МЕЖВЕДОМСТВЕННЫЙ НАБЛЮДАТЕЛЬНЫЙ СОВЕТ
РЕШЕНИЕ № 16
от 22-11-2024
о применении международных ограничительных мер Европейского Союза против кибератак, которые представляют собой угрозу Европейскому Союзу или его государствам-членам
Опубликован : 26-11-2024 в Monitorul Oficial № 490-493 статья № 927
ИЗМЕНЕНО
РМНС25 от 26.05.25, МО257-260/28.05.25 ст.8; в силу с 28.05.25

В соответствии с положениями части (7) статьи 11 Закона № 25/2016 о применении международных ограничительных мер (повторное опубликование: Официальный монитор Республики Молдова, 2024 г., №28–31, ст.45), с последующими изменениями, для обеспечения введения в действие Приказа министра иностранных дел № 200-s-9 от 15 ноября 2024 года о присоединении к международным ограничительным мерам Европейского Союза против кибератак, которые представляют собой угрозу Европейскому Союзу или его государствам-членам, с последующими изменениями и дополнениями (Решение (ОВПБ) 2019/797 от 17 мая 2019 года, с последующими изменениями и дополнениями), Межведомственный наблюдательный совет РЕШИЛ:

1. Применить замораживание средств и экономических ресурсов, принадлежащих, находящихся в собственности, владении или под контролем физических и юридических лиц, групп, организаций и органов, перечисленных в приложении (в дальнейшем – *субъекты ограничений*).

2. Запретить предоставление средств и экономических ресурсов в распоряжение, а также в пользование субъектов ограничений.

3. В целях введения в действие мер по замораживанию средств и экономических ресурсов, указанных в пунктах 1 и 2:

3.1. **отчетным единицам**, предусмотренным в части (1) статьи 4 Закона №308/2017 о предупреждении и борьбе с отмыванием денег и финансированием терроризма (в дальнейшем – *Закон № 308/2017*):

3.1.1. применять меры предосторожности в отношении клиентов, аналогичные мерам, установленным в Законе №308/2017 при выявлении субъектов ограничений, в целях блокирования средств и экономических ресурсов, указанных в части (1) статьи 28 Закона № 25/2016 о применении международных ограничительных мер (в дальнейшем – *Закон № 25/2016*). Также, во избежание попыток обхода международных ограничительных мер, отчетным единицам применять меры повышенной предосторожности в отношении клиентов и к субъектам, указанных в части (1) статьи 6 Закона № 25/2016;

3.1.2. замораживать средства и экономические ресурсы, находящиеся в собственности, принадлежащие субъектам ограничений либо находящиеся

под их прямым или косвенным контролем, и незамедлительно, но не позднее чем в течение 24 часов, сообщать об этом в Государственную налоговую службу;

3.1.3. сохранять меры по замораживанию до получения решения Государственной налоговой службы в соответствии со статьей 29 Закона № 25/2016;

3.2. Государственному учреждению «Кадастр недвижимого имущества», Агентству государственных услуг, Единому центральному депозитарию ценных бумаг, Национальной комиссии по финансовому рынку и другим юридическим лицам, наделенным правом регистрации/отчуждения имущества и прав, в том числе долей в уставном капитале юридических лиц, воздержаться от осуществления любых действий, способствующих их передаче и/или конвертации для субъектов ограничений. Информация о действиях, предпринятых для выполнения положений настоящего подпункта, направляется в Государственную налоговую службу незамедлительно, но не позднее 24 часов со дня выявления и применения соответствующей меры;

3.3. в соответствии с положениями статьи 29 Закона № 25/2016, **Государственной налоговой службе**:

3.3.1. принимать решения о замораживании средств или экономических ресурсов субъектов ограничений, выявленных или в отношении которых получено уведомление в соответствии с подпунктом 3.1 или согласно статьям 23 и 28 Закона № 25/2016;

3.3.2. информировать органы, указанные в части (3) статьи 29 Закона № 25/2016 и Межведомственный надзорный совет о мерах, предпринятых в соответствии с положениями подпункта 3.3;

3.3.3. периодически, но не реже одного раза в год, анализировать предписанную меру по замораживанию средств или экономических ресурсов и отменить по собственной инициативе или по запросу, если устанавливается, что ее сохранение более не оправдано, незамедлительно информируя об этом Межведомственный наблюдательный совет.

4. Надзор за выполнением отчетными единицами, предусмотренными в части (1) статьи 4 Закона № 308/2017, мер, установленных в пунктах 1 и 2 решения, осуществляется органами, наделенными функциями по надзору за отчетными единицами, предусмотренными в части (1) статьи 15 Закона № 308/2017 и, соответственно, Службой по предупреждению и борьбе с отмыванием денег – для субъектов, находящихся в сфере ее компетенции, в соответствии с действующим законодательством в сфере предупреждения и борьбы с отмыванием денег и финансированием терроризма.

5. При осуществлении своих обязанностей в сфере международных ограничительных мер **Службе информации и безопасности:**

5.1. информировать Государственную налоговую службу, Службу по предупреждению и борьбе с отмыванием денег и Национальный банк Молдовы в случае получения информации о подготовке и/или применении механизмов обхода мер, предусмотренных настоящим решением, которые

могут повлечь за собой риски осуществления операций, указанных в подпунктах 3.1, 3.2 и 3.3;

5.2. составлять и утверждать в кратчайший срок и в зависимости от располагаемой информации список юридических лиц, в отношении которых имеется документально подтвержденная информация о том, что они находятся под контролем субъекта ограничений, указанного в приложении или являются его фактическими бенефициарами и передать его Государственной налоговой службе с целью рассмотрения целесообразности принятия решения о замораживании средств или экономических ресурсов в соответствии с положениями статьи 29 Закона № 25/2016.

6. Исключения в отношении замораживания средств или экономических ресурсов.

