01.11.2019 № 23-13/83

Банки, небанковские кредитно-финансовые организации (по списку)

ОАО ”Банк развития Республики Беларусь“

Ассоциация белорусских банков

О совершенствовании
управления киберриском

Развитие направлений банковской деятельности в настоящее время непосредственным образом связано с наращиванием информационной инфраструктуры[1] банков, открытого акционерного общества ”Банк развития Республики Беларусь“ и небанковских кредитно-финансовых организаций (далее – банки).

Национальный банк поддерживает и стимулирует обновление имеющихся и использование банками новых технических средств, систем и технологий работы с информацией с учетом всесторонней оценки рисков, присущих такой деятельности. В международной банковской практике одним из существенных видов рисков, присущих указанной деятельности, признается киберриск.

К настоящему времени международными финансовыми организациями и надзорными органами различных стран разработан и применяется ряд документов, направленных на формирование системных подходов к обеспечению кибербезопасности, управлению киберриском путем его включения в общую систему управления рисками

[1] Информационная инфраструктура – совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации.

банка и распространения на него режима надзора с учетом специфики этого риска[2].

Национальным банком уделяется серьезное внимание вопросам управления киберриском и обеспечения кибербезопасности банков. В Национальном банке создан центр мониторинга и реагирования на компьютерные угрозы в банковской сфере Республики Беларусь (FinCERTby), одними из основных задач которого являются организация, координация и осуществление оперативного взаимодействия Национального банка с банками и иными организациями по вопросам противодействия кибератакам, сбор и анализ данных о них, а также о киберугрозах и уязвимостях информационной инфраструктуры банков.

Национальным банком в целях совершенствования подходов банков к управлению рисками киберриск включен в перечень основных видов операционного риска, предусмотренных Инструкцией об организации системы управления рисками в банках, открытом акционерном обществе ”Банк развития Республики Беларусь“, небанковских кредитно-финансовых организациях, банковских группах и банковских холдингах, утвержденной постановлением Правления Национального банка Республики Беларусь от 29 октября 2012 г. № 550.

Исходя из требований указанной Инструкции в отношении управления киберриском применяются все требования, предъявляемые к организации управления основными видами рисков, включая ответственность органов управления банка, определение толерантности к риску, разработку локальных правовых актов, регламентирующих управление риском, проведение стресс-тестирования, составление и

---

[2] Следующие документы:

Комитета по платежам и рыночной инфраструктуре и Совета Международной организации комиссий по ценным бумагам ”Руководство по киберустойчивости для инфраструктур финансового рынка“, июнь 2016 г. (https://www.bis.org/cpmi/publ/d146.pdf);

Института финансовой стабильности при Банке международных расчетов ”Регуляторные подходы к усилению системы обеспечения кибербезопасности в банках“, август 2017 г. (https://www.bis.org/fsi/publ/insights2.pdf);

Совета по финансовой стабильности ”Обзор опубликованных правил в отношении кибербезопасности, руководство и надзорные практики“, октябрь 2017 г. (https://www.fsb.org/wp-content/uploads/P131017-2.pdf);

Всемирного банка ”Кибербезопасность финансового сектора: правила и надзор“, 2018 г. (http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf);

Базельского Комитета по банковскому надзору ”Киберустойчивость: обзор практик“, декабрь 2018 г. (https://www.bis.org/bcbs/publ/d454.pdf);

Всемирного банка ”Кибербезопасность финансового сектора: дайджест для регуляторов“, май 2019 г. (http://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf).

представление управленческой отчетности и иные элементы системы управления рисками.

С учетом этого, а также применяемых в международной практике подходов к управлению киберриском, банкам следует обеспечить решение следующих задач:

интеграция подходов к управлению киберриском в общую систему корпоративного управления, управления рисками банка и внутреннего контроля;

разработка локальных правовых актов по управлению киберриском;

создание и использование эффективных процедур управления киберриском;

периодическое проведение проверки (оценки) эффективности управления киберриском;

раскрытие соответствующей информации об управлении киберриском в банке.

Интеграция подходов к управлению киберриском в общую систему корпоративного управления проводится с учетом размера и организационно-функциональной структуры банка, масштабов и особенностей осуществляемых банком операций и видов деятельности, а также степени подверженности информационной инфраструктуры банка киберриску.

