УТВЕРЖДЕНО
Постановление Правления
Национального банка
Республики Беларусь
20.11.2019 № 466

КОНЦЕПЦИЯ
обеспечения кибербезопасности в банковской сфере

РАЗДЕЛ I
ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Концепция представляет собой структурированный документ, разработанный на основе результатов анализа и видения Национальным банком сложившейся ситуации в области обеспечения кибербезопасности банков, небанковских кредитно-финансовых организаций, открытого акционерного общества ”Банк развития Республики Беларусь“ (далее, если не указано иное, – банки), содержащий перспективные направления решения имеющихся и предотвращения возможных проблем в сфере обеспечения кибербезопасности в банках и Национальном банке (далее, если не указано иное, – банковская сфера) в виде систематизированного изложения целей, задач, особенностей текущей ситуации и возможных способов достижения требуемого уровня обеспечения кибербезопасности в банковской сфере.

Концепция является основой для выработки практических мер по обеспечению кибербезопасности в банковской сфере. Положения Концепции будут использованы в правовых актах, регулирующих вопросы обеспечения кибербезопасности в банковской сфере.

Концепция разработана в соответствии с законодательством, в том числе нормативными правовыми актами Национального банка, Оперативно-аналитического центра при Президенте Республики Беларусь, связанными с обеспечением безопасности информационной инфраструктуры, а также с использованием международных стандартов и подходов в области обеспечения кибербезопасности.

1.Основные понятия и определения

Для целей настоящей Концепции используются следующие термины и их определения:

киберпространство – виртуальное пространство (среда), предоставляющее возможности для осуществления коммуникаций и

(или) реализации общественных отношений, образовавшихся в результате функционирования технологий, устройств и сетей, объединенных в коммуникационные системы, и обеспечивающее электронные коммуникации с использованием сети Интернет и (или) других сетей передачи данных;

киберугроза – имеющиеся и (или) возможные явления и факторы, реализуемые в киберпространстве, оказывающие негативное влияние на состояние кибербезопасности и угрожающие интересам банка, Национального банка или банковской сферы в целом;

киберриск – потенциальная возможность (вероятность) для банка, Национального банка понести потери (убытки), иные дополнительные затраты, не получить запланированные доходы вследствие противоправных действий лица либо группы лиц, совершенных посредством использования информационных технологий, в целях несанкционированного доступа к объектам информационной инфраструктуры банка, Национального банка и направленных на нарушение конфиденциальности, целостности, доступности, подлинности и сохранности защищаемой информации.

Термин ”защита информации“ используется в значении, определенном статьей 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З ”Об информации, информатизации и защите информации“.

Термины ”информационная инфраструктура“, ”кибератака“, ”кибербезопасность“, ”киберинцидент“ и ”киберустойчивость“ используются в значениях, определенных в постановлении Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 ”О Концепции информационной безопасности Республики Беларусь“.

2.Международный опыт обеспечения кибербезопасности в банковской сфере

2.1. В связи с процессами цифровизации всех отраслей человеческой деятельности в международной практике отмечается увеличение противоправной активности в киберпространстве, в частности, в отношении информационной инфраструктуры банков, основанной на использовании современных информационных систем и технологий в целях предоставления цифровых финансовых услуг.

2.2. Анализ международной практики показывает, что на мировом уровне можно выделить следующие наиболее характерные для банковской сферы виды киберугроз:

воздействие через аппаратные уязвимости – уязвимости, присутствующие в микропроцессорах разных производителей,

открывающие новые возможности для злоумышленников, неустранимые при помощи программных обновлений;

компьютерный шпионаж – направлен на долговременное присутствие в сетях объектов критической информационной инфраструктуры с целью саботажа и шпионажа за деятельностью финансовых организаций;

целенаправленные кибератаки – атаки, направленные на конкретные финансовые организации и позволяющие злоумышленникам проникать в сеть организаций и далее к изолированным финансовым системам для вывода денежных средств;

клиент-ориентированные кибератаки – направлены непосредственно на клиентов банков, а именно на хищение их личных денежных средств.

