СОБЫТИЯ

Центробанк и МВД будут обмениваться данными о мошенничестве

21 октября вступили в силу положения Федерального закона от 20 октября 2022 года № 408-ФЗ «О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе»», которые обеспечивают информационное взаимодействие между МВД России и Банком России.

Банк России будет автоматически обмениваться с МВД данными о попытках переводов денег клиентов без их согласия. Это необходимо для повышения скорости расследования дел по фактам мошенничества при денежных переводах.

Согласно справке Государственно-правового управления, в соответствии с Федеральным законом Банк России имеет право предоставлять МВД России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента. Порядок информационного обмена, форма и перечень предоставляемых сторонами сведений будут определены в соглашении, заключаемом между Банком России и МВД России.

Ранее при рассмотрении таких дел значительное время уходило на запросы данных и переписку между правоохранительными органами и банками. При этом сроки возбуждения уголовных дел определены уголовно-процессуальным законодательством и требуют незамедлительного принятия решений, а сроки рассмотрения кредитными организациями обращений правоохранительных органов по фактам дистанционных хищений (до 30 дней) делали невозможным проведение срочных оперативно-разыскных и процессуальных мероприятий. В результате принятие окончательных решений по материалам и по возбужденным уголовным делам этой категории затягивалось до трех-четырех месяцев, из-за чего существенно снижался уровень их раскрываемости.

Вступивший в силу закон предусматривает подключение МВД к автоматизированной системе ФинЦЕРТ Банка России, в которой содержится информация об операциях, проведенных без согласия клиентов. «Благодаря этому правоохранительные органы смогут практически в онлайн-режиме получать сведения о мошеннических операциях, в том числе о получателях похищенных денег. Обмен данными будет происходить с соблюдением всех норм банковской тайны», – отметили в Банке России. МВД России будет передавать в базу ФинЦЕРТ сведения о совершенных противоправных действиях, что позволит банкам учитывать эти данные в своих бизнес-процессах для предотвращения мошеннических переводов.

Сами не платим и другим не дадим

США вместе с группой из 48 стран, Европейским союзом и Интерполом в рамках международной инициативы противодействия программам-вымогателям (*International Counter Ransomware Initiative*, CRI) заявили об отказе от уплаты выкупов в случае кибератак. Главной целью инициативы является прекращение финансирования вымогателей.

Кроме того, группа обсудила новые подходы к борьбе с киберпреступностью, включая использование искусственного интеллекта и анализа блокчейн-данных, а также создание специализированной платформы для обмена информацией между странами-участниками.

Также был достигнут прогресс в разработке совместной политики, которая включает в себя обмен списками заблокированных криптовалютных кошельков, связанных с атаками программ-вымогателей. Несмотря на сложности в координации международных усилий и противоречивые мнения о запрете на выплаты выкупов, участники согласились считать такие выплаты недопустимыми.

Более того, участники инициативы намерены искать способы привлечения других стран к ответственности за их роль в игнорировании принятых правил или содействии вымогателям.

ПЛАНЫ

СМИ и операторы связи перейдут на российские СЗИ

С 2025 года российские СМИ и операторы связи должны будут соответствовать новым требованиям по информационной безопасности, разработанным Минцифры. Об этом сообщают «Ведомости» со ссылкой на источники в отрасли.

По данным издания, требование будет касаться всех телеканалов первого и второго мультиплексов, «Российской газеты», ИТАР-ТАСС и МИА «Россия сегодня», операторов мобильной связи и спутникового ТВ.

Перечисленные организации должны создать внутренние структурные ИБ-подразделения, а также использовать только отечественные СЗИ. Эксперты полагают, что выполнение новых требований будет сопряжено с рядом сложностей, как финансового, так и технического характера.

Для создания отделов по ИБ потребуются дополнительные инвестиции от компаний. По оценке экспертов, на финансирование новых структур, в зависимости от размера бизнеса, потребуется от 5 до 50 млн руб. в год. Кроме того, формирование ИБ-структур и обучение сотрудников потребует от 2 до 5 лет. Замена СЗИ тоже потребует дополнительных расходов.

«Проблемы в переходе на отечественные решения связаны с тем, что невозможно обеспечить бесшовный переезд с одного решения на другое, а также с отсутствием некоторых классов специализированной аппаратуры, необходимой для обработки больших потоков данных, характерных для сетей связи», – уточнил собеседник «Ведомостей».

С другой стороны, как отметил еще один собеседник «Ведомостей» в одном из спутниковых операторов, компании-вещатели ежегодно перечисляют иностранным ИБ-вендорам порядка 50 млн долл., поэтому переход на доверенные отечественные СЗИ поз-

волит снизить такие затраты, заметно возросшие после падения курса рубля.

Порядок согласия на обработку персональных данных может измениться

В Совете Федерации обсуждается вопрос изменения порядка обработки персональных данных. Речь идет о разделении пользовательского соглашения и согласия на обработку данных.

Сейчас гражданин, единожды посетив сайт, уведомляется его владельцем о том, что он принимает условия пользовательского соглашения, в которое автоматически заложено согласие на обработку персональных данных. Авторы инициативы считают, что необходимо рассматривать пользовательское соглашение как «соглашение между субъектами персональных данных и оператором по определению прав и обязанностей, связанных с использованием информационных ресурсов», не включающее в себя согласия на обработку персональных данных.

