ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
25 ноября 2025 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

2025

1. Общие положения

1.1. Настоящая Методика анализа защищенности информационных систем (далее – Методика) разработана в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1.2. Настоящая Методика определяет организацию, порядок проведения и содержание работ, проводимых в ходе испытаний систем защиты информации информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей (далее – информационные системы) в соответствии с подпунктом «б» пункта 16 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29 апреля 2021 г. № 77[1].

1.3. Настоящая Методика предназначена для организации и проведения работ по анализу защищенности информационных систем, целью проведения которого является выявление уязвимостей информационных систем с последующей оценкой возможности их использования нарушителем для реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий (далее – анализ уязвимостей).

1.4. Настоящая Методика применяется в ходе:

а) аттестации информационных систем на соответствие требованиям по защите информации[2];

---

1 Зарегистрирован Минюстом России 10 августа 2021 г., регистрационный № 64589.

2 Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом ФСТЭК России от 11 апреля 2025 г. № 117.

Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых предприятиями оборонно-промышленного комплекса, утвержденные приказом ФСТЭК России от 28 февраля 2017 г. № 31.

Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239.

Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2013 г. № 31.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21.

б) контроля уровня защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в информационных системах, проводимого в соответствии с требованиями по защите информации;

в) оценки соответствия информационных систем требованиям по защите информации (испытания) и достаточности принимаемых мер по защите информации (обеспечению безопасности), реализация которых предусмотрена требованиями по защите информации.

2. Организация работ по проведению анализа уязвимостей

2.1. Анализ уязвимостей проводится по решению руководителя государственного органа (организации), являющегося заказчиком создаваемой информационной системы и (или) осуществляющего эксплуатацию информационной системы (далее – заказчик (оператор)), или уполномоченного им лица.

2.2. Работы по анализу уязвимостей проводятся структурным подразделением, специалистами по защите информации заказчика (оператора) и (или) организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации (с правом проведения работ и оказания услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации, по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации), выданную ФСТЭК России в соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (далее – исполнитель).

2.3. К проведению анализа уязвимостей допускаются специалисты исполнителя, изучившие положения настоящей Методики, и обладающие компетенциями, необходимыми для проведения работ в соответствии с настоящей Методикой. Ответственность за привлечение к проведению анализа уязвимостей специалистов, обладающих необходимыми знаниями и компетенциями, возлагается на исполнителя.

2.4. Основанием для проведения работ по анализу уязвимостей является заключенный между заказчиком (оператором) и исполнителем договор или иной документ, на основании которого проводится анализ уязвимостей.

Основанием для проведения анализа уязвимостей структурным подразделением, специалистами по защите информации заказчика (оператора),

принадлежащих ему информационных систем, является решение (приказ, распоряжение или иной документ) руководителя заказчика (оператора) или уполномоченного им лица на проведение данных работ.

В договоре или ином документе, на основании которого проводится анализ уязвимостей, предусматриваются следующие этапы:

анализ уязвимостей информационной системы, выполняемый исполнителем;

устранение заказчиком выявленных уязвимостей информационной системы;

повторный анализ уязвимостей информационной системы с целью проверки устранения заказчиком (оператором) уязвимостей информационной системы.

2.5. До начала проведения работ по анализу уязвимостей исполнитель по согласованию с заказчиком (оператором) может провести подготовку, которая должна быть направлена на получение необходимых для проведения анализа уязвимостей сведений об информационной системе и информационно-телекоммуникационной инфраструктуре, на базе которой она функционирует, особенностях их эксплуатации. Подготовка предусматривает во взаимодействии с заказчиком (оператором) сбор информации об информационной системе и информационно-телекоммуникационной инфраструктуре, на базе которой она функционирует, особенностях ее эксплуатации и ее пользователях. Полученная информация используется для уточнения границ проведения работ.

2.6. Специалисты заказчика (оператора) и исполнителя, ответственные за оперативное взаимодействие и контроль проведения анализа уязвимостей, осуществляют согласование и контроль времени проведения работ и действий исполнителя и заказчика (оператора) при анализе уязвимостей, контроль за ходом проведения работ, своевременное выявление и решение проблемных вопросов, возникающих при проведении работ.

Специалисты исполнителя, ответственные за оперативное взаимодействие и контроль проведения анализа уязвимостей, должны обладать знаниями о типовых уязвимостях информационных технологий, программных, программно-аппаратных средств, уязвимостях конфигурации и архитектуры информационных систем, способах их выявления и устранения, а также составе и содержании работ, проводимых в ходе анализа уязвимостей в соответствии с настоящей Методикой.

Специалисты заказчика (оператора) должны обладать знаниями о структурно-функциональных характеристиках информационной системы и (или) информационно-телекоммуникационной инфраструктуре, на базе которой она функционирует, составе программных и программно-аппаратных средств, доменной архитектуре, сетевой топологии, применяемых технологиях (системах управления базами данных, виртуализации и контейнеризации, веб-приложениях, мобильных

приложениях), а также о способах и средствах защиты информации, применяемых в информационной системе.

2.7. В ходе анализа уязвимостей информационной системы должно выявляться максимально возможное количество уязвимостей в информационной системе.

К уязвимостям информационной системы относятся уязвимости кода, архитектуры и конфигурации информационной системы[3].

2.8. В случае, если по результатам анализа исполнителем не выявлено уязвимостей критического и высокого уровней опасности, а также уязвимостей среднего и низкого уровней опасности, которые могут быть использованы потенциальным нарушителем для реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий, или установлен факт того, что принятые заказчиком (оператором) меры не позволяют потенциальному нарушителю использовать такие уязвимости для реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий, исполнителем выдается положительное заключение по результатам анализа уязвимостей в информационной системе заказчика (оператора).

