ISSN 2072-0297

МОЛОДОЙ® УЧЁНЫЙ

международный научный журнал

8
2017
Часть III

16+

СОДЕРЖАНИЕ

ГОСУДАРСТВО И ПРАВО

В целях соблюдения законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, целесообразно установление максимальной прозрачности транзакций с биткойнами, возможности идентификации клиентов, их представителей, выгодоприобретателей и бенефициарных владельцев по таким операциям, установления четких правовых оснований доступа к сведениям об операциях с криптовалютами со стороны уполномоченных государственных органов.

Осуществление обязательного контроля в отношении указанных операций будет способствовать созданию правового механизма противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также предотвращению угрозы безопасности государства и общества в финансовой сфере.

Распространение норм законодательства о банковской тайне на отношения, складывающиеся в процессе использования криптовалют, в частности совершения операций с биткойн, нецелесообразно.

Во-первых, криптовалюты не используются в банковской практике, а применяются частными компаниями и физическими лицами как «частные деньги».

Во-вторых, криптовалюты не являются наличными деньгами и законным средством платежа в России. Их квалификация в качестве денежных средств также сомнительна.

Оборот криптовалют, являющихся денежными суррогатами, не регулируется банковским законодательством и законодательством о национальной платежной системе.

В случае разработки нормативного акта, посвященного регулированию оборота криптовалют, необходимо учитывать нежелательность установления тайны операций с биткойнами.

Они являются денежными суррогатами. Поэтому требования статьи 26 Федерального закона от 02.12.1990 № 395−1 (ред. от 03.07.2016) «О банках и банковской деятельности» (с изм. и доп., вступ. в силу с 01.09.2016) не распространяются на операции с указанными денежными суррогатами.

Литература:

1. Федеральный закон от 10.12.2003 № 173-ФЗ (ред. от 03.07.2016) «О валютном регулировании и валютном контроле» // «Российская газета», № 253, 17.12.2003.
2. Валуйсков, Н.В., Арутюнян, А. Д. Гражданско-правовой статус публично-правового образования-государства в современном гражданском обороте // Государственное и муниципальное право: теория и практика: сборник статей Международной научно-практической конференции (10 ноября 2016 г., г. Пермь). — Уфа: АЭТЕРНА, 2016. — 171 с.
3. Валуйсков, Н. В., Арутюнян А. Д., Бондаренко Л. В. Сущность государства в статусе органов государственной власти // Молодой ученый. 2017. № 3 (137). с. 435−437.
4. Арутюнян, А.Д., Валуйсков, Н. В. Рынок ценных бумаг // Символ науки. 2015. Т. 1. № 3−1 (3). с. 77−79.

Методы борьбы с угрозами информационной безопасности государства

Коккоз Махаббат Мейрамкызы, кандидат технических наук, доцент;
Альжанова Алмагуль Ураловна, магистрант;
Аубакиров Алдияр Мейирманович, магистрант;
Жарилхасинова Динара Кунисбаевна, магистрант
Карагандинский государственный технический университет (Казахстан)

В современном деловом мире происходит процесс миграции материальных активов в сторону информационных. По мере развития государства, усложняется информационное пространство и его инфраструктура. Основной задачей надлежащих органов является обеспечение интересов общества и государства в информационной сфере, а также защиты конституционных прав гражданина. Технологическая эволюция становится источником принципиально новых угроз, предоставляя недоступные ранее возможности негативного влияния на личность, общество и государство.

Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями.

Человечество вступило в стадию кардинальных социальных, экономических, политических и иных изменений, характеризующихся быстрым развитием информационной сферы, становящейся одним из ключевых факторов, влияющих на жизнь людей, обществ и государств.

Ведущие государства мира вступили в эру информационного общества, основывающегося на новых технологиях, новых методах и новых подходах, или находятся в процессе его построения. В конечном итоге их использование должно способствовать адекватной новым реалиям реализации конституционных прав граждан, улучшению благосостояния населения, повышению конкурентоспособности компаний, укреплению государственности.