В банках, отнесенных к числу системно значимых банков группы значимости I, целесообразно создание профильного подразделения (например, службы по обеспечению кибербезопасности) и (или) назначение должностного лица, ответственного за обеспечение кибербезопасности[3]. В остальных банках функциями по управлению киберриском могут наделяться профильное подразделение по управлению рисками и (или) профильное подразделение по обеспечению безопасности банка с сохранением действующей структуры подотчетности.

В случае создания службы по обеспечению кибербезопасности необходимо, чтобы такая служба являлась независимой от профильных подразделений банка, ответственных за развитие и поддержание информационных технологий и информационных систем банка (ИТ-служб). Кроме того, для обеспечения возможности получения целостного представления о риск-профиле банка целесообразно предусмотреть эффективное взаимодействие и распределение обязанностей по управлению киберриском между службой по обеспечению

[3] Обеспечение кибербезопасности может осуществляться как отдельная функция в составе подразделения, ответственного за обеспечение информационной безопасности банка, с назначением должностного лица, ответственного за обеспечение информационной безопасности, в том числе кибербезопасности. Для целей настоящего письма используются термины ”кибербезопасность“ и ”лицо, ответственное за обеспечение кибербезопасности“.

кибербезопасности, профильным подразделением по управлению рисками и профильным подразделением по обеспечению безопасности банка.

В случае назначения должностного лица, ответственного за обеспечение кибербезопасности, необходимо, чтобы такое лицо обладало специфическими профессиональными знаниями, необходимым опытом и техническими навыками в области управления киберриском. К основным задачам деятельности указанного должностного лица относятся:

организация работы по обеспечению конфиденциальности, целостности, доступности, подлинности и сохранности информационной инфраструктуры банка и содержащейся в ней информации от внешних и внутренних угроз;

согласование внедрения новых и совершенствования предоставляемых банковских продуктов, осуществляемых видов деятельности и процессов, исходя из анализа их подверженности киберриску, влияния на защищенность информационной инфраструктуры банка, а также способности банка обеспечить защиту от воздействия киберриска в результате такого внедрения и совершенствования;

представление информации о кибербезопасности банка и прогрессе в достижении ее целей.

Должностное лицо, ответственное за обеспечение кибербезопасности, подотчетно совету директоров (наблюдательному совету), или исполнительному органу, или должностному лицу, ответственному за управление рисками.

Служба по обеспечению кибербезопасности подотчетна должностному лицу, ответственному за обеспечение кибербезопасности, а в случае, если оно не назначено, – должностному лицу, ответственному за управление рисками.

Формирование эффективных подходов к управлению киберриском предусматривает осуществление соответствующих инвестиций в информационную инфраструктуру банка как на первых этапах внедрения данных подходов, так и в процессе их применения, что предполагает своевременное обновление и замену устаревших технических средств и технологий создания, преобразования, передачи, использования и хранения информации.

К управлению киберриском целесообразно привлечь достаточное количество сотрудников, обладающих соответствующей квалификацией, в том числе в сфере управления рисками, связанными с аутсорсингом. Данных сотрудников, в том числе должностное лицо, ответственное за обеспечение кибербезопасности, наделяют соответствующими полномочиями, включающими право выносить суждение о необходимости ограничения принятия киберриска или отказа от него в процессе принятия руководством банка управленческих решений.

В целях обеспечения совета директоров (наблюдательного совета) банка знаниями в сфере организации управления киберриском и поддержания их в актуальном состоянии целесообразно предусмотреть соответствующие программы обучения, включающие взаимодействие членов совета директоров (наблюдательного совета) с внутренними и (или) внешними экспертами в области управления киберриском.

Кроме того, целесообразно организовать работу по получению руководителями и (или) сотрудниками банка, непосредственной обязанностью которых является управление киберриском, обеспечение кибербезопасности банка, сертификатов международного образца в области управления киберриском и (или) обеспечения кибербезопасности (например, сертификаты Certified Information Systems Security Professional, Certified in Risk and Information Systems Control, Certified Ethical Hacker).

Формирование подходов к управлению киберриском следует осуществлять в неразрывной связи с процессами управления другими рисками на всех уровнях организационной структуры банка. Эффективное взаимодействие специалистов, ответственных за управление рисками банка, обеспечение кибербезопасности, а также лиц, ответственных за приобретение услуг третьей стороны (например, в случае аутсорсинга), позволяет предотвратить несогласованность и дублирование в управлении рисками.

