ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации Банка России по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка

22.01.2025 № 2-МР

Глава 1. Общие положения

1.1. Настоящие Методические рекомендации Банка России разработаны в целях обеспечения единого подхода к реализации кредитными организациями, некредитными финансовыми организациями[1], субъектами национальной платежной системы, а также бюро кредитных историй (далее при совместном упоминании – организации финансового рынка) обязанности по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее при совместном упоминании – объекты информационной инфраструктуры) в соответствии с подпунктом 3.2 пункта 3 Положения Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», абзацем первым подпункта 1.4.5 пункта 1.4 Положения Банка России от 20 апреля

[1] Для целей настоящих Методических рекомендаций Банка России под некредитными финансовыми организациями понимаются некредитные финансовые организации, реализующие усиленный уровень защиты информации, и некредитные финансовые организации, реализующие стандартный уровень защиты информации, в соответствии с Положением Банка России от 20 апреля 2021 года № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

2021 года № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций», абзацем третьим пункта 1.1, абзацем вторым пункта 2.11, пунктами 3.8, 3.9 Положения Банка России от 17 августа 2023 года № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», пунктом 2.3 Положения Банка России от 17 октября 2022 года № 808-П «О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона «О кредитных историях», при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства». Настоящие Методические рекомендации Банка России также могут применяться иными некредитными финансовыми организациями и лицами, оказывающими профессиональные услуги на финансовом рынке.

1.2. Организациям финансового рынка рекомендуется определить границы проведения тестирования[2] на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры. Организациям финансового рынка в границы проведения тестирования на

[2] Для целей настоящих Методических рекомендаций Банка России под границами проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры понимается перечень объектов информационной инфраструктуры, для которых должны проводиться такие тестирование и анализ в соответствии с нормативными актами Банка России.

проникновение и анализа уязвимостей информационной безопасности рекомендуется включать объекты информационной инфраструктуры, распространяемые клиентам для совершения действий в целях осуществления банковских и (или) иных финансовых операций, а также программное обеспечение, обрабатывающее защищаемую информацию на технологических участках[3], используемое для приема электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») (при наличии соответствующих объектов информационной инфраструктуры), включая:

веб-приложения дистанционного банковского обслуживания (далее – ДБО) физических лиц (далее – ФЛ);

веб-приложения ДБО юридических лиц (далее – ЮЛ);

веб-приложения личных кабинетов клиентов некредитных финансовых организаций;

мобильные приложения ДБО ФЛ для различных мобильных операционных систем;

мобильные приложения ДБО ЮЛ для различных мобильных операционных систем;

мобильные приложения личных кабинетов клиентов некредитных финансовых организаций для различных мобильных операционных систем;

специализированные клиентские приложения ДБО ФЛ для различных операционных систем;

специализированные клиентские приложения ДБО ЮЛ для различных операционных систем;

---

[3] Для целей настоящих Методических рекомендаций Банка России под технологическими участками понимаются технологические участки, указанные в подпункте 2.4.3 пункта 2.4 Методических рекомендаций Банка России по описанию наименований объектов информационной инфраструктуры от 20 декабря 2023 года № 18-МР.

специализированные клиентские приложения личных кабинетов клиентов некредитных финансовых организаций для различных операционных систем;

автоматизированные системы, участвующие во взаимодействии с ДБО ФЛ или ЮЛ, в том числе интеграционные системы и API;

серверы приложений;

серверы систем управления базами данных.

1.3. Рекомендуется в целях обеспечения единства подходов к описанию наименований объектов информационной инфраструктуры приводить наименования объектов информационной инфраструктуры, в том числе относящиеся к критичной архитектуре, в соответствии с Методическими рекомендациями Банка России по описанию наименований объектов информационной инфраструктуры от 20 декабря 2023 года № 18-МР.

1.4. Целями проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры могут являться:

оценка уровня защищенности объектов информационной инфраструктуры;

обеспечение доверия к объектам информационной инфраструктуры, в том числе входящим в критичную архитектуру.