6.1. Государственная налоговая служба может разрешить разблокирование определенных средств или экономических ресурсов или предоставление определенных средств или экономических ресурсов после того, как установит, что соответствующие экономические средства или ресурсы:

6.1.1. необходимы для удовлетворения основных потребностей субъектов ограничений и членов их семей, находящихся на содержании данных физических лиц, включая необходимые платежи для оплаты расходов на питание, по аренде или ипотеке, на лекарства и медицинское обслуживание, налоги, страховые взносы и коммунальные услуги;

6.1.2. предназначены исключительно для оплаты разумных профессиональных гонораров и возмещения понесенных расходов, связанных с оказанием юридических услуг;

6.1.3. предназначены исключительно для оплаты сборов или услуг за текущее хранение или обслуживание замороженных средств или экономических ресурсов;

6.1.4. необходимы для оплаты чрезвычайных расходов, при условии, что Государственная налоговая служба информирует Межведомственный наблюдательный совет о причинах, на основании которых, по его мнению, следует предоставить специальное разрешение, не позднее чем за две недели до предоставления разрешения; или

6.1.5. должны быть перечислены на счет или со счета дипломатического представительства или консульского учреждения или международной организации, пользующейся иммунитетом в соответствии с международным правом, в той мере, в какой такие платежи предназначены для использования в официальных целях дипломатического представительства, консульского учреждения или международной организации;

6.2. Государственная налоговая служба может также разрешить разблокирование определенных средств или экономических ресурсов при соблюдении следующих условий:

6.2.1. средства или экономические ресурсы являются предметом арбитражного решения, вынесенного до даты применения ограничительных мер к субъектам ограничений, предусмотренным в приложении, либо

судебного решения или административных решений, подлежащих исполнению на территории Республики Молдова до или после соответствующей даты;

6.2.2. средства или экономические ресурсы будут использоваться исключительно для удовлетворения запросов, гарантированных судебным решением или решением, указанным в подпункте 6.2.1, или действительность которых признается таким приговором или решением, в пределах, установленных правовыми нормами, регулирующими права лиц, обращающихся с такими запросами;

6.2.3. решение или постановление вынесено не в пользу субъекта ограничений, указанного в приложении; и

6.2.4. признание постановления или решения не противоречит общественному порядку;

6.3. для получения исключений, указанных в подпунктах 6.1 и 6.2, любой субъект ограничений может обратиться в Государственную налоговую службу с письменным заявлением, приложив к нему все соответствующие документы, подтверждающие выполнение условий, указанных в подпунктах 6.1 или 6.2;

6.4. Государственная налоговая служба принимает решение о предоставлении запрашиваемого освобождения после получения заключения Министерства иностранных дел. Заключение Министерства иностранных дел предоставляется в течение 5 рабочих дней со дня получения запроса от Государственной налоговой службы;

6.5. Государственная налоговая служба в течение 15 рабочих дней со дня получения заявления, адресованного в соответствии с подпунктом 6.3, сообщает заявителю ответ в письменной форме. Если исключение запрашивается для удовлетворения основных потребностей или по гуманитарным причинам, ответ сообщается в течение 10 рабочих дней со дня получения заявления;

6.6. если Государственная налоговая служба разрешает разблокирование определенных средств или экономических ресурсов, то это разрешение должно быть строго ограничено целью, для которой оно было предоставлено, и исключительно субъектами ограничений, которых оно непосредственно касается;

6.7. ограничения, указанные в пункте 1, не препятствуют субъектам ограничений, включенным в список, представленный в приложении, осуществлять платежи по договору или соглашению, заключенному субъектом указанных ограничений, или по обязательству, возникшему до даты применения международных ограничительных мер в отношении субъекта данных ограничений, при условии что Государственная налоговая служба установила, что бенефициар данного платежа не является, прямо или косвенно, субъектом ограничений, и в соответствии с положениями статьи 31 Закона № 25/2016;

6.8. ограничения, указанные в пункте 1, не препятствуют кредитованию заблокированных счетов инвестиционными компаниями, банками и другими

поставщиками платежных услуг, которые получают средства, переведенные третьими лицами на счет субъекта ограничения, при условии, что все эти суммы, которые переводятся на данные счета, будут также заблокированы. Соответствующие учреждения должны незамедлительно информировать Государственную налоговую службу о любой такой операции;

6.9. ограничения, указанные в пункте 2, не применяются к суммам, переведенным на заблокированные счета, которые представляют собой:

6.9.1. проценты или другие доходы, накопившиеся на этих счетах;

6.9.2. платежи по заключенным договорам, соглашениям или обязательствам, возникшим до даты применения международных ограничительных мер к соответствующему субъекту ограничений; или

6.9.3. платежи, начисленные по постановлению суда, на основании административных решений или арбитражных решений, подлежащих исполнению на территории Республики Молдова;

6.10. положения подпункта 6.9 применяются при условии, что любые такие проценты, доходы и платежи остаются заблокированными на соответствующих счетах;

6.11. ограничения, предусмотренные в пунктах 1 и 2, не распространяются на предоставление, обработку или выплату денежных средств, других финансовых активов или экономических ресурсов или предоставление товаров и услуг, необходимых для обеспечения своевременной доставки гуманитарной помощи или поддержки другой деятельности, направленной на удовлетворение основных потребностей человека, если такая помощь и деятельность осуществляются:

6.11.1. Организацией Объединенных Наций, в том числе через ее программы, фонды и другие структуры и органы, а также ее специализированными учреждениями и связанными с ней организациями;

6.11.2. международными организациями;

6.11.3. гуманитарными организациями, имеющими статус наблюдателя при Генеральной Ассамблее Организации Объединенных Наций, и членами таких гуманитарных организаций;

6.11.4. финансируемыми на двусторонней или многосторонней основе неправительственными организациями, участвующими в планах гуманитарного реагирования Организации Объединенных Наций, планах реагирования на проблемы беженцев, других гуманитарных призывах Организации Объединенных Наций или кластерах, координируемых Офисом Организации Объединенных Наций по координации гуманитарных вопросов;

6.11.5. организациями и агентствами, которым Европейский Союз выдал сертификат гуманитарного партнерства или которые сертифицированы или признаны государством-членом Европейского Союза или Республикой Молдова в соответствии с национальными процедурами;

6.11.6. специализированными агентствами государств-членов Европейского Союза или Республики Молдова; или

6.11.7. сотрудниками, бенефициарами грантов, филиалами или партнерами по реализации субъектов, указанных в подпунктах 6.11.1–6.11.6,

тогда, когда и в той степени, в которой они действуют в своем соответствующем качестве;

6.12. без ущерба для подпункта 6.11 и в порядке отступления от пунктов 1 и 2 Государственная налоговая служба может разрешить разблокирование определенных замороженных средств или экономических ресурсов или предоставление определенных средств или экономических ресурсов на условиях, которые она сочтет целесообразными, после того как определит, что предоставление указанных средств или экономических ресурсов необходимо для оказания своевременной гуманитарной помощи или для поддержания другой деятельности, отвечающей базовым человеческим потребностям;

6.13. не принимаются к рассмотрению никакие требования в отношении любого договора или сделки, на выполнение которых прямо или косвенно, полностью или частично, повлияли меры, введенные в соответствии с настоящим решением, включая требования о возмещении убытков или любые другие подобные требования, такие как требования о возмещении ущерба или требования об исполнении гарантии, в частности требования о продлении или исполнении обязательства, гарантии или компенсации, особенно финансового характера, независимо от формы, если они предъявлены:

6.13.1. субъектами ограничений, предусмотренными в приложении;

6.13.2. любым физическим или юридическим лицом, организацией или органом, действующими через или от имени субъекта ограничений;

6.14. Государственная налоговая служба незамедлительно информирует Межведомственный наблюдательный совет о предоставлении исключения, предусмотренного в пункте 6.