Во время мирового кризиса, количество аппозиционных, экстремистских электронно-информационных ресурсов, влияющих на общественное сознание, растет, в связи с этим появляется необходимость в создании безопасной информационной зоны на территории Казахстан. В соответствии с данной необходимостью, Указом Президента Республики Казахстан от 14 ноября 2011 года была утверждена «Концепция информационной безопасности Республики Казахстан до 2016».

Целью Концепции является создание национальной системы обеспечения информационной безопасности, гарантирующей защиту национальных интересов Республики Казахстан в информационной сфере. Данная концепция так же направлена на борьбу с рядом угроз национальной безопасности.

Посредством использования информационной инфраструктуры недоброжелатели могут повлиять на стабильность нашего государства и вызвать:

— неконтролируемые миграционные процессы;

— утрату культурного и духовного наследия народа Республики Казахстан;

— обострение социальной и политической обстановки, выражающееся в межнациональных и межконфессиональных конфликтах, массовых беспорядках;

— деятельность, направленную на насильственное изменение конституционного строя, в том числе действия, посягающие на унитарность Республики Казахстан, целостность, неприкосновенность, не отчуждаемость ее территории, безопасность охраняемых лиц;

— терроризм, экстремизм и сепаратизм в любых их формах и проявлениях;

— разведывательно-подрывную деятельность специальных служб иностранных государств, а также организаций и отдельных лиц, направленную на нанесение ущерба национальной безопасности;

— дезорганизацию деятельности государственных органов, нарушение их бесперебойного функционирования, снижение степени управляемости в стране;

— снижение устойчивости финансовой системы;

— создание не предусмотренных законодательством Республики Казахстан военизированных формирований;

— информационное воздействие на общественное и индивидуальное сознание, связанное с преднамеренным искажением и распространением недостоверной информации в ущерб национальной безопасности. [1]

По этой причине одним из основных видов национальной безопасности является информационная. Киберпреступники могут повлиять на работу нашей инфраструктуры и внедриться в наше информационное пространство посредством сети Интернет, таким образом можно предположить, что информационная безопасность во многом зависит от связи со Всемирной паутиной.

Данная статья будет посвящена изучению одного из основных звеньев сетевой безопасности, а именно изучению межсетевых экранов.

Межсетевые экраны (firewall, брандмауэр) делают возможной фильтрацию входящего и исходящего трафика, идущего через систему. Межсетевой экран использует один или более наборов правил для проверки сетевых пакетов при их входе или выходе через сетевое соединение, он или позволяет прохождение трафика или блокирует его. Правила межсетевого экрана могут проверять одну или более характеристик пакетов, включая но не ограничиваясь типом протокола, адресом хоста источника или назначения и портом источника или назначения.

Межсетевые экраны могут серьезно повысить уровень безопасности хоста или сети. Они могут быть использованы для выполнения одной или более нижеперечисленных задач:

— для защиты и изоляции приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети Интернет.

— для ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети интернет.

— для поддержки преобразования сетевых адресов (network address translation, NAT), что дает возможность задействовать во внутренней сети приватные IP адреса и совместно использовать одно подключение к сети Интернет (либо через один выделенный IP адрес, либо через адрес из пула автоматически присваиваемых публичных адресов).

Существует два основных способа создания наборов правил межсетевого экрана: включающий и исключающий. Исключающий межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил. Включающий межсетевой экран действует прямо противоположным образом. Он пропускает только трафик, соответствующий правилам и блокирует все остальное.

Включающий межсетевой экран обеспечивает гораздо большую степень контроля исходящего трафика. Поэтому включающий межсетевой экран является лучшим выбором для систем, предоставляющих сервисы в сети Интернет. Он также контролирует тип трафика, порождаемого вне и направляющегося в приватную сеть. Трафик, не попавший в правила, блокируется, а в файл протокола вносятся соответствующие записи. Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика.