1.5. Задачами проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры могут являться:

выявление уязвимостей, определение способов эксплуатации уязвимостей или выявление нарушений функций безопасности объектов информационной инфраструктуры организации финансового рынка, которые могут привести к возникновению негативных последствий нарушения информационной безопасности;

разработка предложений по устранению уязвимостей информационной безопасности;

идентификация риска информационной безопасности (в том числе выявление нарушений (риска нарушения) требований к обеспечению защиты защищаемой информации или обеспечению операционной надежности), включая случаи, когда реализация такого риска приводит к совершению операций без добровольного согласия клиента, а также описание его влияния на уровень защищенности и формирование возможных решений по минимизации риска.

1.6. Организациям финансового рынка рекомендуется проводить тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры самостоятельно в соответствии с главой 4 настоящих Методических рекомендаций Банка России или с привлечением на договорной основе сторонней организации в соответствии с главой 5 настоящих Методических рекомендаций Банка России (далее при совместном упоминании организации финансового рынка и сторонней организации – стороны).

1.7. Перед проведением тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры в целях реализации мер по минимизации негативных последствий нарушения информационной безопасности объектов информационной инфраструктуры при проведении таких тестирования и анализа организациям финансового рынка рекомендуется разработать и (или) актуализировать следующие документы:

техническое задание на проведение тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры (далее – ТЗ);

соглашение об ответственности сторон тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры;

модель угроз информационной безопасности для объектов информационной инфраструктуры на основе методического документа «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 5 февраля 2021 года);

планы восстановления операционной надежности в случае возникновения нештатных ситуаций в ходе проведения тестирования на проникновение объектов информационной инфраструктуры.

1.8. Организациям финансового рынка рекомендуется отражать в ТЗ:

наименование планируемых работ[4];

количество планируемых этапов проведения работ;

срок проведения работ;

цели проведения работ;

перечень нормативных актов, указанных в пункте 1.1 настоящих Методических рекомендаций Банка России, во исполнение которых проводятся работы;

перечень объектов информационной инфраструктуры, подлежащих тестированию на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры, с указанием технологических участков;

перечень объектов информационной инфраструктуры, входящих в границы тестирования, на которых не планируется проводить тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры, с указанием причин, препятствующих проведению тестирования на проникновение (например, ограничение пропускной способности, промежутка времени, в который возможно провести тестирование на проникновение);

[4] Для целей настоящих Методических рекомендаций Банка России под работами понимаются работы по проведению тестирования на проникновение и анализа уязвимостей объектов информационной инфраструктуры.

метод проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, включающий:

возможные классы атак (поверхности, а также техника и тактика атаки) и уязвимостей;

методы и инструменты, используемые для проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры;

перечень баз данных угроз безопасности информации и иные информационные источники для идентификации уязвимостей (примерный перечень приведен в пункте 2.3 настоящих Методических рекомендаций Банка России);

среды, в которых планируется проведение тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры (например, в тестовой среде, которая соответствует промышленной среде и содержит тестовые данные);

схемы сетевых подключений объектов информационной инфраструктуры, включая адреса и подсети, подлежащие тестированию на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры;

перечень факторов риска, реализуемых в рамках тестирования на проникновение объектов информационной инфраструктуры (например, угрозы, шантаж работников[5], воздействие на личные социальные сети и мобильные устройства работников организации финансового рынка);

события, при наступлении которых незамедлительно прекращается тестирование на проникновение объектов информационной инфраструктуры;

ожидаемые результаты тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной

[5] Для целей настоящих Методических рекомендаций Банка России под работниками понимаются штатные работники организации финансового рынка.

инфраструктуры (например, завершение тестирования при отсутствии уязвимостей, критерии принятия решения о необходимости проведения повторного тестирования на проникновение и (или) анализа уязвимостей и так далее), включая требования к разработке рекомендаций по устранению выявленных уязвимостей информационной безопасности;

формы отчетных документов;

сроки и условия проведения повторного тестирования и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры.