При интеграции подходов к управлению киберриском в общую систему управления рисками предусматривается:

интеграция информационной системы, обеспечивающей управление киберриском, с другими информационными системами банка, позволяющими получать первичную информацию о сбоях, ошибках, отклонениях в деятельности (в том числе продуктах, процессах и системах) банка, возникновении киберинцидентов[4], реализации риска информационных технологий (ИТ-риска), а также иных рисков банка;

интегрированный подход к управлению рисками новых банковских продуктов, видов деятельности, процессов и систем, учитывающий оценку их подверженности воздействию киберриска.

В стратегическом плане развития банка целесообразно отражать информацию о текущем состоянии информационной инфраструктуры банка и ее планируемых изменениях в соответствии с подходами к совершенствованию информационной инфраструктуры банка и

[4] Под киберинцидентом понимается событие, связанное с реализацией киберриска, повлекшее или способное повлечь у банка потери и (или) дополнительные затраты по осуществляемой деятельности, оказывающие негативное влияние на финансовый результат деятельности банка (прямые потери), качество предоставляемых услуг и внутренних процессов, репутацию банка (косвенные потери).

обеспечению ее кибербезопасности, определенными стратегией развития банка.

В стратегии управления рисками банка в отношении управления киберриском следует включать информацию:

о критически важных объектах информационной инфраструктуры, кибербезопасность которых должна быть обеспечена, с учетом приоритетности такой деятельности в отношении каждого из этих объектов;

о характерных для банка киберугрозах с учетом приоритетности их возможной реализации и последствий;

о текущем состоянии кибербезопасности в банке и возможностях противодействия киберугрозам;

о мероприятиях по преодолению имеющихся недостатков и направлениях совершенствования управления киберриском с учетом подходов к совершенствованию информационной инфраструктуры банка и обеспечению ее кибербезопасности, определенных стратегией развития банка.

Стратегия управления киберриском может разрабатываться как отдельный локальный правовой акт банка с учетом определенных советом директоров (наблюдательным советом) стратегических целей развития и стратегии управления рисками банка. Такой подход целесообразно использовать в банках, отнесенных к числу системно значимых банков группы значимости I.

Пересмотр локальных правовых актов по управлению киберриском банка осуществляется на регулярной основе (как правило, не реже 1 раза в год) в зависимости от масштабов и особенностей осуществляемых банком операций, видов деятельности, процессов, изменения внешних факторов, результатов, полученных в процессе управления киберриском и анализа устойчивости банка к данному риску (далее – киберустойчивость), а также результатов оценки эффективности системы управления рисками, в том числе киберриском.

В соответствии с Инструкцией об организации системы управления рисками в банках, открытом акционерном обществе ”Банк развития Республики Беларусь“, небанковских кредитно-финансовых организациях, банковских группах и банковских холдингах в рамках процесса управления киберриском банк должен осуществлять **выявление (идентификацию), измерение (оценку), внутренний мониторинг, ограничение (снижение) уровня, внутренний контроль** киберриска, а также проводить **стресс-тестирование киберустойчивости** и обеспечивать **непрерывность деятельности** банка в случае реализации данного риска.

При ***выявлении (идентификации)*** киберриска определяются основные киберугрозы, которые целесообразно интегрировать в общую

классификацию источников операционного риска. В частности, киберугрозы могут быть выявлены в таких источниках операционного риска, как внутреннее, внешнее мошенничество, клиенты, продукты и деловая практика, нарушение непрерывности функционирования и сбои (отказы) систем, осуществление деятельности и управление процессами.

Анализ международной практики показывает, что на мировом уровне можно выделить следующие наиболее характерные для банков виды киберугроз:

воздействие через аппаратные уязвимости – уязвимости, присутствующие в микропроцессорах различных производителей, открывающие новые возможности для злоумышленников, неустранимые при помощи программных обновлений;

компьютерный шпионаж – деятельность, направленная на долговременное присутствие в сетях объектов критической информационной инфраструктуры с целью саботажа и шпионажа за деятельностью банка;

целенаправленные кибератаки – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи банка, используемые для организации взаимодействия таких объектов, в целях проникновения в сеть конкретных банков и изолированные финансовые системы для вывода денежных средств;

клиентоориентированные кибератаки – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи банка, используемые для организации взаимодействия таких объектов, в целях хищения денежных средств конкретных клиентов или групп клиентов банка.