7. Запрещается въезд, транзит, пребывание и нахождение на территории Республики Молдова физическим лицам, указанным в приложении.

8. Министерству внутренних дел обеспечить применение ограничений, указанных в пункте 7.

9. Исключения из применения ограничений на поездки:

9.1. ограничения, упомянутые в пункте 7, не распространяются на физических лиц, являющихся гражданами Республики Молдова;

9.2. положения пункта 7 не затрагивают случаи, в которых Республика Молдова имеет обязательство по международному праву, а именно:

9.2.1. как страна пребывания международной межправительственной организации;

9.2.2. в качестве страны-организатора международной конференции, созываемой Организацией Объединенных Наций или проводимой под ее эгидой;

9.2.3. в соответствии с многосторонним соглашением, предоставляющим привилегии и иммунитеты;

9.3. исключения из ограничений, введенных в соответствии с пунктом 7, могут быть предоставлены, когда перемещение субъекта ограничений оправдано неотложными гуманитарными причинами или осуществляется с целью участия в межправительственных совещаниях и встречах, продвигаемых или проводимых Европейским Союзом, или встречах,

организованных государством-членом, которое обеспечивает председательство в ОБСЕ, в случае ведения политического диалога, направленного непосредственно на продвижение политических целей ограничительных мер, в том числе безопасность и стабильность в киберпространстве.

9.4. Отступления от мер, предусмотренных пунктом 7, могут быть также разрешены, если въезд или транзит необходим для выполнения судебных процедур.

10. Для получения исключений, указанных в подпунктах 9.2, 9.3 и 9.4, любой субъект, имеющий ограничения на передвижение, может обратиться в Министерство внутренних дел с письменным запросом, приложив к нему все соответствующие документы, подтверждающие цель и обстоятельства перемещения субъекта ограничения.

11. Министерство внутренних дел принимает решение о предоставлении запрошенного исключения после получения заключений Министерства иностранных дел и Службы информации и безопасности. Указанные заключения направляются в течение 5 рабочих дней со дня получения запроса Министерства внутренних дел.

12. Ответ на запрос, адресованный в соответствии с пунктом 10, сообщается заявителю Министерством внутренних дел в письменной форме в течение 15 рабочих дней со дня его получения. Если исключение запрашивается для удовлетворения основных потребностей или по гуманитарным причинам, ответ сообщается в течение 10 рабочих дней со дня получения запроса.

13. Если Министерство внутренних дел дает разрешение на въезд, транзит, пребывание или нахождение на территории Республики Молдова некоторых субъектов ограничений, разрешение строго ограничивается целью, для которой оно было выдано, и исключительно лицами, которых это непосредственно касается.

14. Министерство внутренних дел незамедлительно информирует Межведомственный наблюдательный совет о предоставлении исключений, указанных в пункте 9.

15. Служба информации и безопасности незамедлительно, в зависимости от имеющейся в ее распоряжении информации, составляет список физических и юридических лиц, в отношении которых имеются доказательства и документально подтвержденная информация о том, что они связаны с субъектами ограничений, предусмотренными в приложении, и предпринимает последовательные действия, установленные в статье 6 Закона № 25/2016.

16. В целях выявления, предотвращения и во избежание действий или сделок, направленных на обход международных ограничительных мер, предусмотренных в пунктах 1 и 2, публичные учреждения и органы публичной власти, обладающие компетенцией в соответствующей области, принимают необходимые меры в соответствии со статьей 6 Закона № 25/2016.

17. Органы публичной власти и публичные учреждения, а также физические и юридические лица информируют Межведомственный наблюдательный совет о ситуациях, которые считаются нарушением международных ограничительных мер, применяемых в соответствии с настоящим решением.

18. При получении информации, указанной в пункте 17, Межведомственный наблюдательный совет уведомляет правоохранительные органы о случаях нарушения ограничительных мер, предусмотренных в настоящем решении.

19. Органы публичной власти и публичные учреждения могут напрямую сообщать правоохранительным органам о случаях нарушения ограничительных мер, предусмотренных в настоящем решении. В этих случаях копия уведомления направляется в адрес Межведомственного наблюдательного совета.

20. Органы публичной власти и публичные учреждения, уполномоченные настоящим решением, информируют Межведомственный наблюдательный совет каждые шесть месяцев, а также по запросу о принятых мерах по реализации ограничительных мер, предусмотренных в настоящем решении, а также незамедлительно информируют Межведомственный наблюдательный совет о выявленных трудностях применения.

21. Межведомственный наблюдательный совет через Министерство иностранных дел информирует соответствующие институты Европейского Союза о действиях, предпринятых внутри страны, и о трудностях применения ограничительных мер.

22. Ведение учета ограничительных мер, предусмотренных в настоящем решении, осуществляется с соблюдением положений законодательства о защите и обработке персональных данных. Если такая возможность не предусмотрена специальными правовыми положениями, регулирующими их служебные обязанности, ответственные лица в составе Межведомственного наблюдательного совета и других компетентных органов публичной власти / публичных учреждений могут, если необходимо, обрабатывать соответствующие данные о преступлениях, совершенных субъектами ограничений, предусмотренными в приложении, об их судимости или мерах безопасности в отношении них только в том случае, когда такая обработка необходима для проведения процедур по применению международных ограничительных мер, а также для составления и пополнения национального списка субъектов ограничения. В таких случаях Межведомственный наблюдательный совет и компетентные органы публичной власти / публичные учреждения осуществляют полномочия, предусмотренные Законом № 25/2016, в качестве операторов персональных данных, а ответственные лица в их составе – в качестве уполномоченных оператором лиц, как установлено в законодательстве о защите персональных данных.

23. Обеспечение обнародования информации о субъектах ограничений, предусмотренных в приложении, при соблюдении условий, установленных в Законе №25/2016, не является нарушением правовых норм о защите

персональных данных и не может повлечь за собой привлечение к ответственности ответственных лиц.

24. Настоящее Решение применяется до 18 мая 2028 года и подлежит постоянному пересмотру. Меры, изложенные в пунктах 1–14, применяются к субъектам ограничений, включенным в списки, представленные в приложении, до 18 мая 2026 года.

[Пкт.24 в редакции PMHC25 от 26.05.25, MO257-260/28.05.25 ст.8; в силу с 28.05.25]

25. Настоящее решение вступает в силу с даты опубликования в Официальном мониторе Республики Молдова и публикуется в том числе на официальном веб-сайте Правительства, а также на официальных веб-сайтах публичных органов власти и публичных учреждений, ответственных за его введение в действие.