Кроме того, предлагается на нормативном уровне закрепить положение, согласно которому обработка персональных данных всегда должна соответствовать предмету договора, а в противном случае считать сбор данных незаконным. Также любая информация, касающаяся обработки данных, должна быть изложена ясным и понятным языком, в том числе содержать возможность ознакомления на языке национального меньшинства.

ОЦЕНКИ И ПРОГНОЗЫ

Более половины компаний принимают решения с учетом ИБ-рисков

Из результатов исследования риск-менеджмента информационной безопасности в организациях, проведенного группой компаний «Солар, следует, что более половины (52 %) российских компаний принимают ключевые решения с учетом ИБ-рисков.

В исследовании приняли участие 157 представителей российских компаний из Москвы, Санкт-Петербурга и ряда других городов РФ с населением более 500 тыс. человек, 47 % которых представляют сегмент среднего бизнеса (с выручкой от 800 млн до 5 млрд руб. в год), 26 % – крупного (с выручкой от 5 до 60 млрд руб. в год), 15 % – госсектор и 12 % – сегмент Enterprise (с выручкой от 60 млрд руб. в год). Среднее количество сотрудников в компаниях-респондентах составило 2570 человек.

Согласно исследованию, 60 % компаний сегмента среднего бизнеса большую часть ключевых решений принимают с учетом рисков безопасности. Среди крупных компаний эта доля составляет 46 %, а в госсекторе и Enterprise – по 41 %. При этом в госсегменте компаний, принимающих ключевые решения без учета рисков, больше, чем в других отраслях – 32 %. Для сравнения, в сегментах Enterprise и в среднем бизнесе таких организаций почти в два раза меньше (18 %), а в крупном бизнесе – 17 %.

Лишь в 12 % опрошенных компаний риск-менеджмент находится на стадии формирования, в других он реализован в той или иной степени. По уровню зрелости в вопросах оценки и анализа рисков лидирует Enterprise: в 18 % компаний этого сегмента наиболее развитые и продвинутые системы риск-менеджмента, а почти в половине случаев он существенно влияет на работу организации. На втором месте здесь располагается крупный бизнес (7 %), на третьем – госсектор (5 %), на последнем – средний бизнес (3 %).

Примерно в половине организаций анализ рисков происходит не реже одного раза в год, и лишь у 17 % опрошенных он происходит ситуативно: в случае крупных изменений, после наступления инцидентов и т. д. Средний период между пересмотром моделей рисков и угроз составляет полтора года.

По итогам внедрения процедуры анализа рисков 40 % компаний отмечают сокращение количества инцидентов в ИБ, 33 % – сокращение потерь от инцидентов, 28 % – снижение расходов на ликвидацию их последствий.

НОВОСТИ КОМПАНИЙ

Аладдин выпустил новую версию Secret Disk для Linux 2.0

Secret Disk для Linux – один из флагманских продуктов компании Аладдин – обеспечивает предотвращение утечек конфиденциальной информации с помощью шифрования на рабочих станциях и серверах с отечественными ОС семейства Linux.

Ключевое изменение состоит в возможности развертывания и централизованного управления на большом количестве рабочих станций, что потребовало существенной переработки продукта. Теперь Secret Disk для Linux имеет клиент-серверную архитектуру и включает следующие компоненты: менеджмент-сервер, консоль управления администратора и агент. Все компоненты исполнены в рамках подхода Secure by Design, параметры безопасности системы хранятся в базе данных в защищенном виде. Помимо этого, в продукт встроен сертифицированный модуль СКЗИ Secret Disk Crypto Engine.

На текущий момент реальная практика такова, что переход на Linux зачастую осложняется из-за неготовности ИТ-инфраструктуры организаций к этому шагу. При этом требования к защите данных необходимо соблюдать столь же строго, как и в Windows. Secret Disk для Linux 2.0 позволяет построить систему защиты в Linux-инфраструктуре любой степени зрелости. Бизнес-логика продукта не требует обязательного наличия таких сервисов, как PKI, УЦ и служба каталогов. Продукт совместим с классическими инструментами доставки и развертывания ПО на Linux. Все это позволит клиентам переходить на Linux уже сейчас, не дожидаясь, когда ИТ-инфраструктура этой ОС будет идентична Windows.

Администраторы безопасности получили возможность динамической группировки пользователей и централизованного управления политиками шифрования на большом количестве рабочих станций. В обновленной графической консоли управления, построенной на рекомендуемых для разработки ПО web-технологиях, администратор всегда видит статус пользователей и их ресурсов, может выбирать удобное время для запуска шифрования и отслеживать этот процесс. Помимо графической консоли доступна классическая командная строка.

Программный агент устанавливается на пользовательские компьютеры и реализует функции криптографической защиты информации и двухфакторной аутентификации. С помощью агента, работающего в режиме централизованного управления или автономно, информация о пользователях автоматически регистрируется в консоли управления.

При подготовке новостей использованы материалы сайтов tass.ru, reuters.com, securitylab.ru, vedomosti.ru и собственные источники информации.