Целенаправленные и (или) клиентоориентированные кибератаки могут быть использованы в целях дискредитации банка перед его клиентами (контрагентами) и снижения их уверенности в устойчивости банка и сохранности денежных средств в нем.

Анализ результатов работы FinCERTby показывает, что в настоящее время основными способами реализации киберугроз 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 жестком 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;

компрометация инфраструктур поставщиков услуг и оборудования (аутсорсинга), клиентов банков и отправка писем с вредоносным программным обеспечением от имени белорусских организаций и предприятий с их действующих почтовых адресов;

применение CNP-фрода (card not present, операции без присутствия карточки), в том числе в совокупности с методами социальной инженерии, направленной на получение реквизитов банковских платежных карт, иными методами, используемыми в целях мошенничества с банковскими платежными картами.

При выявлении (идентификации) киберриска устанавливаются основные возможные каналы реализации киберугроз (заражения): по электронной почте, через носители информации, распространение по локальной сети и иные каналы.

На этапе выявления (идентификации) киберриска также предусматривается определение и классификация ключевых направлений деятельности (бизнес-линий) и операций, критически важных объектов информационной инфраструктуры банка и поставщиков услуг (аутсорсинга).

Измерение (оценка) киберриска предусматривает оценку:

склонности банка к этому риску (риск-аппетита) с учетом особенностей деятельности и осуществляемых банком операций, а также ориентиров развития бизнеса, предусмотренных стратегией развития банка;

подверженности киберриску ключевых направлений деятельности (бизнес-линий) и операций, критически важных объектов информационной инфраструктуры и подразделений банка;

зависимости от поставщиков услуг (аутсорсинга) и их киберустойчивости;

квалификации и знаний сотрудников банка по вопросам управления киберриском, в первую очередь сотрудников ИТ-служб и сотрудников, ответственных за обеспечение кибербезопасности.

В этих целях может проводиться анкетирование сотрудников банка, предусматривающее оценку слабых мест и недостатков, способных привести к возникновению киберриска, установленных мер его контроля и ограничения (снижения), а также возможных последствий воздействия киберриска.

По результатам измерения (оценки) могут составляться карты подверженности банка киберриску в различных разрезах: по подразделениям, ключевым направлениям деятельности (бизнес-линиям), бизнес-процессам, отдельным операциям банка, а также в других разрезах в зависимости от установленных целей проведения оценки.

Измерение (оценка) киберриска также предусматривает анализ информации о вероятности возникновения киберинцидентов и потерь от них. В частности, исходя из ретроспективного анализа размеров ранее понесенных банком потерь от киберинцидентов определяется их возможный размер в будущем. При этом в качестве исходных данных используется информация о киберинцидентах, накопленная во внутренней базе данных банка об операционных инцидентах.

Внутренний мониторинг киберриска осуществляется путем регулярного ведения и анализа сведений о киберинцидентах, включаемых во внутреннюю базу данных банка об операционных инцидентах. Для этого целесообразно организовать сбор указанных сведений таким образом, чтобы установленный в банке минимальный порог прямых и (или) потенциальных потерь от операционных инцидентов для включения информации в базу данных позволял отражать в ней сведения о киберинцидентах, признаваемых существенными по основаниям, не связанным с понесением банком прямых потерь, например, вследствие существенного влияния на его репутацию или оттока клиентов. При этом киберинцидентам, включенным в базу данных, целесообразно присвоить соответствующий признак, позволяющий выделять сведения о киберинцидентах из общей совокупности данных об операционных инцидентах. Кроме того, допускается ведение отдельной базы данных о киберинцидентах, обеспечивающее возможность интеграции сведений о них в базу данных об операционных инцидентах банка.

В целях осуществления классификации киберинцидентов для ведения базы данных целесообразно руководствоваться Регламентом передачи данных в FinCERTby, направленным банкам письмом Национального банка от 9 октября 2018 г. № 84-18/13 (с учетом изменений, направленных письмом Национального банка от 30 ноября 2018 г. № 84-18/28).