26. Межведомственный наблюдательный совет может внести изменения в данное решение путем принятия решений о внесении изменений на основании приказов о присоединении к ограничительным мерам Европейского Союза, изданных министром иностранных дел в соответствии с положениями части (8) статьи 11 Закона № 25/2016.

ПРЕМЬЕР-МИНИСТР,
ПРЕДСЕДАТЕЛЬ МЕЖВЕДОМСТВЕННОГО
НАБЛЮДАТЕЛЬНОГО СОВЕТА **Дорин РЕЧАН**

№ 16. Кишинэу, 22 ноября 2024 г.

ПРИЛОЖЕНИЕ

СПИСОК
субъектов, в отношении которых применены международные ограничительные меры согласно Решению (ОВПБ) 2019/797 Совета Европейского Союза от 17 мая 2019 года

A. ФИЗИЧЕСКИЕ ЛИЦА

№ п/п	Фамилия, имя	Идентифицирующая информация	Причины применения ограничительных мер Европейским Союзом	Дата включения в список Европейским Союзом и дата применения ограничений Республикой Молдова
1.	Гао Цян (GAO Qiang)	Дата рождения: 4 октября 1983 г. Место рождения: Shandong Province, China Адрес: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Гражданство: китайское Пол: мужской	Гао Цян (Gao Qiang) участвует в операции „Operation Cloud Hopper", серии кибератак с серьезными последствиями, происходящих за пределами Союза и представляющих внешнюю угрозу для Союза или его государств-членов, а также кибератак с серьезными последствиями для третьих стран. „Operation Cloud Hopper" была нацелена на информационные системы транснациональных предприятий на шести континентах, включая предприятия, расположенные в Союзе, и получила несанкционированный доступ к коммерчески конфиденциальным данным, что привело к значительным экономическим потерям. Актер, широко известный как „APT10" („Advanced Persistent Threat 10") (*псевдоним*: „Red. Apollo", „CVNX", „Stone Panda", „MenuPass" и „Potassium") осуществил „Operation Cloud Hopper". Между Гао Цяном и APT10 может быть установлена связь, в том числе путем его подключения к инфраструктуре управления и контроля APT10. Кроме того, Гао Цян был сотрудником компании Huaying Haitai, организации, назначенной для оказания поддержки и содействия операции «Cloud Hopper». Он связан с Чжан Шилун, который сам был назначен в связи с операцией „Cloud Hopper". Таким образом, Гао Цян связан как с Хуайин Хайтаем, так и с Чжан Шилуном	ЕС- 30.07.2020 РМ- 13.06.2023
2.	Чжан Шилун (ZHANG Shilong)	Дата рождения: 10 сентября 1981 г. Место рождения: Китай	Чжан Шилун (Zhang Shilong) участвует в операции „Operation Cloud Hopper", серии кибератак с серьезными последствиями, происходящих за пределами Союза и представляющих внешнюю	ЕС- 30.07.2020 РМ- 13.06.2023

		Адрес: Hedong, Yuyang Road No 121, Tianjin, China Гражданство: китайское Пол: мужской	угрозу для Союза или его государств-членов, а также кибератак с серьезными последствиями для третьих стран. „Operation Cloud Hopper" была нацелена на информационные системы транснациональных предприятий на шести континентах, включая предприятия, расположенные в Союзе, и получила несанкционированный доступ к коммерчески конфиденциальным данным, что привело к значительным экономическим потерям. Актер, широко известный как «APT10» («Продвинутая постоянная угроза 10») (псевдоним: „Red. Apollo", „CVNX", „Stone Panda", „MenuPass" и „Potassium") провел операцию «Cloud Hopper». Связь между Чжан Шилун и APT10 может быть установлена, в том числе через вредоносное ПО, которое он разработал и протестировал в связи с кибератаками, осуществленными APT10. Кроме того, в Huaying Haitai, организации, назначенной для оказания поддержки и содействия операции «Cloud Hopper», работал Чжан Шилун. Он связан с Гао Цяном, который, в свою очередь, был назначен в связи с операцией «Cloud Hopper». Таким образом, Чжан Шилун связан как с Хуайин Хайтаем, так и с Гао Цяном	
3.	Алексей Валерьевич МИНИН	Алексей Валерьевич МИНИН Дата рождения: 27.05.1972 Место рождения: Пермский край, РСФСР (ныне Российская Федерация) Номер паспорта: 120017582 Выдано: Министерством иностранных дел Российской Федерации Действительно с 17.4.2017 по 17.4.2022 Место: Москва, Российская Федерация Гражданство: Русский Пол: мужской	Алексей Минин принимал участие в попытке кибератаки с потенциально значительными последствиями на Организацию по запрещению химического оружия (ОЗХО) в Нидерландах, а также в кибератаках с существенными последствиями на третьи государства. Будучи офицером по поддержке агентурной разведки Главного управления Генерального штаба Вооруженных сил Российской Федерации (ГУ/ГРУ), Алексей Минин входил в группу из четырех офицеров российской военной разведки, которые в апреле 2018 года попытались получить несанкционированный доступ к сети Wi-Fi ОЗХО в Гааге, Нидерланды. Целью попытки кибератаки было получение несанкционированного доступа к сети Wi-Fi ОЗХО, что в случае успеха поставило бы под угрозу безопасность сети и текущую следственную работу ОЗХО. Служба безопасности, разведки и обороны Нидерландов (Militaire Inlichtingen- en Veiligheidsdienst) пресекла попытку кибератаки, тем самым предотвратив нанесение серьезного ущерба ОЗХО.	ЕС – 30.07.2020 РМ – 13.06.2023