Порядок оценки и устранения выявленных уязвимостей информационной системы приведен в разделе 3.4 настоящей Методики.

2.9. Заказчик (оператор) с учетом назначения, архитектуры и особенностей эксплуатации информационной системы в договоре или ином документе, на основании которого проводится анализ уязвимостей, определяет период времени, в течение которого должны быть проведены все работы по анализу уязвимостей в соответствии с настоящей Методикой.

При необходимости заказчиком (оператором) могут быть установлены перерывы в проведении работ. В этом случае исполнителем должны быть прекращены все работы по анализу уязвимостей. Возобновление работ исполнителем осуществляется с достигнутого результата.

2.10. В ходе анализа уязвимостей применяются следующие виды анализа:

а) внешнее сканирование (С1), в ходе которого исполнителем проводится анализ периметра информационной системы. Работы проводятся удаленно из сети «Интернет». В ходе внешнего сканирования выявляются уязвимости телекоммуникационного оборудования, средств защиты информации, программного обеспечения, сетевых сервисов и служб, приложений, размещенных на периметре информационной системы;

---

3 Национальный стандарт Российской Федерации ГОСТ Р 65546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»

б) внутреннее сканирование (С2), в ходе которого исполнителем проводится анализ информационной инфраструктуры информационной системы, находящейся внутри периметра (внутренней инфраструктуры). Заказчик (оператор) предоставляет исполнителю доступ ко внутренней инфраструктуре. В ходе внутреннего сканирования выявляются уязвимости программных, программно-аппаратных средств (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации, программируемых логических контроллеров, средств автоматизации технологических процессов и «умных» устройств), расположенных во внутренней информационной инфраструктуре заказчика (оператора).

2.11. Внутреннее сканирование (С2) может проводиться:

локально с предоставлением исполнителю возможности непосредственного подключения его средства вычислительной техники к портам программно-аппаратного средства информационной системы и (или) информационно-телекоммуникационной инфраструктуры, на базе которой она функционирует;

удаленно с предоставлением исполнителю доступа к информационной системе и (или) информационно-телекоммуникационной инфраструктуре, на базе которой она функционирует, с использованием защищенного подключения.

Внутреннее сканирование проводится удаленно с предоставлением исполнителю доступа к информационной системе только по согласованию с заказчиком (оператором). В данном случае исполнитель обязуется принять меры по защите информации в информационной инфраструктуре, задействованной для проведения анализа уязвимостей, а также обеспечить защищенное подключение к информационной системе заказчика (оператора).

Внутреннее сканирование (С2) проводится от лица привилегированного пользователя с административными правами доступа и правами сетевого доступа. В этом случае заказчик (оператор) организует создание соответствующей тестовой привилегированной учетной записи для проведения анализа уязвимостей, которая подлежит удалению (блокированию) заказчиком после завершения проведения испытаний.

Дополнительно внутреннее сканирование (С2) может проводиться путем сканирования без аутентификации исполнителя (например, в отношении прикладного программного обеспечения, являющего самостоятельной разработкой заказчика (оператора), а также иного программного обеспечения, предназначенного для выполнения значимых функций информационной системы).

2.12. В ходе анализа уязвимостей исполнителем применяются следующие методы:

а) сравнение наименований, версий программного обеспечения, а также иных атрибутов с базой данных уязвимостей, размещенных в банке данных угроз безопасности информации ФСТЭК России, а также иных базах данных уязвимостей, (пассивные методы анализа уязвимостей) в автоматизированном режиме;

б) выявление уязвимостей на основе анализа поведения программного обеспечения путем формирования специальных тестовых запросов (активные методы сканирования) и анализа конфигураций и настроек.

2.13. Границы проведения работ при анализе уязвимостей определяются заказчиком (оператором) совместно с исполнителем с учетом пунктов 2.14 и 2.15 настоящей Методики. Перед началом проведения анализа уязвимостей заказчик (оператор) обеспечивает резервирование информации, программных, программно-аппаратных средств информационной системы, включенных в границы проведения работ (при необходимости).

2.14. В границы проведения работ при внешнем сканировании (С1) включаются публичные сетевые адреса, службы и сервисы информационной системы и информационно-телекоммуникационной инфраструктуры, на базе которой она функционирует, доступные из сети «Интернет», а также их доменные имена. Перечень сетевых адресов, портов, служб и сервисов, доменных имен предоставляется заказчиком (оператором) или по согласованию с ним выявляется исполнителем при инвентаризации информационной системы и информационно-телекоммуникационной инфраструктуры, на базе которой она функционирует, в ходе подготовки к анализу уязвимостей.

2.15. В границы проведения работ при внутреннем сканировании (С2) включаются программные и программно-аппаратные средства, в том числе системное и прикладное программное обеспечение, сетевые службы и интерфейсы взаимодействия, сервисы, приложения, образы контейнеров, а также программируемые логические контроллеры, средства автоматизации технологических процессов и «умные» устройства. Перечень программных и программно-аппаратных средств предоставляется заказчиком (оператором) или по согласованию с ним выявляется исполнителем при инвентаризации информационной системы и информационно-телекоммуникационной инфраструктуры, на базе которой она функционирует, в ходе подготовки к анализу уязвимостей. Внутреннему сканированию подлежат все серверные сегменты (серверы), входящие в состав информационной системы, сетевое оборудование и средства защиты информации, а также автоматизированные рабочие места привилегированных и непривилегированных пользователей.