2.3. Международные организации и надзорные органы различных стран уделяют существенное внимание вопросам обеспечения кибербезопасности в банковской сфере. К настоящему времени в мировой практике разработан и применяется ряд документов, направленных на формирование системных подходов к обеспечению кибербезопасности, управлению киберриском и распространению на него режима надзора с учетом специфики этого риска, в том числе:

документ Комитета по платежам и рыночной инфраструктуре и Совета Международной организации комиссий по ценным бумагам ”Руководство по киберустойчивости для инфраструктур финансового рынка“, июнь 2016 г. (CPMI-IOSCO: Guidance on cyber-resilience for financial market infrastructures, June 2016);

документ Института финансовой стабильности ”Регуляторные подходы к усилению системы обеспечения кибербезопасности в банках“, август 2017 (Financial Stability Institute: FSI Insights on policy implementation № 2 ”Regulatory approaches to enhance banks’ cyber-security frameworks, August 2017);

документ Всемирного банка ”Кибербезопасность финансового сектора: дайджест для регуляторов“, октябрь 2017 (World Bank Group: Financial Sector’s Cybersecurity: A Regulatory Digest, October 2017);

документ Всемирного банка ”Кибербезопасность финансового сектора: правила и надзор“, 2018 (World Bank Group: Financial Sector’s Cybersecurity: Regulations and Supervision, 2018);

документ Совета по финансовой стабильности ”Обзор опубликованных правил в отношении кибербезопасности, руководство и надзорные практики“, октябрь 2017 (Financial Stability Board: Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, October 2017);

документ Базельского Комитета по банковскому надзору ”Кибер-устойчивость: обзор практик“, декабрь 2018 г. (Basel Committee on Banking Supervision: Cyber-resilience: Range of practices, December 2018).

Требования и (или) принципы обеспечения кибербезопасности в банковской сфере и подходы к управлению киберриском разработаны надзорными органами Австралийского союза, Канады, Великобритании, Европейского союза, Соединенных Штатов Америки, Швейцарии, Сингапура, Гонконга.

2.4. Настоящая Концепция разработана с учетом результатов анализа международного опыта обеспечения кибербезопасности в банковской сфере.

3.Цели и задачи Концепции

3.1. Основной целью настоящей Концепции является формирование единообразного понимания и подходов к обеспечению кибербезопасности для устойчивого функционирования банковской сферы.

3.2. Реализация данной цели позволит обеспечить защиту созданной в банках и Национальном банке информационной инфраструктуры от случайных (ошибочных) и целенаправленных противоправных действий, нарушения конфиденциальности, целостности, доступности, подлинности и сохранности защищаемой информации.

3.3. Задачами настоящей Концепции являются:

обеспечение эффективного взаимодействия между банками, Национальным банком по вопросам кибербезопасности;

обеспечение реализации прав граждан на защиту персональных данных, банковской тайны и защиту иной информации, обрабатываемой в информационных инфраструктурах банков, Национального банка;

методологическое обеспечение прогнозирования, своевременного выявления, реагирования и устранения киберугроз, расследования причин возникновения киберинцидентов и принятия соответствующих мер по их предотвращению;

формирование основы для определения каждым участником банковской сферы правовых, организационных и инженерно-технических мер, обеспечивающих выход на необходимый уровень обеспечения кибербезопасности и его поддержание.

4.Актуальность, значение и область применения Концепции

4.1. В современных условиях формирования открытого рынка цифровых финансовых услуг одним из важнейших вопросов

обеспечения безопасности деятельности в банковской сфере является обеспечение защиты ее информационной инфраструктуры, и определение в связи с этим основополагающих подходов к обеспечению кибербезопасности банковской сферы.

4.2. Поскольку банковская сфера занимает одно из ведущих мест в реализации национальных стратегий и планов создания цифровой экономики, координация деятельности ее субъектов в процессах обеспечения кибербезопасности является необходимым условием проведения государственной политики в этой области.

4.3. Актуальность настоящей Концепции обусловлена:

существенным увеличением в последние годы объемов предоставляемых банками цифровых финансовых услуг, и нарастанием присущего такой деятельности риска, в том числе ростом количества киберугроз, в первую очередь ставящих целью хищение денежных средств;

принятием новых нормативных правовых актов, установлением новых банковских практик, требующих использования единообразного отраслевого понятийного аппарата;

интеграцией банковских сфер Республики Беларусь и государств – членов Евразийского экономического союза, и необходимостью определения в связи с этим единообразных целей и задач обеспечения кибербезопасности в банковской сфере, повышения концептуальной и технологической совместимости систем обеспечения кибербезопасности в банковской сфере Республики Беларусь с соответствующими системами кибербезопасности государств – членов Евразийского экономического союза, а также других государств и организаций.