			Большое жюри Западного округа Пенсильвании (Соединенные Штаты Америки) предъявило Алексею Минину как офицеру Главного разведывательного управления России (ГРУ) обвинения в компьютерном взломе, мошенничестве с использованием электронных средств связи, краже личных данных при отягчающих обстоятельствах и отмывании денег ГРУ продолжает активно проводить кибератаки против Союза или его государств-членов. Таким образом, как сотрудник ГРУ, г-н Алексей Минин причастен к кибератакам со значительными последствиями, включая попытки кибератак с потенциально значительными последствиями, которые представляют собой внешнюю угрозу для Союза или его государств-членов.	
4.	Алексей Сергеевич МОРЕНЕЦ	Алексей Сергеевич МОРЕНЕЦ Дата рождения: 31.07.1977 Место рождения: Мурманская область, РСФСР (ныне Российская Федерация) Номер паспорта: 100135556 Выдан: Министерством иностранных дел Российской Федерации Действителен с 17.04.2017 по 17.04.2022 Место: Москва, Российская Федерация Гражданство: российское Пол: мужской	Алексей Моренец принимал участие в попытке кибератаки с потенциально значительными последствиями на Организацию по запрещению химического оружия (ОЗХО) в Нидерландах, а также в кибератаках с существенными последствиями на третьи государства. Работая оператором ЭВМ Главного управления Генерального штаба Вооруженных сил Российской Федерации (ГУ/ГРУ), Алексей Моренец входил в группу из четырех офицеров российской военной разведки, которые в апреле 2018 года попытались получить несанкционированный доступ к сети Wi-Fi ОЗХО в Гааге, Нидерланды. Целью попытки кибератаки был несанкционированный доступ к сети Wi-Fi ОЗХО, что в случае успеха поставило бы под угрозу безопасность сети и текущую следственную работу ОЗХО. Служба безопасности, разведки и обороны Нидерландов (Militaire Inlichtingen- en Veiligheidsdienst) пресекла попытку кибератаки, тем самым предотвратив нанесение серьезного ущерба ОЗХО. Большое жюри Западного округа Пенсильвании (Соединенные Штаты Америки) предъявило обвинение Алексею Моренцу как военнослужащему воинской части 26165 во взломе компьютеров, мошенничестве с использованием электронных средств связи, тяжком хищении личных данных и отмывании денег. ГРУ продолжает активно осуществлять кибератаки против Союза и его государств-членов. Таким образом, будучи	ЕС – 30.07.2020 РМ – 13.06.2023

			сотрудником ГРУ, Алексей Моренец участвует в кибератаках со значительным эффектом, включая попытки кибератак с потенциально значительным эффектом, которые представляют собой внешнюю угрозу Союзу или его государствам-членам.	
5.	Евгений Михайлович СЕРЕБРЯКОВ	Евгений Михайлович СЕРЕБРЯКОВ Дата рождения: 26.07.1981 г. Место рождения: Курск, РСФСР (ныне Российская Федерация) Номер паспорта: 100135555 Выдано: Министерством иностранных дел Российской Федерации Действительно с 17.04.2017 г. по 17.04.2022 г. Место: Москва, Российская Федерация Гражданство: российское Пол: мужской	Евгений Серебряков принимал участие в попытке кибератаки с потенциально значительными последствиями на Организацию по запрещению химического оружия (ОЗХО) в Нидерландах, а также в кибератаках с существенными последствиями на третьи государства. Будучи кибероператором Главного управления Генерального штаба Вооруженных сил Российской Федерации (ГУ/ГРУ), Евгений Серебряков входил в группу из четырех офицеров российской военной разведки, которые в апреле 2018 года попытались получить несанкционированный доступ к сети Wi-Fi ОЗХО в Гааге, Нидерланды. Целью попытки кибератаки было получение несанкционированного доступа к сети Wi-Fi ОЗХО, что в случае успеха поставило бы под угрозу безопасность сети и продолжающуюся следственную работу ОЗХО. Служба безопасности, разведки и обороны Нидерландов (Militaire Inlichtingen- en Veiligheidsdienst) пресекла попытку кибератаки, тем самым предотвратив нанесение серьезного ущерба ОЗХО. С весны 2022 года Евгений Серебряков возглавляет «Sandworm» (также известные как «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» и «Telebots») — актёрскую и хакерскую группу, связанную с подразделением 74455 Главного разведывательного управления РФ. Sandworm осуществил кибератаки на Украину, в том числе на украинские	ЕС – 30.07.2020 РМ – 13.06.2023

			государственные учреждения, после начала агрессивной войны России против Украины. ГРУ продолжает активно осуществлять кибератаки против Союза и его государств-членов. Таким образом, будучи сотрудником ГРУ, Евгений Серебряков участвует в кибератаках со значительными последствиями, включая попытки кибератак с потенциально значительными последствиями, которые представляют собой внешнюю угрозу Союзу или его государствам-членам.	
6.	Олег Михайлович СОТНИКОВ	Олег Михайлович СОТНИКОВ Дата рождения: 24.08.1972 г. Место рождения: Ульяновск, РСФСР (ныне Российская Федерация) Номер паспорта: 120018866 Выдано: Министерством иностранных дел Российской Федерации Действительно с 17.4.2017 г. по 17.4.2022 г. Место: Москва, Российская Федерация Гражданство: российское Пол: мужской	Олег Сотников принимал участие в попытке кибератаки с потенциально значительными последствиями на Организацию по запрещению химического оружия (ОЗХО) в Нидерландах, а также в кибератаках с существенными последствиями на третьи государства. Будучи офицером поддержки агентурной разведки Главного управления Генерального штаба Вооруженных сил Российской Федерации (ГУ/ГРУ), Олег Сотников входил в группу из четырех офицеров российской военной разведки, которые в апреле 2018 года попытались получить несанкционированный доступ к сети Wi-Fi ОЗХО в Гааге, Нидерланды. Целью попытки кибератаки было получение несанкционированного доступа к сети Wi-Fi ОЗХО, что в случае успеха поставило бы под угрозу безопасность сети и текущую следственную работу ОЗХО. Служба безопасности, разведки и обороны Нидерландов (Militaire Inlichtingen- en Veiligheidsdienst) пресекла попытку кибератаки, тем самым предотвратив нанесение серьезного ущерба ОЗХО. Большое жюри Западного округа Пенсильвании (Соединенные Штаты Америки) предъявило обвинение Олегу Сотникову как офицеру ГРУ во взломе компьютеров, мошенничестве с использованием электронных средств связи, тяжком хищении личных данных и отмывании денег. ГРУ продолжает активно осуществлять кибератаки против Союза и его государств-членов. Таким образом, будучи сотрудником ГРУ, Олег Сотников участвует в кибератаках со	ЕС – 30.07.2020 РМ – 13.06.2023

			значительным эффектом, включая попытки кибератак с потенциально значительным эффектом, которые представляют собой внешнюю угрозу Союзу или его государствам-членам.	
7.	Дмитрий Сергеевич БАДИН	Дмитрий Сергеевич БАДИН Дата рождения: 15.11.1990 г. Место рождения: Курск, РСФСР (ныне Российская Федерация) Гражданство: российское Пол: мужской	Дмитрий Бадин принимал участие в кибератаке, повлекшей за собой значительные последствия для Федерального парламента Германии (Deutscher Bundestag), а также в кибератаках, повлекших за собой значительные последствия для третьих государств. Будучи офицером военной разведки 85-го Главного центра специального назначения (ГЦСС) Главного управления Генерального штаба Вооруженных сил Российской Федерации (ГУ/ГРУ), Дмитрий Бадин входил в группу сотрудников российской военной разведки, организовавших в апреле-мае 2015 года кибератаку на Федеральный парламент Германии. Кибератака была направлена на компьютерную систему парламента, что нарушило его работу на несколько дней. Был украден значительный объем данных, пострадали учетные записи электронной почты нескольких парламентариев, а также бывшего канцлера Ангелы Меркель. Большое жюри Западного округа Пенсильвании (Соединенные Штаты Америки) предъявило обвинение Дмитрию Бадину как военнослужащему воинской части 26165 во взломе компьютеров, мошенничестве с использованием электронных средств связи, тяжком хищении личных данных и отмывании денег. ГРУ продолжает активно осуществлять кибератаки против Союза и его государств-членов. Таким образом, являясь сотрудником ГРУ, Дмитрий Бадин участвует в кибератаках со значительным эффектом, включая попытки кибератак с	ЕС – 22.10.2020 РМ – 13.06.2023