В случае наличия в информационной системе типовых по составу и структуре

автоматизированных рабочих мест непривилегированных пользователей и при условии, что конфигурация таких автоматизированных рабочих мест не изменялась относительно типовой в процессе эксплуатации информационной системы, допускается проводить анализ уязвимостей в отношении 30 процентов мест.

2.16. Состав и содержание работ по анализу уязвимостей, проводимых в соответствии с настоящей Методикой в рамках аттестации информационной системы, в ходе оценки соответствия информационной системы или контроля защищенности информации от несанкционированного доступа включается в программу и методики аттестационных испытаний, приказ, распоряжение руководителя заказчика (оператора) или уполномоченного им лица на проведение работ (в случае проведения работ структурным подразделением, специалистами по защите информации) или в иной документ, на основании которого исполнителем проводятся испытания.

2.17. В информационной инфраструктуре исполнителя, с использованием которой проводится анализ уязвимостей, а также в отношении каналов взаимодействия указанной инфраструктуры с информационной системой должны быть приняты меры по защите информации, препятствующие реализации угроз безопасности информации информационной системы со стороны инфраструктуры исполнителя или через инфраструктуру исполнителя.

2.18. Заказчик (оператор) во время проведения анализа уязвимостей по запросу исполнителя может изменять отдельные настройки в программных, программно-аппаратных средствах информационной системы, в том числе в средствах защиты информации, если это необходимо исполнителю для проведения анализа уязвимостей.

Заказчик (оператор) осуществляет сбор данных о событиях, связанных с внесением изменений в отдельные настройки программных, программно-аппаратных средств информационной системы, в том числе средств защиты информации.

2.19. По результатам проведения анализа уязвимостей исполнитель предоставляет заказчику (оператору) разработанный в соответствии с разделом 4 настоящей Методики отчет (протокол), в котором подтверждается или не подтверждается наличие уязвимостей информационной системы и возможность использования потенциальным нарушителем выявленных уязвимостей для реализации угроз безопасности информации (векторов атак).

2.20. При проведении анализа уязвимостей информационной системы применяются сертифицированные по требованиям безопасности информации ФСТЭК России средства выявления уязвимостей.

При проведении анализа уязвимостей дополнительно могут применяться иные инструментальные средства, функциональные возможности которых обеспечивают реализацию положений настоящей Методики, имеющие техническую поддержку и возможность адаптации (доработки) под особенности проводимых работ, либо свободно распространяемые в исходных кодах, либо средства собственной разработки, не имеющие каких-либо ограничений по их применению, адаптации (доработке) на территории Российской Федерации.

Допускается использовать средства выявления уязвимостей, принадлежащие исполнителю, и (или) по согласованию с исполнителем средства выявления уязвимостей заказчика (оператора).

Размещение в тестируемой информационной системе или подключение к ней средств выявления уязвимостей и инструментальных средств исполнителя согласовывается заказчиком (оператором).

Информация об используемых в системе средствах выявления уязвимостей, инструментальных средствах включается в отчет (протокол), содержащий результаты анализа уязвимостей. Исполнитель приводит в отчете (протоколе) обоснование необходимости применения иных инструментальных средств и сведения о работах по анализу уязвимостей, для которых используются иные инструментальные средства.

Перед проведением анализа уязвимостей исполнитель проверяет актуальность баз данных уязвимостей, содержащихся в средствах выявления уязвимостей.

2.21. При использовании средств выявления уязвимостей, инструментальных средств для анализа уязвимостей исполнитель обязан принять все возможные меры по недопущению нарушения функционирования информационной системы и информационно-телекоммуникационной инфраструктуры, на базе которой она функционирует.

2.22. После завершения анализа уязвимостей заказчик (оператор) должен обеспечить удаление из информационной системы и информационно-телекоммуникационной инфраструктуры, на базе которой она функционирует, используемых средств выявления уязвимостей, инструментальных средств (в случае их установки исполнителем при проведении анализа уязвимостей), а также обеспечить изменение конфигурации программного обеспечения до исходной (базовой) конфигурации (в случае внесения изменений).

2.23. Исполнитель обязан обеспечить конфиденциальность информации, полученной в ходе анализа уязвимостей, в соответствии с договором или иным документом, на основании которого проводился анализ уязвимостей, и с учетом нормативных правовых актов Российской Федерации.

Исполнитель не должен без разрешения заказчика (оператора) отчуждать на внешние машинные носители информации или передавать, распространять по сети «Интернет» любую информацию, относящуюся к проводимому анализу и информационным системам. Исполнитель не должен использовать информацию, полученную в ходе проведения анализа уязвимостей, ни для каких целей, кроме как для реализации договора или иного документа, на основании которого проводился анализ уязвимостей.

2.24. Действия исполнителя по анализу уязвимостей в информационной системе не должны создавать угрозы безопасности информации для иных информационных систем.

2.25. Условия и ограничения при проведении анализа уязвимостей, предусмотренные настоящей Методикой, подлежат включению в договор или иной документ, на основании которого проводятся испытания.

3. Порядок проведения анализа уязвимостей

Анализ уязвимостей информационной системы предусматривает следующие этапы проведения:

а) сбор исходной информации;

б) внешний анализ уязвимостей;

в) внутренний анализ уязвимостей;

г) оценка выявленных уязвимостей.