4.4. Разработка настоящей Концепции позволит обеспечить единообразное понимание банками ожиданий Национального банка в отношении формирования безопасного киберпространства в банковской сфере.

РАЗДЕЛ II
ТЕКУЩЕЕ СОСТОЯНИЕ

5.Правовое регулирование

5.1. В настоящее время в Республике Беларусь обеспечение кибербезопасности в банковской сфере основывается на взаимодействии различных иерархически зависимых видов регулирования.

5.2. Общее регулирование вопросов обеспечения кибербезопасности в банковской сфере осуществляется на основе законодательства, в том числе соответствующих нормативных правовых актов Оперативно-аналитического центра при Президенте Республики Беларусь, и международных практик, а именно:

Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1;

Закона Республики Беларусь от 10 ноября 2008 г. № 455-З ”Об информации, информатизации и защите информации“;

Закона Республики Беларусь от 21 июля 2008 г. № 418-З ”О регистре населения“;

приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 ”О некоторых вопросах технической и криптографической защиты информации“;

международных стандартов серии ISO/IEC 27000 (ISO/IEC 27001 – ”Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования“; ISO/IEC 27002 – ”Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности“; ISO/IEC 27005 – Руководство по менеджменту рисков информационной безопасности).

5.3. Отраслевое регулирование в банковской сфере осуществляется Национальным банком на основе соответствующих технических нормативных правовых актов, а именно:

СТБ 34.101.41-2013. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения;

СТБ 34.101.42-2013. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности;

СТБ 34.101.61-2013. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки рисков нарушения информационной безопасности;

СТБ 34.101.62-2013. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методические рекомендации по документации в области

обеспечения информационной безопасности в соответствии с требованиями СТБ 34.101.41;

СТБ 34.101.68-2013. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки соответствия информационной безопасности банков Республики Беларусь требованиям СТБ 34.101.41.

В соответствии с законодательством указанные стандарты не являются обязательными к исполнению банками, Национальным банком и носят рекомендательный характер.

5.4. В отношении вопросов обеспечения кибербезопасности, не предусмотренных в законодательстве, в том числе в нормативных правовых актах Оперативно-аналитического центра при Президенте Республики Беларусь, Национального банка, и международных стандартах, банки, Национальный банк определяют подходы и регулирование процессов обеспечения кибербезопасности в локальных правовых актах самостоятельно.

6.Отраслевое реагирование (деятельность FinCERTby)

6.1. В Национальном банке создан центр мониторинга и реагирования на компьютерные угрозы в банковской сфере Республики Беларусь (FinCERTby).

Данное подразделение, в целях реализации задач по снижению степени угроз от киберпреступлений в банковской сфере, противоправных посягательств на объекты информационной инфраструктуры банковской сферы и обеспечению безопасности оказания банковских услуг, осуществляет информационное взаимодействие с банками. В данной деятельности, в рамках соответствующих соглашений, участвуют правоохранительные органы Республики Беларусь, Центральный банк Российской Федерации, Национальный банк Республики Казахстан, ряд отечественных и зарубежных коммерческих организаций.

Указанное взаимодействие направлено на обмен информацией о потенциальных кибератаках, актуальных угрозах кибербезопасности и уязвимостях программного обеспечения, используемого в банковской сфере.

6.2. Основными задачами FinCERTby являются:

организация, координация и осуществление оперативного взаимодействия Национального банка с банками и иными организациями по вопросам противодействия кибератакам и

мошенничеству с использованием электронных платежных инструментов и средств платежа;

сбор и анализ данных о кибератаках, киберугрозах, уязвимостях информационной инфраструктуры банков, а также о мошенничестве с использованием электронных платежных инструментов и средств платежа, подготовка аналитических материалов;

установление требований к обеспечению защиты объектов информационной инфраструктуры банков, совершенствование методологии, направленной на противодействие киберугрозам и мошенничеству с использованием электронных платежных инструментов и средств платежа.