			потенциально значительным эффектом, которые представляют собой внешнюю угрозу Союзу или его государствам-членам.	
8.	Игорь Олегович КОСТЮКОВ	Игорь Олегович КОСТЮКОВ Дата рождения: 21.02.1961 г. Гражданство: российское Пол: мужской	Игорь Костюков — нынешний начальник Главного управления Генерального штаба Вооружённых Сил Российской Федерации (ГУ/ГРУ), где ранее занимал должность первого заместителя начальника. Одним из подразделений, находящихся под его командованием, является 85-й Главный центр специального назначения (ГЦСС) (он же «в/ч 26165», «АПТ28», «Fancy Bear», «Sofacy Group», «Pawn Storm» и «Стронций»). В этой должности Игорь Костюков несет ответственность за кибератаки, осуществляемые ГЦСС, в том числе за атаки со значительными последствиями, представляющими внешнюю угрозу Союзу или его государствам-членам. В частности, сотрудники военной разведки ГЦСС принимали участие в кибератаке на федеральный парламент Германии (Deutscher Bundestag) в апреле и мае 2015 года, а также в попытке кибератаки в апреле 2018 года с целью взлома сети Wi-Fi Организации по запрещению химического оружия (ОЗХО) в Нидерландах. Кибератака на федеральный парламент Германии была направлена на его компьютерную систему, что на несколько дней нарушило его работу. Был украден значительный объем данных, пострадали учетные записи электронной почты нескольких парламентариев, а также бывшего канцлера Ангелы Меркель. ГРУ продолжает активно осуществлять кибератаки против Союза и его государств-членов. Таким образом, будучи	ЕС – 22.10.2020 РМ - 13.06.2023

			сотрудником ГРУ, Игорь Костюков участвует в кибератаках со значительным эффектом, включая попытки кибератак с потенциально значительным эффектом, которые представляют собой внешнюю угрозу Союзу или его государствам-членам.	
9.	Руслан Александрович Перетятько (Ruslan Aleksandrovich PERETYATKO)	Руслан Александрович ПЕРЕТЯТЬКО Дата рождения: 3.8.1985 Гражданство: российское Пол: мужской	Руслан Перетьятко участвовал в кибератаках со значительным эффектом, представляющим внешнюю угрозу Союзу или его государствам-членам. Руслан Перетятько входит в «группу Каллисто» российских военных разведчиков, которые проводят кибероперации против стран-членов ЕС и третьих стран. Группа Callisto (также известная как «Seaborgium», «Star Blizzard», «ColdRiver», «TA446») запустила многолетние фишинговые кампании, используемые для кражи данных учетной записи и личных данных для входа. Кроме того, группа Каллисто отвечает за кампании, направленные против отдельных лиц и важнейших функций государства, в том числе в сфере обороны и международных отношений. Таким образом, Руслан Перетятько причастен к кибератакам, значительный эффект которых представляет собой внешнюю угрозу Союзу или его государствам-членам	ЕС- 24.06.2024 РМ- 26.11.2024
10.	Андрей Станиславович Коринец (Andrey Stanislavovich KORINETS)	Андрей Станиславович КОРИНЕЦ Дата рождения: 18.5.1987 Место рождения: город Сыктывкар, Россия Гражданство: российское Пол: мужской	Коринец Андрей Станиславович участвовал в кибератаках, значительный эффект которых представлял собой внешнюю угрозу Союзу или его государствам-членам. Андрей Станиславович Коринец — сотрудник «Центра 18» Федеральной службы безопасности (ФСБ) Российской Федерации. Андрей Станиславович Коринец входит в «группу Каллисто» российских военных разведчиков, которые проводят кибероперации против государств-членов ЕС и третьих стран. Группа Callisto (также известная как «Seaborgium», «Star Blizzard», «ColdRiver», «TA446») запустила многолетние фишинговые кампании, используемые для кражи данных учетной записи и личных данных для входа. Кроме того, группа Каллисто отвечает за кампании, направленные против отдельных лиц и важнейших функций государства, в том числе в сфере обороны и международных отношений. Таким образом, Андрей Станиславович Коринец причастен к кибератакам, значительный эффект которых представляет собой внешнюю угрозу Союзу или его государствам-членам	ЕС- 24.06.2024 РМ- 26.11.2024

11.	Александр Склянко (Oleksandr SKLIANKO)	Александр СКЛЯНКО (русское правописание) Олександр СКЛЯНКО (украинское правописание) Дата рождения: 5.8.1973 Паспорт: ЕС 867868, выдан 27.11.1998 (Украина) Пол: мужской	Александр Склянко участвовал в кибератаках со значительным эффектом против государств-членов ЕС, а также в кибератаках со значительным эффектом против третьих стран. Александр Склянко входит в состав хакерской группы «Армагеддон», поддерживаемой Федеральной службой безопасности (ФСБ) Российской Федерации, которая осуществила различные кибератаки, оказавшие существенное влияние на правительство Украины и государств-членов ЕС и их правительственных чиновников, в том числе с использованием фишинговых писем и кампаний по распространению вредоносного ПО. Таким образом, Александр Склянко причастен к кибератакам со значительным эффектом против третьих стран, а также к кибератакам со значительным эффектом, которые представляют собой внешнюю угрозу Союзу или его государствам-членам	ЕС- 24.06.2024 РМ- 26.11.2024
12.	Николай Черных (Mykola CHERNYKH)	Николай ЧЕРНЫХ (русское правописание) Микола ЧЕРНИХ (украинское правописание) Дата рождения: 12.10.1978 Паспорт: СЕ 922162, выдан 20.1.1999 (Украина) Пол: мужской	Николай Черных участвовал в кибератаках со значительным эффектом против государств-членов ЕС, а также в кибератаках со значительным эффектом против третьих стран. Николай Черных входит в состав хакерской группы «Армагеддон», поддерживаемой Федеральной службой безопасности (ФСБ) Российской Федерации, которая осуществляет различные кибератаки, оказывающие существенное влияние на правительство Украины и государств-членов ЕС, а также их правительственных чиновников, в том числе с использованием фишинговые электронные письма и кампании по распространению вредоносного ПО. Как бывшему сотруднику Службы безопасности Украины ему предъявлено обвинение в Украине в государственной измене и несанкционированном вмешательстве в работу электронных вычислительных машин и автоматизированных систем. Таким образом, Николай Черных участвует в кибератаках, значительный эффект которых представляет собой внешнюю угрозу Союзу или его государствам-членам	ЕС- 24.06.2024 РМ- 26.11.2024

