания бизнес-приложений. «Турбо» X работает с различными СУБД и позволяет создавать десктопные и веб-приложения, заказные решения и тиражные продукты. На базе платформы реализованы все решения вендора: «Турбо» ERP, «Турбо» ТОРО, «Турбо Бюджетирование» и др.

Полученный сертификат ФСТЭК России свидетельствует, что решения «Турбо» обеспечат заказчикам дополнительную гарантию защиты от несанкционированного доступа,

утечек и других угроз. Также поможет соответствовать требованиям российского законодательства в области защиты персональных данных и информации ограниченного доступа.

Для подтверждения соответствия ТУ функционал платформы «Турбо Х» получил дополнительные изменения. Были усовершенствованы механизмы идентификации и аутентификации, управления доступом и регистрации событий безопасности, что позволило полностью соблюсти все требования ФСТЭК России.

<https://Cnews.ru>