|  |  |  |
| --- | --- | --- |
|  |  |  |

**СОГЛАШЕНИЕ**

о взаимодействии

Центрального банка Российской Федерации и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

по вопросу противодействия компьютерным атакам

г. \_\_\_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_\_ 202\_ г.

Центральный банк Российской Федерации в лице первого заместителя директора Департамента информационной безопасности \_\_\_\_\_\_\_\_\_\_\_, действующего на основании доверенности \_\_\_\_\_\_\_\_\_\_\_\_\_\_, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемый в дальнейшем «\_\_\_\_\_\_\_\_\_\_», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_, именуемые в дальнейшем «Стороны», заключили настоящее Соглашение (далее – «Соглашение») о нижеследующем.

**1. Общие положения**

1.1. Настоящее Соглашение заключено в целях организации взаимодействия Сторон по вопросу противодействия компьютерным атакам, направленного на предупреждение и выявление компьютерных атак, создание условий для их пресечения и повышение уровня информационной безопасности Сторон.

1.2. Настоящее Соглашение определяет формы и порядок взаимодействия Сторон по вопросу противодействия компьютерным атакам.

1.3. Взаимодействие Сторон осуществляется на безвозмездной основе.

1.4. Стороны обмениваются информацией в порядке, установленном законодательством Российской Федерации, а также настоящим Соглашением.

1.5. В настоящем Соглашении используются следующие термины:

 комплексный анализ инцидентов – исследование ряда выявленных компьютерных инцидентов с целью выявления закономерностей их возникновения и динамики распространения, классификации и типизации, разработки моделей развития, подготовки прогнозов угроз информационной безопасности и повышения эффективности стратегий предупреждения, обнаружения и установления причин компьютерных инцидентов, реагирования на них и ликвидации их последствий;

фишинг – информационная система, которая применяется для получения от третьих лиц (пользователей системы) конфиденциальных сведений за счет введения этих лиц в заблуждение относительно ее принадлежности (подлинности) вследствие сходства доменных имен или оформления либо содержания информации;

Информационный бюллетень – документ Банка России в формате PDF о компьютерном инциденте, форма которого приведена в приложении к настоящему Соглашению.

**2. Формы взаимодействия Сторон**

* 1. Взаимодействие Сторон осуществляется в следующих формах:

2.1.1. Сбор, обработка и обмен информацией о компьютерных инцидентах.

2.1.2. Обмен опытом работы по вопросам противодействия и предупреждения нарушений в сети Интернет, связанных с фишингом и распространением вредоносного программного обеспечения.

2.1.3. Проведение консультаций, семинаров, конференций по вопросам противодействия компьютерным атакам.

2.2. Настоящее Соглашение не препятствует Сторонам в определении и развитии иных взаимоприемлемых форм взаимодействия.

**3. Порядок взаимодействия Сторон по вопросам противодействия компьютерным атакам**

3.1. При обнаружении или получении информации о компьютерных инцидентах Стороны информируют друг друга. Информирование осуществляется в форме электронных сообщений. Информация о технологиях подготовки, направления и форматах электронных сообщений размещается на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (www.cbr.ru/fincert).

 3.2. Банк России размещает сведения о компьютерном инциденте в Информационном бюллетене.

3.3. Стороны осуществляют передачу информации о компьютерных инцидентах, используя следующие контактные данные:

**Банк России**:

электронный почтовый адрес: fincert@cbr.ru;

контактный номер: +7 (495) 772-70-90.

\_\_\_\_\_\_\_\_\_:

электронный почтовый адрес: \_\_\_\_\_\_\_;

контактный номер: \_\_\_\_\_\_\_\_\_\_\_.

3.4. При наличии технической возможности каждая из Сторон проводит комплексный анализ инцидента, в том числе информации о нем.

3.5. Для установления причин компьютерной атаки Банк России и \_\_\_\_\_\_\_\_\_ вправе обращаться к третьим лицам для сбора дополнительной информации, документов и материалов для всестороннего и независимого рассмотрения информации о компьютерном инциденте.

1. **Заключительные положения**
	1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу с момента его подписания Сторонами.
	2. Полученная в результате взаимодействия информация может быть использована Сторонами для повышения уровня информационной безопасности каждой из Сторон.

4.3. Стороны самостоятельно определяют меры, направленные на ликвидацию возникших последствий, а также меры, необходимые для предупреждения аналогичных компьютерных инцидентов.

4.4. Настоящее Соглашение может быть расторгнуто по инициативе одной из Сторон. В случае расторжения настоящего Соглашения по инициативе одной из Сторон она обязуется уведомить другую Сторону в письменной форме не позднее, чем за 30 (тридцать) календарных дней до даты его расторжения.

4.5. Внесение изменений в настоящее Соглашение осуществляется в письменной форме путем подписания Сторонами Дополнительного соглашения, которое является неотъемлемой частью настоящего Соглашения.

4.6. Соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному для каждой Стороны.

1. **Реквизиты Сторон**

|  |  |
| --- | --- |
| **Центральный банк Российской** **Федерации**  | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| Адрес (местонахождение): 107016, г. Москва, улица Неглинная, д. 12Адрес веб-сайта: http://cbr.ru/Телефон: +7 (495) 771-91-00Факс: +7 (495) 621-64-65 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_[[1]](#footnote-1)/М.П. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/М.П. |

Приложение









1. Просьба заранее уточнять по электронной почте info\_fincert@cbr.ru подписанта со стороны Банка России. [↑](#footnote-ref-1)