3.1. Сбор исходной информации

3.1.1. На этапе сбора исходной информации исполнителем должна быть получена информация о составе, наименованиях и версиях программных, программно-аппаратных средств, входящих в состав информационной системы, а также о сетевой инфраструктуре и сегментах информационной системы, пользователях информационной системы и иной информации, необходимой для проведения анализа уязвимостей.

3.1.2. В ходе сбора исходной информации исполнителем проводится:

а) инвентаризация сетевых адресов, портов, служб и сервисов, сетевых протоколов, внешних интерфейсов взаимодействия, находящихся на периметре информационной системы и информационно-телекоммуникационной инфраструктуры, на базе которой она функционирует, а также расположенных во внутренней инфраструктуре;

б) инвентаризация программных, программно-аппаратных средств, находящихся на периметре, а также во внутренней инфраструктуре информационной системы.

3.1.3. Для проведения сбора информации заказчик (оператор) представляет исполнителю перечни IP-адресов и (или) доменных имен программно-аппаратных средств, сервисов и приложений, находящихся на периметре информационной системы.

В случае отсутствия у заказчика (оператора) указанной информации исполнитель самостоятельно проводит сбор информации путем сканирования публичных сетевых адресов и портов с целью обнаружения доступных из сети «Интернет» сетевых служб, сервисов, доменных имен, интерфейсов программных, программно-аппаратных средств, находящихся на периметре информационной системы. Полученный путем сбора исполнителем перечень сетевых адресов, портов, сетевых служб, сервисов, доменных имен, интерфейсов согласуется с заказчиком (оператором) до начала проведения работ.

В случае выявления по результатам инвентаризации не используемых (не идентифицированных) сетевых адресов, служб и сервисов, доменных имен, исполнитель уведомляет об этом заказчика (оператора) информационной системы.

3.1.4. Инвентаризация программных, программно-аппаратных средств, находящихся на периметре информационной системы, проводится с целью определения наименований программного обеспечения и версий сетевых служб и сервисов, программных, программно-аппаратных средств, доступных из сети «Интернет», путем:

поиска в сети «Интернет» информации об IP-адресах и доменных именах, принадлежащих заказчику (обращение к сервисам типа WHOIS);

сканирования IP-адресов и доменных имен с использованием средств выявления уязвимостей, иных инструментальных средств в автоматизированном режиме;

интервьюирования специалистов заказчика (оператора), изучения проектной и эксплуатационной документации на информационную систему.

3.1.5. Инвентаризация программных, программно-аппаратных средств, входящих в состав внутренней инфраструктуры информационной системы, проводится исполнителем с целью определения IP-адресов, доменных имен, MAC-адресов устройств, входящих в состав информационной системы, наименований и версий установленного на них программного обеспечения путем:

сканирования внутренней инфраструктуры с использованием средств выявления уязвимостей, иных инструментальных средств в автоматизированном режиме;

анализа конфигурационной информации, содержащейся в контроллерах доменов, системах сбора и мониторинга событий безопасности и иных системах мониторинга информационной системы;

интервьюирования специалистов заказчика (оператора), изучения проектной и эксплуатационной документации на информационную систему.

3.1.6. По результатам сбора исходной информации формируются следующие исходные данные, необходимые для проведения внешнего и внутреннего сканирования в соответствии с настоящей Методикой:

а) состав и версии системного и прикладного программного обеспечения, средств защиты информации, а также сетевых служб и приложений;

б) наличие актуальных обновлений системного и прикладного программного обеспечения, средств защиты информации, а также сетевых служб и приложений;

в) архитектуру (карту) сети передачи данных информационной системы и ее сегментов (при наличии), включая перечень IP-адресов, доменных имен;

г) способы и технологии идентификации и аутентификации пользователей информационной системы, включая типы пользователей, учетные данные пользователей;

д) сведения о типовых конфигурациях системного и прикладного программного обеспечения, средств защиты информации, а также сетевых служб и приложений (при их наличии).

3.1.7. Перечень работ, проводимых на этапе сбора исходной информации, приведен в таблице 1.

Таблица 1

Условное обозначение и номер работы	Наименование работ	Вид анализа	
		С1	С2
Сбор исходной информации			
ИНП	Инвентаризация периметра информационной системы		
ИНП.1	Определение внешних IP-адресов, находящихся на периметре информационной системы	+	-
ИНП.2	Определение доменных имен информационной системы	+	-
ИНП.3	Определение веб-ресурсов информационной системы	+	-
ИНП.4	Поиск внешних интерфейсов взаимодействия, открытых	+	-

Условное обозначение и номер	Наименование работ	Вид анализа	
		С1	С2
	портов служб, находящихся на периметре информационной системы (SMTP, IMAP, OWA, DNS-серверы, FTP/SFTP, RDP/SSH и других служб)		
ИНП.5	Сбор информации о сетевых службах и сервисах (сервисах удаленного доступа, DNS и иных сервисах)	+	-
ИНП.6	Сбор информации о версиях системного и прикладного программного обеспечения, а также программно-аппаратных средств, средств защиты информации, доступных из сети «Интернет»	+	-
ИНП.7	Определение конфигураций, находящихся на периметре сетевых служб и сервисов, системного и прикладного программного обеспечения, а также программно-аппаратных средств и средств защиты информации	+	-
ИНП.8	Сбор информации о способах и технологиях идентификации и аутентификации пользователей информационной системы	+	-
ИНП.9	Сбор информации о программном обеспечении, реализующем модели машинного обучения (технологии искусственного интеллекта)	+	-
ИНП.10	Выявление неиспользуемых (не идентифицированных) сетевых адресов, портов, сетевых служб, сервисов, доменных имен, интерфейсов, находящихся на периметре информационной системы	+	-
ИНП.11	Выявление несанкционированных точек подключения устройств, сетевых сервисов и служб, приложений, открытых портов программно-аппаратных средств и средств защиты информации, находящихся на периметре информационной системы	+	-
ИВИ	Инвентаризация внутренней инфраструктуры		
ИВИ.1	Сбор информации об архитектуре внутренней сети передачи данных информационной системы, включая перечень IP-адресов, доменных имен (DNS-имен), портов сетевых служб	-	+
ИВИ.2	Сбор информации о сетевых службах и сервисах внутренней инфраструктуры	-	+
ИВИ.3	Инвентаризация серверов и систем хранения данных (физические и виртуальные сервера, системы управления базами данных, файловые хранилища, почтовые сервера, системы виртуализации), а также наименований и версий программного обеспечения серверов и систем хранения данных	-	+
ИВИ.4	Инвентаризация автоматизированных рабочих мест	-	+