Банку также целесообразно организовать получение сведений о киберинцидентах из внешних источников информации. В дополнение к обмену данными о возникновении киберинцидентов с FinCERTby целесообразно организовать такой обмен с другими банками и

заинтересованными сторонами, а также анализировать аналогичную получаемую от них информацию, что позволяет оперативно предусмотреть меры защиты от воздействия киберриска. К тому же подобные сведения могут использоваться при проведении стресс-тестирования киберриска и способствуют выявлению недостатков в системе внутреннего контроля банка.

В соответствии с пунктом 12[3] Инструкции о порядке составления и представления банками, открытым акционерным обществом ”Банк развития Республики Беларусь“ и небанковскими кредитно-финансовыми организациями пруденциальной отчетности в Национальный банк Республики Беларусь, утвержденной постановлением Правления Национального банка Республики Беларусь от 31 октября 2006 г. № 172, банк обязан в течение пяти рабочих дней с момента обнаружения информировать Национальный банк о возникновении угроз информационной безопасности банка, признаваемых банком существенными. В рамках такого информирования целесообразно направление подробных сведений о возникновении угроз кибербезопасности банка, признаваемых банком существенными.

Банку также следует установить *ключевые индикаторы киберриска*, связанные с его уровнем, показывающие потенциальные источники данного риска и позволяющие осуществлять их анализ на регулярной основе.

Ключевые индикаторы целесообразно установить для всех направлений деятельности (бизнес-линий) и объектов информационной инфраструктуры, подверженных воздействию киберриска, в первую очередь объектов, необходимых для осуществления операций, приостановка или отказ от которых окажет значительное негативное влияние на финансовое состояние, эффективность и (или) репутацию банка.

С учетом постоянного развития технических средств, систем и технологий работы с информацией в виртуальном пространстве помимо ключевых индикаторов, установленных исходя из анализа последствий реализации киберриска в банке и (или) других банках, целесообразно определение индикаторов, позволяющих отражать увеличение подверженности банка киберриску с учетом такого развития.

В состав ключевых индикаторов киберриска включаются индикаторы, позволяющие отслеживать изменения кибербезопасности банка и присущего ему киберриска, в том числе актуальность и периодичность обновления объектов информационной инфраструктуры, а также соответствие подходов к управлению данным риском на практике принятой в банке политике управления киберриском.

Ключевыми индикаторами киберриска могут служить:

количество заблокированных попыток сканирования портов для взлома сети;

количество обнаруженных фишинговых интернет-сайтов банка;

количество заблокированных фишинговых сообщений, поступивших в банк;

количество попыток социальной инженерии;

количество возникших в банке киберинцидентов;

доля отраженных кибератак в их общем количестве;

количество киберинцидентов в конкретной предметной области, включенных во внешние базы данных об операционных инцидентах за последние месяцы;

количество выявленных за последние месяцы киберугроз, характерных для программного обеспечения конкретного контрагента, поставщика услуг (аутсорсинга);

сумма потерь от киберинцидентов;

увеличение негативных оценок подверженности кибер риску по результатам измерения (оценки) кибер риска;

доля сотрудников, прошедших обучение по вопросам обеспечения кибербезопасности;

доля сотрудников, не соблюдающих установленные требования к управлению кибер риском.

Ключевые индикаторы кибер риска должны быть взаимоувязаны с инструментами реагирования на изменение как одного индикатора риска, так и их совокупности. Целесообразно установить такие инструменты реагирования, которые бы позволяли представлять информацию соответствующим органам управления банка и иным заинтересованным в зависимости от существенности киберинцидентов, а также срочности реагирования или оперативности принятия решений и мер ограничения (снижения) кибер риска, в том числе в целях исключения распространения киберугрозы на всю банковскую систему (эффект заражения).

Порядок реагирования на изменение индикаторов кибер риска и случаи оповещения Национального банка, банков и других заинтересованных о нарастании киберугроз определяются в локальных правовых актах банка.

Банку также следует проводить периодический пересмотр ключевых индикаторов кибер риска, в том числе установленных лимитов и (или) пороговых значений индикаторов, и дополнять их перечень новыми индикаторами, особенно в случае начала осуществления новых видов деятельности, внедрения новых объектов информационной инфраструктуры или иного существенного изменения, влияющего на риск-профиль банка.

Для ***ограничения (снижения) уровня киберриска*** принимаются меры, направленные на снижение вероятности возникновения киберинцидентов или их последствий в случае реализации киберугроз.