6.3. Анализ результатов работы FinCERTby показал, что в настоящее время наиболее популярными у злоумышленников методами осуществления кибератак являются:

рассылка вредоносного программного обеспечения – рассылка электронных писем с вредоносными вложениями или ссылками на их скачивание (в большинстве случаев имеют привычные для офисных работников форматы файлов), целями которых являются заражение конечных устройств пользователей, получение несанкционированного доступа к системам, хищение учетных данных пользователей, осуществление сетевых атак, рассылки спама, блокировки доступа к файловой системе или шифрованию данных на жёстком диске и вымогательства денежного вознаграждения за восстановление доступа к файлам;

взлом и подделка сайтов – осуществляется для введения в заблуждение клиентов банков, получения несанкционированного (в том числе неавторизованного) доступа к счетам и денежным средствам пользователей;

социальная инженерия – выманивание реквизитов банковских карточек посредством использования взломанных аккаунтов социальных сетей, либо совершения определенных действий в целях перевода денежных средств посредством мобильного или интернет-банкинга.

Зафиксированы факты компрометации инфраструктур поставщиков услуг и оборудования, клиентов банков и отправки писем с вредоносным программным обеспечением от имени и с легитимных почтовых адресов белорусских организаций.

В мошенничестве с использованием банковских платежных карточек по-прежнему остается актуальным мировой тренд – применение CNP-фрода (card not present, операции без присутствия карточки), также используемого и в банковской сфере Республики Беларусь. В настоящее время злоумышленниками активно

используются методы социальной инженерии для получения реквизитов банковских платежных карточек, а тандем CNP и социальной инженерии – механизм, который наиболее часто и эффективно используется мошенниками.

В абсолютном большинстве случаев основной причиной успешности тех или иных кибератак в банковской сфере Республики Беларусь стал человеческий фактор, что также соответствует мировой тенденции.

6.4. Анализ типов кибератак, проведенный FinCERTby, позволяет сделать выводы о необходимости принятия банками, Национальным банком для успешного предотвращения большинства кибератак в банковской сфере следующих мер:

поддержка и своевременное обновление инфраструктуры имеющихся средств защиты информации;

проведение обучения работников, ответственных за защиту информации и реагирование на киберугрозы;

проведение информирования работников, не задействованных в сфере организации кибербезопасности, а также клиентов банков (как правило, успешность кибератак во многом зависит от человеческого фактора (любопытства, невнимательности, доверчивости).

7. Применение средств криптографической защиты информации

7.1. На сегодняшний день в Республике Беларусь применяются сертифицированные средства криптографической защиты информации. Для взаимодействия систем обмена информацией между государственными органами, а также в банковской сфере используется Государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

Данная система предназначена для обеспечения возможности получения всеми заинтересованными организациями и физическими лицами информации об открытых ключах проверки электронной цифровой подписи и их владельцах в Республике Беларусь и представляет собой систему взаимосвязанных и аккредитованных в ней удостоверяющих центров и регистрационных центров.

7.2. В целях формирования единых подходов к взаимодействию государств – членов Евразийского экономического союза в сфере обмена информацией и обеспечения надлежащего уровня кибербезопасности в банковской сфере, а также в ходе такого взаимодействия необходимо применение средств криптографической защиты информации, обеспечивающих операционную надежность, защиту информации и управление киберриском.

8. Международное сотрудничество

8.1. Национальным банком поддерживаются тесные взаимоотношения с международным банковским сообществом. Используется опыт иностранных финансовых организаций.

В рамках оказания технической помощи в 2018 году Всемирным банком осуществлены оценка киберготовности Национального банка, анализ нормативной базы в области кибербезопасности, дана оценка текущему состоянию информационной инфраструктуры, практике управления кибербезопасностью и определены возможности для совершенствования состояния обеспечения кибербезопасности банковской сферы.

Национальному банку рекомендовано оперативно укрепить свою систему кибербезопасности для повышения уровня зрелости и эффективности управления рисками. Необходимо принять исчерпывающие меры в интересах своевременного обнаружения и реагирования на киберугрозы, которые могут негативно повлиять на миссию и стратегические цели Национального банка.

С целью поддержки данных инициатив в перспективе необходимо формализовать общую стратегию обеспечения кибербезопасности вместе с системой управления киберриском, предусматривающей в том числе установление эффективных и последовательных процедур управления им (идентификацию, измерение (оценку), мониторинг, контроль, ограничение (снижение) уровня киберриска), а также формирования соответствующей отчетности и механизмов информирования о киберриске.

8.2. Национальный банк принимает участие в реализации комплекса мероприятий по гармонизации подходов к формированию требований к обеспечению кибербезопасности и киберустойчивости в банковской сфере государств – членов Евразийского экономического союза.