1.9. При проведении тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры рекомендуется руководствоваться в том числе следующими документами:

соглашение сторон о разрешении тестирования на проникновение и анализа уязвимостей информационной безопасности адресов и подсетей, в том числе относящихся к критичной архитектуре;

соглашение сторон о неразглашении конфиденциальной информации;

перечень средств защиты информации, используемых на объектах информационной инфраструктуры, с регламентами их работы (используемыми настройками);

правила выделения учетных записей для специалистов[6], привлекаемых к тестированию на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры (в случае необходимости);

парольные политики, применяемые на объектах информационной инфраструктуры;

инструкции пользователей к объектам информационной инфраструктуры;

---

[6] Для целей настоящих Методических рекомендаций Банка России под специалистами понимаются работники сторонней организации, не находящиеся в штате организации финансового рынка.

инструкции администраторов к объектам информационной инфраструктуры;

график работы работников организации финансового рынка.

1.10. Организациям финансового рынка при проведении тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры рекомендуется руководствоваться положениями национального стандарта Российской Федерации ГОСТ Р 58143-2018 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения» (далее – ГОСТ Р 58143-2018).

1.11. Кредитным организациям и некредитным финансовым организациям при проведении тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры рекомендуется руководствоваться подпунктом 7.2.6 пункта 7.2 «Оценка уязвимостей (AVA)» методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций», опубликованного на официальном сайте Банка России[7] в сети «Интернет».

1.12. Результаты тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры рекомендуется оформлять отчетом по результатам тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры (далее – отчет), форма которого приведена в приложении к настоящим Методическим рекомендациям Банка России. К отчету рекомендуется прилагать материалы

[7] http://www.cbr.ru/content/document/file/132666/inf_note_feb_0422.pdf.

об объектах информационной инфраструктуры, предоставленные организацией финансового рынка в соответствии с ТЗ.

1.13. Отчет рекомендуется оформлять в электронном виде в формате, не допускающем его редактирования, и подписывать усиленной квалифицированной электронной подписью руководителя сторонней организации, сертификат ключа проверки которой действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен (электронными подписями работников организации финансового рынка, на которых возложено проведение тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры).

При оформлении отчета на бумажном носителе рекомендуется использовать сквозную нумерацию страниц, прошивать отчет нитью, не имеющей разрывов, и скреплять печатью организации с указанием количества листов в заверительной надписи, подписанной руководителем сторонней организации (работниками организации финансового рынка, на которых возложено проведение тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры). Также рекомендуется присваивать отчету регистрационный номер.

Рекомендуемый срок хранения отчета не менее 5 лет.

1.14. Результаты тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры рекомендуется доводить до сведения заместителя руководителя организации финансового рынка, ответственного за обеспечение информационной безопасности в организации финансового рынка, в том числе ответственного за обнаружение, предупреждение и

ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты[8].

Глава 2. **Рекомендации по проведению тестирования на проникновение объектов информационной инфраструктуры**

2.1. Организациям финансового рынка рекомендуется проводить как внешнее тестирование на проникновение (имитация действий внешнего нарушителя), так и внутреннее тестирование на проникновение (имитация действий внутреннего нарушителя) объектов информационной инфраструктуры.

2.2. Рекомендуется проводить тестирование на проникновение объектов информационной инфраструктуры следующими методами:

методом «черного ящика», при котором исполнитель[9] не владеет информацией об объектах информационной инфраструктуры организации финансового рынка;

методом «серого ящика», при котором исполнитель владеет частичной информацией об объектах информационной инфраструктуры организации финансового рынка;

методом «белого ящика», при котором исполнитель владеет полной информацией об объектах информационной инфраструктуры организации финансового рынка.

2.3. Организациям финансового рынка при проведении тестирования на проникновение объектов информационной инфраструктуры рекомендуется использовать базы данных угроз безопасности информации и иные информационные источники для идентификации уязвимостей и формализованного представления результатов (например, БДУ ФСТЭК

---

[8] Указанная роль предусмотрена в постановлении Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

[9] Для целей настоящих Методических рекомендаций Банка России под исполнителем понимается лицо, привлекаемое к проведению тестирования на проникновение.