Условное обозначение и номер	Наименование работ	Вид анализа	
		С1	С2
	пользователей (определение типов рабочих устройств (компьютеры, ноутбуки, мобильные устройства), наименований и версий операционных систем и иного программного обеспечения, установленного на указанных устройствах)		
ИВИ.5	Инвентаризация прикладного программного обеспечения (наименований и версий веб-серверов, бухгалтерских систем, систем электронного документооборота, мобильных приложений и иного прикладного программного обеспечения)	-	+
ИВИ.6	Сбор информации о пользователях, групповых политиках, способах аутентификации пользователей (учетные записи пользователей, группы пользователей, парольные политики и многофакторная аутентификация)	-	+
ИВИ.7	Определение конфигураций, находящихся во внутренней инфраструктуре сетевых служб и сервисов, системного и прикладного программного обеспечения, а также программно-аппаратных средств и средств защиты информации	-	+
ИВИ.8	Выявление неиспользуемых (не идентифицированных) сетевых адресов, портов, сетевых служб, сервисов, доменных имен, интерфейсов	-	+
ИВИ.9	Выявление несанкционированных точек подключения устройств, сетевых сервисов и служб, приложений	-	+

Знаком «+» отмечены необходимые работы для каждого из видов анализа. Знаком «-» отмечены работы, которые неприменимы для данного вида тестирования.

3.2. Внешний анализ уязвимостей

3.2.1. Работы по внешнему анализу уязвимостей должны предусматривать выявление уязвимостей сетевых служб и сервисов, системного и прикладного программного обеспечения, доступных из сети «Интернет», в том числе уязвимостей, связанных с недостатками их конфигураций.

3.2.2. В целях проведения внешнего анализа уязвимостей осуществляется:

а) выявление известных уязвимостей программного обеспечения сетевых служб, сервисов, программных, программно-аппаратных средств, интерфейсы которых доступны из сети «Интернет»;

б) выявление уязвимостей конфигурации сетевых протоколов, системного и прикладного программного обеспечения, интерфейсы которых доступны из сети «Интернет»;

в) выявление уязвимостей аутентификации, использования паролей, заданных по умолчанию, и устойчивости паролей;

г) выявление уязвимостей кода и конфигурации прикладного программного обеспечения (веб-приложений, мобильных приложений, программного обеспечения, реализующего модели машинного обучения и другого прикладного программного обеспечения), доступных из сети «Интернет».

3.2.3. Внешний анализ уязвимостей проводится исполнителем:

путем сканирования интерфейсов сетевой инфраструктуры информационной системы, приложений с использованием средств выявления уязвимостей, иных инструментальных средств, предназначенных для поиска уязвимостей программного кода и конфигурации с использованием пассивных и активных методов анализа уязвимостей в автоматизированном режиме;

путем поиска информации об уязвимостях программных, программно-аппаратных средств, средств защиты информации, находящихся на периметре информационной системы, в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также в иных базах данных уязвимостей в автоматизированном режиме;

путем применения пассивных и активных методов анализа уязвимостей в ручном режиме.

3.2.4. По результатам проведения внешнего анализа исполнителем формируется перечень уязвимостей периметра информационной системы, включающий:

а) уязвимости программного обеспечения телекоммуникационного оборудования и межсетевых экранов, находящихся на периметре информационной системы;

б) уязвимости конфигурации сетевой инфраструктуры периметра информационной системы;

в) уязвимости сетевых служб, сервисов, веб-серверов, приложений, мобильных приложений, систем управления базами данных, операционных систем, прокси-серверов и иного программного обеспечения, интерфейсы которых доступны из сети «Интернет»;

г) уязвимости, связанные с недостатками конфигурации сетевых служб, сервисов, веб-приложений, мобильных приложений, систем управления базами

данных, операционных систем, прокси-серверов и иного программного обеспечения, интерфейсы которых доступны из сети «Интернет».

3.2.5. Перечень работ, проводимых исполнителем в ходе внешнего сканирования, приведен в таблице 2.