13.	Михаил Михайлович Царев (Mikhail Mikhailovich TSAREV)	Михаил Михайлович ЦАРЕВ Дата рождения: 20.4.1989 Место рождения: Серпухов, Российская Федерация Гражданство: российское Адрес: Серпухов Пол: мужской	Михаил Михайлович Царев участвовал в кибератаках со значительным эффектом, представляющих внешнюю угрозу для стран-членов ЕС. Михаил Михайлович Царев, также известный под псевдонимами „Mango”, „Alexander Grachev”, „Super Misha”, „Ivanov Mixail”, „Misha Krutysha” и „Nikita Andreevich Tsarev”, является ключевым игроком в распространении вредоносного ПО „Conti” и „Trickbot”, а также участвует во враждебной группировке „Wizard Spider” в России. Вредоносные программы «Conti» и «Trickbot» были созданы и разработаны компанией Wizard Spider. Wizard Spider проводил кампании по распространению программ-вымогателей в различных секторах, включая критически важные услуги, такие как здравоохранение и банковское дело. Группа заразила компьютеры по всему миру, а ее вредоносное ПО превратилось в модульный набор вредоносных программ. Кампании Wizard Spider, использующие такие вредоносные программы, как Conti, «Ryuk» и TrickBot, наносят существенный экономический ущерб Европейскому Союзу. Таким образом, Михаил Михайлович Царев причастен к кибератакам со значительным эффектом, которые представляют собой внешнюю угрозу Союзу или его государствам-членам	ЕС- 24.06.2024 РМ- 26.11.2024
14.	Максим Сергеевич Галочкин (Maksim Sergeevich GALOCHKIN)	Максим Сергеевич ГАЛОЧКИН Дата рождения: 19.5.1982 Место рождения: Абакан, Российская ФедерацияГражданство: российское Пол: мужской	Максим Галочкин участвовал в кибератаках, последствия которых представляют собой внешнюю угрозу для стран-членов ЕС. Максим Галочкин также известен под псевдонимами «Benalen», «Bentley», «Volhvb», «volhvb», «manuel», «Max17» и «Crypt». Галочкин является ключевым игроком в распространении вредоносных программ «Conti» и «Trickbot» и участвует во враждебной российской группировке «Wizard Spider». Он возглавлял группу тестировщиков, ответственных за разработку, контроль и применение тестов шпионской программы TrickBot, созданной и развернутой Wizard Spider. Wizard Spider проводил кампании по распространению программ-вымогателей в различных секторах, включая критически важные услуги, такие как здравоохранение и банковское дело. Группа заразила компьютеры по всему миру, а ее вредоносное ПО превратилось в модульный набор вредоносных программ. Кампании Wizard Spider, использующие такие вредоносные программы, как Conti, «Ryuk» и TrickBot,	ЕС- 24.06.2024 РМ- 26.11.2024

			наносят существенный экономический ущерб Европейскому Союзу. Таким образом, Максим Галочкин причастен к кибератакам со значительным эффектом, представляющим внешнюю угрозу Союзу или его государствам-членам	
15.	Николай Александрович КОРЧАГИН	Николай Александрович Корчагин Дата рождения: 16.9.1997 г. Гражданство: российское Пол: мужской Связанная организация: Главное управление Генерального штаба Вооруженных Сил Российской Федерации	Николай Корчагин участвует в кибератаках со значительными последствиями и несет ответственность за них, проводя разведывательную деятельность против Эстонии и незаконно получая доступ к информационной системе. Николай Корчагин – офицер воинской части 29155 Главного управления Генерального штаба Вооруженных Сил Российской Федерации (ГРУ). В этом качестве он участвует и несет ответственность за кибератаки на информационные системы, атаки, направленные на сбор из систем данных нескольких учреждений, данных, которые независимо или в сочетании дают обзор политики кибербезопасности Эстонии, государственных кибервозможностей, конфиденциальных личных данных и других конфиденциальных данных с целью использования этих данных для угрозы безопасности Эстонии. Таким образом, атаки нацелены на хранение секретной информации. Атаки были направлены против союзников и партнеров Эстонии. Таким образом, Николай Корчагин участвует и несет ответственность за кибератаки со значительными последствиями,	ЕС –27.01.2025 РМ – 07.03.2025 г.

			представляющими внешнюю угрозу для государства-члена	
16.	Виталий ШЕВЧЕНКО	Виталий Шевченко Дата рождения: 1.9.1997 г. Гражданство: российское Пол: мужской Связанная организация: Главное управление Генерального штаба Вооруженных Сил Российской Федерации	Виталий Шевченко участвует в кибератаках со значительными последствиями и несет ответственность за них, проводя разведывательную деятельность против Эстонии и незаконно получая доступ к информационной системе. Виталий Шевченко – офицер воинской части 29155 Главного управления Генерального штаба Вооруженных Сил Российской Федерации (ГРУ). В этом качестве он участвует и несет ответственность за кибератаки на информационные системы, атаки, направленные на сбор данных из систем данных нескольких учреждений, которые по отдельности или вместе предоставляют обзор политики кибербезопасности Эстонии, кибервозможностей государства, конфиденциальных личных данных и других конфиденциальных данных с целью использования этих данных для угрозы безопасности Эстонии. Таким образом, атаки нацелены на хранение секретной информации. Атаки были направлены против союзников и партнеров Эстонии. Таким образом, Виталий Шевченко участвует и несет ответственность за кибератаки со значительными последствиями, которые представляют собой внешнюю угрозу для государства-члена	ЕС –27.01.2025 РМ – 07.03.2025 г.
17.	Юрий Федорович ДЕНИСОВ	Юрий Федорович Денисов Дата рождения: 17.6.1980 г. Гражданство: российское Пол: мужской	Юрий Денисов участвует в кибератаках со значительными последствиями и несет ответственность за них, проводя разведывательную	ЕС –27.01.2025 РМ – 07.03.2025 г.