России[10], CAPEC[11], MITRE ATT&CK[12], OWASP[13], STIX[14], WASC[15], CWE[16], CVE[17] и иные).

2.4. Рекомендуется при проведении тестирования на проникновение объектов информационной инфраструктуры учитывать потенциал нарушителя, указанного в модели угроз информационной безопасности. При этом рекомендуется использовать автоматизированные средства, позволяющие моделировать атаки с учетом идентифицированных уязвимостей, указанных в главе 3 настоящих Методических рекомендаций Банка России.

2.5. В результаты тестирования на проникновение объектов информационной инфраструктуры рекомендуется включать сравнение полученных результатов с ожидаемыми результатами, указанными в ТЗ.

2.6. Рекомендуется фиксировать фактические результаты выполнения тестирования на проникновение объектов информационной инфраструктуры и исследовать причины возникновения любых непредвиденных ситуаций.

2.7. Рекомендуется проводить повторное тестирование на проникновение объектов информационной инфраструктуры после устранения выявленных уязвимостей. Повторное проведение тестирования на проникновение объектов информационной инфраструктуры может не проводиться для тех объектов информационной инфраструктуры, в которых не были выявлены уязвимости.

---

[10] Банк данных угроз безопасности информации ФСТЭК России по адресу https://bdu.fstec.ru/threat.
[11] Common Attack Pattern Enumerations and Classifications по адресу https://capec.mitre.org.
[12] MITRE ATT&CK по адресу https://attack.mitre.org.
[13] Open Web Application Security Project по адресу https://owasp.org.
[14] Security Threat Information Expression по адресу https://stixproject.github.io.
[15] Web Application Security Consortium по адресу https://www.webappsec.org.
[16] Common Weakness Enumeration по адресу https://cwe.mitre.org.
[17] Common Vulnerabilities and Exposures по адресу https://cve.mitre.org.

Глава 3. **Рекомендации по проведению анализа уязвимостей информационной безопасности объектов информационной инфраструктуры**

3.1. В процессе проведения анализа уязвимостей информационной безопасности объектов информационной инфраструктуры рекомендуется проводить выявление, оценку и устранение уязвимостей информационной безопасности объектов информационной инфраструктуры. Выявление, оценку и устранение уязвимостей рекомендуется проводить на этапах создания и эксплуатации объектов информационной инфраструктуры. Периодичность проведения указанных мероприятий рекомендуется устанавливать на основе нормативных актов Банка России с учетом риск-ориентированного подхода.

3.2. Рекомендуется проводить выявление уязвимостей информационной безопасности объектов информационной инфраструктуры, связанных с ошибками кода в программном обеспечении (общесистемное, прикладное, специальное), а также программном обеспечении средств защиты информации, технических средств.

3.3. Выявление уязвимостей информационной безопасности на объектах информационной инфраструктуры рекомендуется проводить с использованием средств анализа защищенности, прошедших процедуру сертификации не ниже 4 уровня доверия в соответствии с приказом ФСТЭК России от 2 июня 2020 года № 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (далее – приказ ФСТЭК России от 2 июня 2020 года № 76).

3.4. При выявлении уязвимостей информационной безопасности объектов информационной инфраструктуры организациям финансового рынка рекомендуется оценивать уровень критичности уязвимостей, руководствуясь методическим документом «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств» (утвержден ФСТЭК России 28 октября 2022 года).

3.5. Выявление уязвимостей путем анализа кода программного обеспечения рекомендуется проводить с использованием средств анализа исходного кода, прошедших процедуру сертификации не ниже 4 уровня доверия в соответствии с приказом ФСТЭК России от 2 июня 2020 года № 76.

3.6. Рекомендуется для выявления и описания уязвимостей, информация о которых не включена в средства анализа защищенности, указанные в пункте 3.3 настоящих Методических рекомендаций Банка России, а также для формализованного представления результатов использовать БДУ ФСТЭК России и иные базы данных, указанные в пункте 2.3 настоящих Методических рекомендаций Банка России, содержащие сведения об уязвимостях объектов информационной инфраструктуры.