Таблица 2

Условное обозначение и номер работы	Наименование работы[4]	Вид анализа
		С1
Внешнее сканирование		
СИН	Сетевая инфраструктура	
СИН.1	Поиск уязвимостей программного обеспечения телекоммуникационного оборудования и межсетевых экранов	+
СИН.2	Поиск уязвимостей конфигурации сетевых служб и протоколов (HTTP, HTTPS, SMTP, SSH, NTP, IPSec, SNMP, DNS, FTP, RDP, RPC, PPTP, NetBIOS, Telnet, SIP, POP3, IMAP и других протоколов)	+
СИН.3	Поиск уязвимостей, связанных с использованием паролей, заданных по умолчанию	+
СИН.4	Поиск уязвимостей механизмов аутентификации (например, применение протокола Telnet вместо SSH)	+
СИН.5	Поиск уязвимостей управления доступом к интерфейсам управления сетевых служб	+
СИН.6	Поиск уязвимостей, связанных с отсутствием блокировки учётной записи пользователей после неудачных попыток входа	+
СИН.7	Поиск активных сетевых служб, использующих небезопасные протоколы передачи данных (FTP, Telnet, rlogin, rsh, Finger)	+
СИН.8	Поиск безопасных версий сетевых протоколов (SMBv1, SSL 2.0/3.0, TLS 1.0, NTLMv1)	+
СУД	Службы удаленного доступа	
СУД.1	Поиск уязвимостей конфигурации служб удаленного доступа	+
СУД.1.1	Поиск уязвимостей реализации аутентификации	+
СУД.1.2	Поиск недостатков управления доступом к порту служб удаленного доступа	+
СУД.1.3	Поиск уязвимостей протоколов служб удаленного доступа	+
СУД.1.4	Поиск иных уязвимостей служб удаленного доступа	+

4 Если в информационной системе не применяются информационные технологии, приведенные в наименовании работы не проводятся.

Условное обозначение и номер	Наименование работы	Вид анализа
		С1
СУД.2	Поиск уязвимостей в программном обеспечении служб удаленного доступа	+
СДИ	Службы доменных имен (DNS)	
СДИ.1	Поиск уязвимостей конфигурации службы доменных имен	+
СДИ.1.1	Поиск уязвимостей, связанных с отсутствием проверки и валидации данных	+
СДИ.1.2	Поиск уязвимостей, связанных с недостатками защиты протоколов передачи данных	+
СДИ.1.3	Поиск иных уязвимостей службы доменных имен	+
СДИ.2	Поиск уязвимостей программного обеспечения DNS-сервера	+
ИСС	Иные сетевые сервисы и службы	
ИСС.1	Поиск уязвимостей конфигурации иных сетевых сервисов и служб	+
ИСС.2	Поиск уязвимостей программного обеспечения сетевых сервисов и служб	+
ВЕБ	Веб-приложения	
ВЕБ.1	Поиск уязвимостей конфигурации веб-приложений	+
ВЕБ.1.1	Поиск уязвимостей идентификации и аутентификации пользователей	+
ВЕБ.1.2	Поиск уязвимостей управления доступом пользователей к ресурсам	+
ВЕБ.1.3	Поиск уязвимостей, связанных с возможностью запуска произвольного программного кода	+
ВЕБ.1.4	Поиск уязвимостей в управлении ресурсами, доступными веб-приложению	+
ВЕБ.1.5	Поиск уязвимостей, связанных с недостатками проверки вводимых данных	+
ВЕБ.1.6	Поиск уязвимостей реализации криптографических механизмов	+
ВЕБ.1.7	Поиск неправильной конфигурации приложения (например, включенный режим отладки)	+
ВЕБ.1.8	Поиск небезопасной конфигурации веб-сервера	+
ВЕБ.1.9	Поиск иных уязвимостей конфигурации веб-приложений	+
ВЕБ.2	Поиск уязвимостей в программном обеспечении веб-	+

Условное обозначение и номер	Наименование работы	Вид анализа
		С1
	приложений (например, в веб-сервере, CMS, фреймворках и иных компонентах)	
ДИС	Доменные инфраструктурные службы	
ДИС.1	Поиск уязвимостей конфигурации доменных инфраструктурных служб	+
ДИС.1.1	Поиск уязвимостей реализации идентификации и аутентификации пользователей	+
ДИС.1.2	Поиск уязвимостей управления и разграничения доступом	+
ДИС.1.3	Поиск иных уязвимостей конфигурации домена	+
ДИС.2	Поиск уязвимостей в программном обеспечении доменных служб	+
МОБ	Мобильные приложения	
МОБ.1	Поиск уязвимостей конфигурации мобильных приложений	+
МОБ.1.1	Поиск уязвимостей в реализации функций идентификации и аутентификации пользователей	+
МОБ.1.2	Поиск уязвимостей в реализации функций управления доступом	+
МОБ.1.3	Поиск уязвимостей, связанных с небезопасным хранением данных на мобильном устройстве	+
МОБ.1.4	Поиск уязвимостей, связанных с возможностью запуска произвольного программного кода	+
МОБ.1.5	Поиск уязвимостей, связанных с некорректной работой с памятью	+
МОБ.1.6	Поиск уязвимостей защиты протоколов передачи данных	+
МОБ.1.7	Поиск иных уязвимостей конфигурации мобильных приложений	+
МОБ.2	Поиск уязвимостей программного обеспечения мобильных приложений	+
МИИ	Модели машинного обучения	
МИИ.1	Поиск уязвимостей конфигурации модели машинного обучения	+
МИИ.1.1	Поиск уязвимостей, позволяющих исказить поведение модели машинного обучения путем формирования специальных запросов (промптов)	+
МИИ.1.2	Поиск уязвимостей, связанных с использованием для обучения	+

Условное обозначение и номер	Наименование работы	Вид анализа
		С1
	модели машинного обучения модифицированных данных или наборов данных	
МИИ.1.3	Поиск уязвимостей, позволяющих в результате ответа модели машинного обучения получить конфиденциальную информацию	+
МИИ.1.4	Поиск уязвимостей контроля и управления данными, используемыми моделью машинного обучения	+
МИИ.1.5	Поиск уязвимостей, позволяющих модифицировать обучающие наборы данных	+
МИИ.1.6	Поиск уязвимостей управления доступом к модели машинного обучения	+
МНИ.1.7	Поиск уязвимостей механизмов фильтрации и контроля входных и выходных данных модели машинного обучения	+
МИИ.1.8	Поиск прочих уязвимостей конфигурации модели машинного обучения	+

Знаком «+» отмечены необходимые работы для каждого из видов анализа.