Безопасность может быть дополнительно повышена с использованием межсетевого «экрана с сохранением состояния». Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только

трафик через открытые соединения или открытие новых соединений. Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (Denial of Service, отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением состояния и без сохранения состояния, что позволяет создавать оптимальную конфигурацию для каждой конкретной системы.

Глобальная сеть Интернет создавалась как открытая система, предназначенная для свободного обмена информации. В силу открытости своей идеологии Интернет предоставляет злоумышленникам значительно большие возможности по проникновению в информационные системы.

Через интернет нарушитель может:

— вторгнуться во внутреннюю сеть Государства и получить несанкционированный доступ к конфиденциальной информации;

— незаконно скопировать важную и ценную для Государства информацию;

— получить пароли, адреса серверов, а подчас и их содержимое;

— осуществить информационное воздействие на общественное и индивидуальное сознание, связанное с преднамеренным искажением и распространением недостоверной информации в ущерб национальной безопасности и т. д.

Посредством получения злоумышленником секретной информации может быть серьезно подорвана конкурентоспособность государства.

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать межсетевые экраны. Межсетевой экран — это система межсетевой защиты, позволяющая разделить каждую сеть на две и более части и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между сетью государства и глобальной сетью Интернет. Использование межсетевых экранов позволяет организовать внутреннюю политику безопасности сети, разделив всю сеть на сегменты. Это позволяет сформулировать основные принципы архитектуры безопасности сети

Межсетевой экран пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение: дать ему возможность пройти или нет. Для того чтобы межсетевой экран мог осуществить эту операцию, ему необходимо определить набор правил фильтрации. Решение о том, фильтровать ли с помощью межсетевого экрана конкретные протоколы и адреса, зависит от принятой в защищаемой сети политики безопасности. Межсетевой экран представляет собой набор компонентов, настраиваемых для реализации выбранной политики безопасности.

Политика сетевой безопасности каждого государства должна включать две составляющие:

1. Политика доступа к сетевым сервисам.
2. Политика реализации межсетевых экранов.

Политика доступа к сетевым сервисам должна быть уточнением общей политики государства в отношении защиты информационных ресурсов в государстве. Для того чтобы межсетевой экран успешно защищал ресурсы государства, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Таковой считается политика, при которой найден гармоничный баланс между защитой сети государства от известных рисков и необходимостью доступа пользователей к сетевым сервисам. В соответствии с принятой политикой доступа к сетевым сервисам определяется список сервисов интернета, к которым пользователи должны иметь ограниченный доступ. Задаются также ограничения на методы доступа, необходимые для того, чтобы пользователи не могли обращаться к запрещенным сервисам интернета обходными путями.

Эффективность защиты внутренней сети с помощью межсетевых экранов зависит не только от выбранной политики доступа к сетевым сервисам и ресурсам внутренней сети, но и от рациональности выбора и использования основных компонентов межсетевого экрана. [2]

Таким образом сетевая безопасность является фундаментом, на основе которого выстраивается вся информационная безопасность, поскольку с развитием компьютерных технологий, количество информации передаваемой при помощи сети интернет ежегодно растет. Из-за отсутствия технической возможности отследить каждый пользовательский сеанс, в целях создания безопасной информационной зоны на территории Казахстан, каждый интернет-провайдер должен быть под надзором соответствующих органов. В связи с тем, что запрещённые сайты с легкостью могут менять свои адреса, необходим постоянный мониторинг и обновление списка ограниченных ресурсов.

Литература:

1. Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» // Закон КЗ. URL: http://online.zakon.kz/Document/?doc_id=31106860#pos=0;0 (дата обращения: 20.02.2017).
2. Межсетевые экраны. Способы организации защиты // Компьютер пресс. URL: http://compress.ru/article.aspx?id=10145 (дата обращения: 20.02.2017).