3.7. При проведении работ по анализу и устранению уязвимостей, выявленных в объектах информационной инфраструктуры, рекомендуется руководствоваться методическим документом «Руководство по организации процесса управления уязвимостями в органе (организации)» (утвержден ФСТЭК России 17 мая 2023 года).

Глава 4. **Рекомендации по самостоятельному проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры**

4.1. Рекомендуется самостоятельно проводить тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры в случаях:

изменения архитектуры и (или) изменения конфигурации объектов информационной инфраструктуры, которые не затрагивают функционирование объектов критической информационной инфраструктуры или функционал, связанный с обеспечением информационной безопасности;

контроля устранения недостатков, выявленных при тестировании объектов информационной инфраструктуры на проникновение с привлечением сторонней организации.

4.2. В случае если организация финансового рынка принимает решение о самостоятельном проведении тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, в организации финансового рынка рекомендуется выделить отдельное структурное подразделение или необходимое количество работников в штате, на которых будут возложены функции по тестированию на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры.

4.3. Не рекомендуется возлагать на структурное подразделение и работников, указанных в пункте 4.2 настоящих Методических рекомендаций Банка России, функции по обеспечению информационной безопасности объектов информационной инфраструктуры, в отношении которых планируется проведение тестирования на проникновение объектов информационной инфраструктуры.

4.4. Для самостоятельного проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организациям финансового рынка рекомендуется назначить не менее двух работников, имеющих опыт в проведении тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры не менее 3 лет, и ежегодно направлять назначенных работников на прохождение курсов повышения квалификации по направлению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры в организации финансового рынка. Функции по тестированию на проникновение объектов информационной инфраструктуры рекомендуется определить в должностных регламентах (инструкциях) работников.

4.5. Организациям финансового рынка не рекомендуется привлекать заинтересованных работников (разработчики, владельцы, администраторы и администраторы информационной безопасности объектов информационной

инфраструктуры, подлежащих тестированию на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры) к тестированию на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры.

Глава 5. **Рекомендации по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры с привлечением сторонней организации**

5.1. Для проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры сторонней организацией рекомендуется привлекать на договорной основе сторонние организации, соответствующие следующим критериям:

наличие у сторонней организации действующей лицензии на осуществление деятельности по технической защите конфиденциальной информации для оказания услуг, предусмотренных подпунктом «б» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

наличие опыта работы по проведению тестирования на проникновение объектов информационной инфраструктуры не менее 3 лет в организациях финансового рынка, подтвержденного не менее чем тремя соответствующими завершенными договорами (контрактами, соглашениями);

наличие подтвержденного опыта проведения тестирования на проникновение объектов информационной инфраструктуры у привлекаемых специалистов сторонней организации не менее 3 лет.

5.2. В договорах на проведение работ рекомендуется указывать, что проведение тестирования на проникновение и анализа уязвимостей

информационной безопасности объектов информационной инфраструктуры должно соответствовать требованиям нормативных актов Банка России, указанных в пункте 1.1 настоящих Методических рекомендаций Банка России.

5.3. Организациям финансового рынка рекомендуется обеспечить нахождение специалистов сторонней организации и автоматизированных средств, используемых для проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, на территории Российской Федерации при проведении тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры.

5.4. Организациям финансового рынка рекомендуется допускать к проведению тестирования на проникновение объектов информационной инфраструктуры специалистов сторонней организации, которые не принимали участия на стадиях формирования требований к системе защиты объектов информационной инфраструктуры, проектирования, внедрения и оценки соответствия системы защиты объектов информационной инфраструктуры.

Глава 6. **Информирование Банка России о результатах проведения тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры**

6.1. Организациям финансового рынка рекомендуется обеспечивать регистрацию инцидентов защиты информации, связанных с проведением тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры.