		Зависимое лицо: Главное управление Генерального штаба Вооруженных Сил Российской Федерации	деятельность против Эстонии и незаконно получая доступ к информационной системе. Юрий Денисов – офицер воинской части 29155 Главного управления Генерального штаба Вооруженных Сил Российской Федерации (ГРУ). В этом качестве он участвует и несет ответственность за кибератаки на информационные системы, атаки, направленные на сбор данных из систем данных нескольких учреждений, данных, которые независимо или в сочетании предоставляют обзор политики кибербезопасности Эстонии, кибервозможностей государства, конфиденциальных личных данных других конфиденциальных данных с целью использования этих данных для угрозы безопасности Эстонии. Таким образом, атаки нацелены на хранение секретной информации. Атаки были направлены против союзников и партнеров Эстонии. Таким образом, Юрий Денисов участвует и несет ответственность за кибератаки со значительными последствиями, которые представляют собой внешнюю угрозу для государства-члена	

B. Юридические лица, учреждения и организации

№ п/п	Наименование	Идентифицирующая информация	Причины применения ограничительных мер Европейским Союзом	Дата включения в список Европейским Союзом и дата применения ограничений Республикой Молдова
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	*известна также как* Haitai Technology Development Co. Ltd Местоположение: Тяньцзинь, Китай	Хуайин Хайтай (Huaying Haitai) предоставил финансовую, техническую или материальную поддержку и содействовал операции «Operation Cloud Hopper», серии кибератак с серьезными последствиями, происходящих за пределами Союза и представляющих внешнюю угрозу для Союза или его государств-членов, а также в кибератаках, имеющих важные последствия для третьих стран. Операция «Operation Cloud Hopper» была нацелена на информационные системы транснациональных предприятий на шести континентах, включая предприятия, расположенные в Союзе, и получила несанкционированный доступ к коммерчески конфиденциальным данным, что привело к значительным экономическим потерям. Актер, широко известный как «APT10» («Advanced Persistent Threat 10») (известна также как «Red. Apollo», «CVNX», «Stone Panda», «MenuPass» и «Katassium»), провел Операцию «Operation Cloud Hopper». Между Huaying Haitai и APT10 может быть установлена связь. Кроме того, Гао Цян и Чжан Шилун, оба внесенные в список в связи с операцией «Operation Cloud Hopper», были сотрудниками Huaying Haitai. Таким образом, Хуайин Хайтай ассоциируется с Гао Цяном и Чжан Шилуном	30.07.2020
2.	Chosun Expo	*известна также как* Chosen Expo; Korea Export Joint Venture Locație RPDC	Chosun Expo предоставила финансовую, техническую или материальную поддержку и способствовала серии кибератак со значительными последствиями, возникшими за пределами Союза и представляющими внешнюю угрозу для Союза или его государств-членов, а также в кибератаках, имеющих значительные последствия для третьих стран, включая кибератаки, известные	30.07.2020

			как «WannaCry», и кибератаки на Управление финансового надзора Польши и Sony Pictures Entertainment, а также киберкражу банка Бангладеш и попытку киберкражи во вьетнамском банке «Tien Phong Bank». «WannaCry» нарушил работу информационных систем по всему миру, атаковав информационные системы программами-вымогателями и заблокировав доступ к данным. Это затронуло информационные системы предприятий в Союзе, включая информационные системы, связанные с услугами, необходимыми для поддержания основных услуг и экономической деятельности в государствах-членах. Атака «WannaCry» была осуществлена злоумышленником, широко известным как «APT38» («Advanced Persistent Threat 38») или «Lazarus Group». Также может быть установлена связь между Chosun Expo и APT38/Lazarus Group, в том числе через учетные записи, используемые для кибератак	
3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [Главный центр специальных технологий (ГЦСТ) Главного управления Генерального штаба Вооруженных Сил России (ГУ/ГРУ)]	Адрес: 22 Kirova Street, Moscow, Russian Federation (Российская Федерация, г. Москва, ул. Кирова, д. 22)	Главный центр специальных технологий (ГЦСТ) Главного управления Генерального штаба Вооруженных Сил России (ГУ/ГРУ), известный также под полевым почтовым индексом 74455, участвует в серии мощных кибератак, в результате которых происходящие за пределами Союза и представляющие внешнюю угрозу Союзу или его государствам-членам, а также в кибератаках, имеющих значительные последствия для третьих стран, включая кибератаки, публично известные как «NotPetya» или «EternalPetya» в июне 2017 года, и кибератаки против украинской энергосистемы зимой 2015 и 2016 годов. «NotPetya» или «EternalPetya» заблокировали доступ к данным на нескольких предприятиях в Союзе, Европе в целом и по всему миру, атаковав компьютеры программами-вымогателями и заблокировав доступ к данным, что привело, в том числе, к значительным экономическим потерям. Кибератака на украинскую энергосистему привела к отключению некоторых ее частей зимой. Актер, широко известный как «Sandworm» (также известный как „Sandworm Team", „BlackEnergy Group", „Voodoo Bear", „Quedagh", „Olympic Destroyer" и „Telebots"), также стоит за атакой на энергосистему Украины, атаку совершил «NotPetya» или «EternalPetya». Sandworm провела кибератаки против Украины, в том числе против украинских правительственных учреждений и критически важной украинской инфраструктуры, после	30.07.2020

			агрессивной войны России против Украины. Эти кибератаки включают целевые фишинговые кампании, атаки вредоносных программ и программы-вымогатели. Главный центр специальных технологий Главного управления Генерального штаба Вооруженных Сил РФ играет активную роль в кибердеятельности Sandworm, и между ним и центром может быть установлена связь	
4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [85-й Главный центр специальных служб (ГЦСС) Главного управления Генерального штаба Вооруженных Сил Российской Федерации (ГУ/ГРУ)]	Адрес: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation (Комсомольский проспект, 20, Москва, 119146, Российская Федерация)	85-й Главный центр специальных служб (ГЦСС) в составе Главного управления Генерального штаба Вооруженных Сил Российской Федерации (ГУ/ГРУ) (известен также как «в/ч 26165», «APT28», «Необычный Медведь», «Sofacy Group», «Pawn Storm» и «Strontium») участвует в кибератаках со значительными последствиями, представляющими внешнюю угрозу Союзу или его государствам-членам, а также в кибератаках со значительными последствиями против третьих стран. В частности, сотрудники военной разведки ГЦСС принимали участие в кибератаке на федеральный парламент Германии (Deutscher Bundestag) в апреле и мае 2015 года, а также попытке кибератаки в апреле 2018 года, направленной на взлом Wi-Fi-сети Организации по запрету химического оружия (ОЗХО) в Нидерландах. Кибератака на федеральный парламент Германии была направлена против его компьютерной системы, что блокировало его работу на несколько дней. Был украден большой объем данных, пострадали учетные записи электронной почты нескольких парламентариев, а также аккаунты бывшего канцлера Ангелы Меркель. После агрессивной войны России против Украины ГЦСС осуществила против Украины кибератаки (целевой фишинг и вредоносное ПО)	22.10.2020