3.3. Внутренний анализ уязвимостей

3.3.1. Работы по внутреннему анализу уязвимостей должны предусматривать выявление уязвимостей программных, программно-аппаратных средств, включая уязвимости сетевых служб и сервисов, системного и прикладного программного обеспечения, расположенных во внутренней инфраструктуре информационной системы, а также уязвимостей, связанных с недостатками их конфигурации.

3.3.2. В целях проведения внутреннего анализа уязвимостей осуществляются:

а) выявление известных уязвимостей в программных, программно-аппаратных средствах, входящих в состав внутренней инфраструктуры информационной системы;

б) выявление уязвимостей конфигурации системного и прикладного программного обеспечения, входящего в состав внутренней инфраструктуры информационной системы;

в) выявление уязвимостей аутентификации, использования паролей, заданных по умолчанию, и устойчивости паролей;

г) выявление уязвимостей кода и конфигурации прикладного программного обеспечения (веб-приложений, мобильных приложений, программного обеспечения, реализующего модели машинного обучения и другого прикладного программного обеспечения).

3.3.3. Внутренний анализ уязвимостей проводится исполнителем:

путем сканирования интерфейсов внутренней инфраструктуры информационной системы, автоматизированных рабочих мест пользователей информационной системы, серверов, телекоммуникационного оборудования, средств защиты информации с использованием средств выявления уязвимостей, иных инструментальных средств, предназначенных для поиска уязвимостей программного кода и конфигурации с использованием пассивных и активных методов анализа уязвимостей в автоматизированном режиме;

путем поиска информации об уязвимостях программных, программно-аппаратных средств, средств защиты информации, входящих в состав информационной системы, в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также в иных базах данных уязвимостей;

путем применения пассивных и активных методов анализа уязвимостей в ручном режиме.

3.3.4. По результатам проведения внутреннего анализа исполнителем формируется перечень уязвимостей внутренней инфраструктуры информационной системы:

а) уязвимости программного обеспечения автоматизированных рабочих мест пользователей информационной системы, серверов, телекоммуникационного оборудования, средств защиты информации;

б) уязвимости конфигурации автоматизированных рабочих мест пользователей информационной системы, серверов, телекоммуникационного оборудования, средств защиты информации;

в) уязвимости системного и прикладного программного обеспечения;

г) уязвимости конфигурации системного и прикладного программного обеспечения (операционных систем, систем управления базами данных, сетевых служб, сервисов, веб-приложений, серверов приложений и иного программного обеспечения);

д) уязвимости конфигурации внутренней сетевой инфраструктуры информационной системы;

е) уязвимости программируемых логических контроллеров, средств автоматизации технологических процессов и «умных» устройств.

3.3.5. Перечень работ, проводимых исполнителем в ходе внутреннего сканирования, приведен в таблице 3.

Таблица 3

Условное обозначение и номер работы	Наименование работы[5]	Вид анализа
		С2
Внутреннее сканирование		
УСИ	Сетевая инфраструктура	
УСИ.1	Поиск уязвимостей программного обеспечения телекоммуникационного оборудования и межсетевых экранов	+
УСИ.2	Поиск уязвимостей конфигурации сетевых служб и протоколов (ARP, BOOTP, CDP, DTP, LLD, LLMNR, mDNS, MNDP, NDP, STP, SSDP, VRRP и HSRP, VTP и других протоколов)	+
УСИ.3	Поиск уязвимостей, связанных с использованием паролей, заданных по умолчанию	+
УСИ.4	Поиск уязвимостей механизмов аутентификации (передача аутентификационной информации в открытом виде и других механизмов аутентификации)	+
УСИ.5	Поиск уязвимостей управления доступом к файлам и каталогам, к интерфейсам управления сетевыми службами и устройствам	+
УСИ.6	Поиск уязвимостей, связанных с отсутствием блокировки учётной записи после неудачных попыток входа	+
УСИ.7	Поиск активных сетевых служб, использующих небезопасные протоколы передачи данных (FTP, Telnet, rlogin, rsh, Finger и других служб)	+
УСИ.8	Поиск небезопасных версий сетевых протоколов (SMBv1, SSL 2.0/3.0, TLS 1.0, NTLMv1)	+
СУД	Службы удаленного доступа	
СУД.1	Поиск уязвимостей конфигурации служб удаленного доступа	+
СУД.1.1	Поиск уязвимостей реализации аутентификации	+
СУД.1.2	Поиск недостатков управления доступом к порту служб удаленного доступа	+
СУД.1.3	Поиск уязвимостей защиты протоколов служб удаленного доступа	+
СУД.1.4	Поиск иных уязвимостей конфигурации служб удаленного доступа	+
СУД.2	Поиск уязвимостей в программном обеспечении служб удаленного доступа	+

5 Если в информационной системе не применяются информационные технологии, приведенные в наименовании работы не проводятся.