6.2. Организациям финансового рынка, которые должны информировать Банк России о выявленных инцидентах в соответствии с нормативными актами Банка России, указанными в пункте 1.1 настоящих Методических рекомендаций Банка России, рекомендуется информировать Банк России о выявленных в рамках проведения тестирования на проникновение и анализа уязвимостей информационной безопасности

объектов информационной инфраструктуры инцидентах защиты информации, включенных в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на официальном сайте в сети «Интернет», а также о причинах возникновения инцидента защиты информации, принятых мерах и проведенных мероприятиях по реагированию на инцидент защиты информации.

6.3. Кредитным организациям, некредитным финансовым организациям и субъектам национальной платежной системы в целях информирования Банка России о выявленных инцидентах защиты информации рекомендуется руководствоваться порядком, а также сроками и формами взаимодействия организаций финансового рынка с Банком России, определенными стандартом Банка России СТО БР БФБО-1.5-2023 «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности», который размещен на официальном сайте Банка России в сети «Интернет» в разделе «Информационная безопасность» (по адресу http://www.cbr.ru/information_security/).

6.4. При информировании Банка России организациям финансового рынка рекомендуется отражать связанность выявленных инцидентов защиты информации с проведением тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры.

Глава 7. **Заключительные положения**

7.1. Настоящие Методические рекомендации Банка России подлежат опубликованию в «Вестнике Банка России» и размещению на официальном сайте Банка России в сети «Интернет».

Председатель Банка России Э.С. Набиуллина

Приложение
к Методическим рекомендациям Банка России по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка

Рекомендуемая форма

Отчет по результатам тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры
<Наименование организации финансового рынка>

1. Раздел «Общие положения»:

описание объекта оценки;

общее описание проводимых работ;

технологические участки;

краткое описание результатов тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры;

период проведения тестирования на проникновение объектов информационной инфраструктуры;

реквизиты сторон;

Ф.И.О. и должности исполнителей тестирования на проникновение объектов информационной инфраструктуры;

сведения об учетных записях и их ролях, предоставленных для проведения тестирования на проникновение объектов информационной инфраструктуры (при наличии);

дополнительная информация, предоставленная для проведения тестирования на проникновение объектов информационной инфраструктуры;

описание потенциала нарушителя безопасности информации в соответствии с моделью угроз безопасности информации;

определение негативных последствий и (или) недопустимых событий, которые могут быть реализованы в случае эксплуатации уязвимостей;

перечень объектов доступа, в отношении которых возможен несанкционированный доступ с использованием выявленных уязвимостей;

виды тестирования на проникновение объектов информационной инфраструктуры с указанием тестируемых объектов информационной инфраструктуры;

описание области исключений тестирования на проникновение объектов информационной инфраструктуры или сведения об отсутствии таких исключений, а также причины исключения этой области.

2. Раздел «Методология проведения тестирования на проникновение объектов информационной инфраструктуры»:

описание стадий тестирования на проникновение объектов информационной инфраструктуры в соответствии с ГОСТ Р 58143-2018;

описание условий и обобщенных результатов проведения тестирования на проникновение объектов информационной инфраструктуры.

3. Раздел «Описание выявленных уязвимостей»:

общий перечень выявленных уязвимостей и их описание в соответствии с национальным стандартом Российской Федерации ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»;

использованный инструментарий тестирования на проникновение объектов информационной инфраструктуры;

IP-адрес объекта сканирования, DNS-имя (при наличии) и любая дополнительная информация, позволяющая однозначно идентифицировать объекты информационной инфраструктуры или их анализируемую часть.

4. Раздел «Эксплуатация уязвимостей»:

описание использования шаблонов атак, включая алгоритм шаблона, подтверждающее возможность эксплуатации выявленных уязвимостей;

дата и время использования шаблонов атак;

описание негативных последствий и (или) недопустимых событий, которые могут произойти при успешной реализации выявленных уязвимостей.

5. Раздел «Рекомендации по устранению»:

описание уязвимостей с указанием их критичности;

рекомендации по устранению уязвимостей.