В этих целях следует предусмотреть мероприятия по повышению уровня знаний о киберриске и их грамотному использованию (киберграмотности), обучению сотрудников по вопросам обеспечения кибербезопасности, доведению принципов и подходов банка к управлению киберриском сотрудникам всех подразделений банка, членам совета директоров (наблюдательного совета), исполнительного органа, а также клиентам (контрагентам) и поставщикам банка, в том числе поставщикам услуг аутсорсинга.

Кроме того, ограничению (снижению) киберриска способствуют:

создание информационной инфраструктуры банка, позволяющей надлежащим образом обеспечивать его кибербезопасность;

определение порядка управления проектами, связанными с разработкой, приобретением, внедрением новых и (или) обновлением имеющихся объектов информационной инфраструктуры банка;

установление процедур обеспечения конфиденциальности информации банка и его клиентов, в том числе заключение с сотрудниками соглашений о неразглашении такой информации;

установление порядка управления доступом и распределения прав по изменению объектов информационной инфраструктуры и обрабатываемой в ней информации банка;

надлежащая идентификация клиентов (контрагентов) банка;

установление регламентов проведения операций банка, включающих возможность приостановки или отказа от их осуществления в связи с обнаружением или реализацией киберугроз, а также мероприятия по восстановлению их проведения;

стандартизация бизнес-процессов;

разработка подходов к ограничению (снижению) киберриска в системах дистанционного банковского обслуживания, в том числе интернет-банкинге;

разработка и реализация планов действий на случай непредвиденных обстоятельств;

создание необходимых дублирующих (резервных) объектов информационной инфраструктуры, в том числе удаленных;

создание автономных систем электропитания;

страхование риска;

передача риска или его части третьей стороне (аутсорсинг в сфере финансовых услуг, аутсорсинг информационных технологий, услуг удаленного хранения данных, иной деятельности банка, осуществляемой

для собственных нужд и (или) необходимой для обеспечения осуществления банковских операций).

Использование страхования в целях ограничения (снижения) киберриска рассматривается в качестве инструмента, дополняющего, но не исключающего необходимость надлежащего управления киберриском.

Поскольку аутсорсинг также предусматривает возможность реализации киберугроз, для ограничения (снижения) киберриска банку целесообразно установить подходы к управлению аутсорсингом, предусматривающие включение в договоры аутсорсинга требований к поставщику услуг об управлении киберриском, в том числе требований:

о создании защищенных каналов связи с поставщиками услуг и обеспечении конфиденциальности передаваемой по ним информации банка и его клиентов (контрагентов);

об обеспечении непрерывности деятельности поставщика услуг и доступности переданных в аутсорсинг операций;

о предоставлении банку доступа к информации о деятельности поставщика услуг, необходимой для его проверки (оценки) по вопросам управления киберриском;

о периодическом проведении поставщиком услуг независимой проверки (оценки) по вопросам управления киберриском;

об ограничении использования поставщиком услуг в отношении переданных ему операций банка возможностей применения субаутсорсинга, то есть последующей передачи операций банка в аутсорсинг и (или) привлечения других поставщиков услуг для их обслуживания, либо установлении к субаутсорсингу требований к управлению киберриском, аналогичных перечисленным.

Банкам необходимо установить подходы к управлению киберриском, который может реализоваться посредством использования банком услуг субъектов финансового рынка (платежных и расчетных систем, торговых площадок (бирж), депозитариев и прочих субъектов), поставщиков электрической энергии, линий связи, а также услуг аренды аппаратного и программного обеспечения.

Составной частью управления киберриском является его всесторонний ***внутренний контроль***. При этом меры контроля устанавливаются с учетом размера и организационно-функциональной структуры банка, масштабов и особенностей осуществляемых банком операций и видов деятельности, степени подверженности информационной инфраструктуры банка киберриску, а также результатов устранения ранее выявленных нарушений.

В рамках управления киберриском и обеспечения кибербезопасности следует проводить на регулярной основе, как правило, ежегодно, ***стресс-тестирование киберустойчивости*** объектов информационной

инфраструктуры банка и защищенности обрабатываемой в ней информации. В этих целях разрабатываются сценарии стресс-тестов, которые могут предусматривать симулирование:

кибератак на банк и (или) его основных контрагентов, в том числе других банков (эффект заражения);

сбоев в работе поставщиков услуг (аутсорсинга) в результате реализации киберугроз;

сбоев в предоставлении услуг субъектами финансового рынка в результате реализации киберугроз;

реализации иных киберугроз банка.