В рамках совместной работы представителей центральных (национальных) банков государств – членов Евразийского экономического союза подписаны Протокол по направлениям формирования единых стандартов в области информационной безопасности, взаимного признания результатов внешнего аудита и применения средств криптографии при обмене электронной информацией и Соглашение о создании рабочей группы по вопросам обеспечения информационной безопасности финансового рынка и противодействия компьютерным атакам в банковской сфере.

РАЗДЕЛ III
ПЕРСПЕКТИВЫ И НАПРАВЛЕНИЯ РАЗВИТИЯ

9.Совершенствование правового обеспечения и регулирования

9.1. Принимая во внимание положения международных стандартов в области регулирования кибербезопасности, в ближайшей перспективе наиболее актуальным направлением является деятельность по совершенствованию нормативной правовой базы в данной области, доработка методологии обеспечения кибербезопасности в банковской сфере, в частности, разработка пакета стандартов информационной безопасности, включающего:

обеспечение кибербезопасности в банковской сфере, общие положения и терминология;

требования к системам управления кибербезопасностью;

требования по обеспечению кибербезопасности при использовании технологий виртуализации;

управление киберриском;

оценка соответствия кибербезопасности субъектов банковской сферы требованиям стандартов;

рекомендации по документационному обеспечению деятельности в области обеспечения кибербезопасности в соответствии с требованиями стандартов;

рекомендации по управлению киберугрозами и киберинцидентами;

требования по обеспечению кибербезопасности мобильных программных продуктов (мобильных приложений).

9.2. С целью придания стандартам информационной безопасности статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, потребуется внесение изменений в Банковский кодекс Республики Беларусь.

Реализация направлений методологического обеспечения деятельности по обеспечению кибербезопасности в банковской сфере позволит усовершенствовать действующее регулирование в данной области.

9.3. Разработка Национальным банком стандартов информационной безопасности позволит:

установить единые требования к обеспечению кибербезопасности в банковской сфере;

определить цели обеспечения кибербезопасности информационной инфраструктуры банков, Национального банка;

создать эффективную систему управления кибербезопасностью;

повысить эффективность мероприятий по обеспечению и поддержанию кибербезопасности в банковской сфере;

рассчитывать совокупность детализированных качественных и количественных показателей для оценки соответствия состояния кибербезопасности поставленным целям;

предотвращать и (или) снижать ущерб от киберинцидентов;

применять методики управления и инструментарий обеспечения кибербезопасности и оценки ее текущего состояния;

повысить эффективность мер по защите от реальных киберугроз;

повысить стабильность функционирования банков, Национального банка и на этой основе – стабильность функционирования банковской сферы в целом.

9.4. После придания стандартам информационной безопасности статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, на постоянной основе будет организован контроль за соблюдением стандартов. С этой целью необходима реализация мер по следующим направлениям:

определение требований по обеспечению кибербезопасности банками в соответствии с разработанной методологией обеспечения кибербезопасности в банковской сфере, указанной в подпункте 9.1 пункта 9 настоящей Концепции;

определение требований к применяемым мерам ответственности к банкам, Национальному банку за выявленные нарушения и осуществлению контроля исполнения этих мер. Контроль соблюдения стандартов по обеспечению кибербезопасности будет осуществляться как Национальным банком (дистанционный контроль, контроль в рамках проведения аудита, внеплановых проверок), так и банками (контроль со стороны подразделений, ответственных за кибербезопасность, а также контроль в рамках проведения внутреннего аудита);

определение подходов к управлению киберриском, предусматривающих, его идентификацию, измерение (оценку), мониторинг, контроль, ограничение (снижение), обеспечение непрерывности деятельности, формирование соответствующей отчетности и механизмов информирования о киберриске, проведение стресс-тестирования, испытаний на проникновение (пен-тестов) и иных мероприятий.

10.Перспективы развития FinCERTby

10.1. Перспективы развития FinCERTby предусматривают:

проведение обучения, повышения квалификации работников FinCERTby;

организацию и проведению совещаний, семинаров и рабочих встреч, направленных на повышение компетенций, а также отработку методов и способов оперативного взаимодействия работников FinCERTby и взаимодействующих организаций;

организацию мероприятий по повышению киберграмотности.

10.2. Создание автоматизированной системы обработки инцидентов, которая предусматривает реализацию функционала по автоматизации основных процессов FinCERTby и автоматизированное взаимодействие систем защиты информации банков с FinCERTby.