Стресс-тестирование киберустойчивости позволяет оценить эффективность принятых мер контроля и разработанной системы ключевых индикаторов киберриска, а также скорректировать или дополнить их новыми мерами контроля и индикаторами, позволяющими преодолеть выявленные в результате стресс-тестирования недостатки обеспечения кибербезопасности объектов информационной инфраструктуры банка и обрабатываемой в ней информации. Кроме того, стресс-тестирование позволяет оценить эффективность инструментов реагирования на киберинциденты и мер по устранению их последствий, в том числе обеспечения непрерывности деятельности банка и ее восстановления.

В целях обеспечения ***непрерывности деятельности банка*** в случае возникновения неблагоприятных (кризисных) ситуаций следует разработать *планы действий на случай непредвиденных обстоятельств* для ключевых направлений деятельности (бизнес-линий) и операций, критически важных объектов информационной инфраструктуры, в том числе поддерживаемых внешним поставщиком услуг (аутсорсинга), подразделений банка, а также услуг, оказываемых субъектами финансового рынка.

В процессе разработки таких планов целесообразно:

определять порядок реагирования на киберинциденты;

определять обязанности и полномочия органов управления, подразделений и должностных лиц банка по выполнению предусмотренных планами мер;

определять возможности и сроки передачи услуг в аутсорсинге другому поставщику;

согласовывать планы с заинтересованными сторонами, деятельность которых будет затронута в случае осуществления данных планов, в том числе поставщиками услуг аутсорсинга и субъектами финансового рынка;

утверждать планы органами управления банка;

проверять работоспособность планов (тестирование);

регулярно пересматривать и создавать новые планы, в том числе в случае изменения объемов операций банка, выпуска новых банковских продуктов, осуществления новых видов деятельности, появления новых объектов информационной инфраструктуры банка.

В международной практике приемлемым считается восстановление безопасного функционирования банка в течение двух часов с момента его прекращения.

Банком организуется периодическое проведение проверки (оценки) эффективности управления киберриском. В частности, внутреннему аудиту банка следует проводить периодические проверки полноты применения и эффективности установленных процедур управления киберриском и обеспечения кибербезопасности. В дополнение к этому целесообразно проводить независимую оценку такого управления с привлечением внешнего аудита, в том числе организовывать периодический аудит соответствия подходов к управлению киберриском и обеспечению кибербезопасности используемым в мировой практике стандартам в указанной сфере (например, COBIT, ISO/IEC, NIST, US (FFIEC), UK (CBEST). Результаты проведенных проверок (оценок) учитываются при разработке и совершенствовании подходов к управлению киберриском.

Результаты, получаемые в процессе управления киберриском, являются основой регулярного информирования совета директоров (наблюдательного совета), исполнительного органа банка.

При формировании *управленческой отчетности об управлении киберриском* целесообразно отражать сведения в динамике на установленные банком даты для выявления негативных тенденций, а также включать в нее сведения:

о киберугрозах банка, возникновение которых вероятно;

о новых тенденциях и киберугрозах в области обеспечения кибербезопасности;

о возникших киберинцидентах и их последствиях, в том числе крупных;

о крупных кибератаках на банк, результатах их предотвращения и последствиях;

о результатах стресс-тестирования киберустойчивости;

о проверке работоспособности (тестировании) планов действий на случай непредвиденных обстоятельств.

В случае если банк является головной организацией банковской группы (банковского холдинга), органам управления такого банка целесообразно предусмотреть формирование в рамках банковской группы или банковского холдинга единообразных подходов к управлению

киберриском, позволяющих получать информацию о реальном уровне данного риска как по банковской группе или банковскому холдингу в целом, так и по отдельным ее (его) участникам.

Регулярное раскрытие банком информации о подходах к управлению киберриском, результатах предотвращения кибератак и их последствий повышает доверие к банку со стороны пользователей этой информации, а также способствует усилению рыночной дисциплины и развитию лучшей практики управления киберриском в банках.

Национальным банком в рамках осуществления надзора за деятельностью банков будет проводиться оценка киберриска банков. Использования банками подходов к управлению киберриском, изложенных в настоящем письме, в процессе управления рисками будет рассматриваться как фактор, улучшающий качество управления операционным риском банка.