10.3. Совершенствование противодействия мошенничеству с использованием электронных платежных инструментов и средств платежа, которое предусматривает создание в банковской сфере системы ”Фид-Антифрод“, в которой будет организовано накопление и распространение информации о фактах несанкционированного перевода денежных средств.

10.4. Мероприятия по развитию взаимодействия предусматривают:

организацию взаимодействия с командами по реагированию на киберугрозы в банковской сфере других стран;

вступление в международные объединения команд по реагированию на киберугрозы (FIRST – Forum of Incident Response and Security Teams, Trusted Introducer, EAST Expert Group on All Terminal Fraud (EGAF);

дальнейшее развитие отношений с правоохранительными органами, выстраивание модели взаимодействия с ними на основе учета интересов каждой из сторон;

установление взаимоотношений с поставщиками платежных услуг, операторами связи и иными организациями.

11.Взаимодействие с банками, обучение

11.1. Основной целью взаимодействия Национального банка с банками в рамках обеспечения кибербезопасности является организация обеспечения защиты созданной в банках информационной инфраструктуры для безопасного и надежного функционирования банковской сферы.

11.2. Основными задачами для достижения указанной цели являются:

выработка общих единых подходов к обеспечению кибербезопасности для надежного, безопасного и устойчивого функционирования банковской сферы;

осуществление информационного взаимодействия между

Национальным банком и банками в области кибербезопасности;

разработка, поддержание в актуальном состоянии и развитие Национальным банком методологической базы банковской сферы в области кибербезопасности, отвечающей интересам всех субъектов банковской сферы;

организация взаимодействия с подразделениями банков, ответственными за реагирование на киберугрозы;

организация и проведение Национальным банком совместно с банками учебных семинаров, рабочих встреч, иных мероприятий по тематике обеспечения кибербезопасности в банковской сфере.

12.Перспективы развития международного сотрудничества

12.1. Основными целями международного сотрудничества Национального банка в рамках обеспечения кибербезопасности банковской сферы является организация и поддержание между ее субъектами своевременного обмена информацией, опытом и лучшими практиками в интересах выявления (идентификации), предупреждения и ограничения (снижения) киберриска, в том числе нейтрализации киберугроз и кибератак.

12.2. Основными средствами для достижения целей международного сотрудничества в рамках обеспечения кибербезопасности в банковской сфере являются участие, выработка, поддержка и продвижение Национальным банком соответствующих инициатив, отвечающих интересам участников международного финансового и информационного взаимодействия.

12.3. В рамках развития международного сотрудничества Национальным банком будет продолжена целенаправленная работа по следующим направлениям:

дальнейшее развитие взаимодействия (заключение, внесение изменений в меморандумы о взаимопонимании) с национальными и центральными банками других стран, Всемирным банком по вопросам обеспечения кибербезопасности в банковской сфере;

организация взаимодействия с международными платежными системами (Visa, MasterCard, SWIFT);

участие в работе по гармонизации законодательства в области кибербезопасности государств – членов Евразийского экономического союза;

организация взаимодействия с иными международными организациями в целях обмена опытом и обучения.

13.Ожидаемый эффект от реализации положений Концепции

13.1. Ожидаемыми результатами от использования банками, Национальным банком в своей деятельности положений настоящей Концепции являются детализация, конкретизация и оптимизация подходов в рамках развития систем обеспечения кибербезопасности субъектов и, следовательно, банковской сферы в целом.

13.2. Концепция будет способствовать:

формированию и применению в банковской сфере единообразного понятийного аппарата в целях обеспечения кибербезопасности;

совершенствованию стандартов информационной безопасности и управления киберриском;

формированию системы барьеров для реализации киберугроз в банковской сфере;

стимулированию устойчивости систем обеспечения кибербезопасности банков, Национального банка к киберриску, то есть их способности противостоять актуальным и вновь возникающим киберугрозам и (или) киберинцидентам;

совершенствованию координации деятельности и управляемости подразделений, ответственных за обеспечение кибербезопасности, защиту информации субъектов банковской сферы и реагирование на киберугрозы;

повышению устойчивости и совершенствованию функционирования механизмов реагирования на киберугрозы в банковской сфере, а также случаи реализации киберриска (киберинциденты);

обеспечению устойчивого развития международных связей банков, Национального банка с субъектами банковской сферы других государств.