Условное обозначение и номер	Наименование работы	Вид анализа
		С2
СДИ	Службы доменных имен (DNS)	
СДИ.1	Поиск уязвимостей конфигурации службы доменных имен	+
СДИ.1.1	Поиск уязвимостей, связанных с отсутствием проверки и валидации данных	+
СДИ.1.2	Поиск уязвимостей, связанных с недостатками защиты протоколов передачи данных	+
СДИ.1.3	Поиск иных уязвимостей службы доменных имен	+
СДИ.2	Поиск уязвимостей программного обеспечения DNS-сервера	+
ИСС	Иные сетевые сервисы и службы	+
ИСС.1	Поиск уязвимостей конфигурации иных сетевых сервисов и служб	+
ИСС.2	Поиск уязвимостей программного обеспечения сетевых сервисов и служб	+
ДИС	Доменные инфраструктурные службы	
ДИС.1	Поиск уязвимостей конфигурации домена информационной системы	+
ДИС.1.1	Поиск уязвимостей реализации идентификации и аутентификации пользователей	+
ДИС.1.2	Поиск уязвимостей управления и разграничения доступом	+
ДИС.1.3	Поиск иных уязвимостей конфигурации домена	+
ДИС.2	Поиск уязвимостей в программном обеспечении доменных инфраструктурных служб	+
ОПС	Операционные системы	
ОПС.1	Поиск уязвимостей конфигурации операционных систем	+
ОПС.1.1	Поиск учетных записей пользователей, заданных по умолчанию, или с простым паролем	+
ОПС.1.2	Поиск уязвимостей парольной политики	+
ОПС.1.3	Поиск уязвимостей управления доступом пользователей	+
ОПС.1.4	Поиск уязвимостей, связанных с отсутствием блокировки учётной записи при многократных ошибках ввода пароля	+

Условное обозначение и номер	Наименование работы	Вид анализа
		С2
ОПС.1.5	Поиск уязвимостей, связанных с применением одинакового пароля для локальных администраторов на всех автоматизированных рабочих местах	+
ОПС.1.6	Поиск присвоения учетным записям пользователей избыточных прав администратора	+
ОПС.1.7	Поиск присвоения учетным записям пользователей избыточных прав на системные каталоги или файлы	+
ОПС.1.8	Поиск неиспользуемых служб и сервисов (Telnet, FTP, rlogin, SNMP без шифрования и других служб и сервисов)	+
ОПС.1.9	Поиск применения устаревших протоколов (SMBv1, NTLMv1, SSL 2.0/3.0, TLS 1.0 и других протоколов)	+
ОПС.1.10	Поиск реализации неограниченного доступа к службам удалённого доступа (RDP, SSH и других служб) для всех IP-адресов	+
ОПС.1.11	Поиск уязвимостей, связанных с отсутствием логирования событий безопасности	+
ОПС.1.12	Поиск уязвимостей, связанных с использованием гостевых или общих папок без ограничений	+
ОПС.1.13	Поиск уязвимостей, связанных с применением автозагрузки с неучтенных машинных носителей	+
ОПС.1.14	Поиск уязвимостей, связанных с отсутствием ограничений для макросов в офисных приложениях	+
ОПС.1.15	Поиск иных уязвимостей конфигурации операционных систем	+
ОПС.2	Поиск уязвимостей программного обеспечения операционных систем	+
СУБД	Системы управления базами данных	
СУБД.1	Поиск уязвимостей конфигурации систем управления базами данных	+
СУБД.1.1	Поиск учетных записей пользователей, заданных по умолчанию, или с простым паролем (например, `root`/`sa` с пустым паролем)	+
СУБД.1.2	Поиск уязвимостей парольной политики	+
СУБД.1.3	Поиск применения одинаковых паролей у администраторов	+
СУБД.1.4	Поиск неиспользуемых учетных записей	+
СУБД.1.5	Поиск неограниченного количества подключений с любых IP-	+

Условное обозначение и номер	Наименование работы	Вид анализа
		С2
	адресов (например, root@’%’ в MySQL)	
СУБД.1.6	Поиск уязвимостей, связанных с наличием у пользователей всех прав и полномочий (реализован принцип «Full Access»)	+
СУБД.1.7	Поиск уязвимостей, связанных с использованием одинаковых учетных записей для разных приложений	+
СУБД.1.8	Поиск уязвимостей, связанных с наличием у учетных записей прав на изменение системных таблиц	+
СУБД.1.9	Поиск уязвимостей, связанных с реализацией доступа к системе управления базами данных со всех интерфейсов (0.0.0.0)	+
СУБД.1.10	Поиск уязвимостей, связанных с отсутствием ограничений доступа к системе управления базами данных по IP-адресам	+
СУБД.1.11	Поиск уязвимостей, связанных с отсутствием шифрования учетных данных пользователей и защищаемой информации	+
СУБД.1.12	Поиск уязвимостей, связанных с использованием устаревших протоколов или небезопасных параметров SSL/TLS	+
СУБД.1.13	Поиск уязвимостей, связанных с доступностью журналов аудита всем пользователям	+
СУБД.1.14	Поиск уязвимостей, связанных с отсутствием ограничений на число попыток ввода пароля	+
СУБД.1.15	Поиск уязвимостей, связанных с отсутствием контроля доступа пользователей к каталогам, файлам баз данных	+
СУБД.1.16	Поиск иных уязвимостей конфигурации систем управления базами данных	+
СУБД.1.17	Поиск уязвимостей программного обеспечения систем управления базами данных	+
СВИ	Средства виртуализации	
СВИ.1	Поиск уязвимостей конфигурации средств виртуализации	+
СВИ.1.1	Поиск учетных записей пользователей, заданных по умолчанию, или с простым паролем	+
СВИ.1.2	Поиск возможности доступа к интерфейсам управления из любой сети (подсети)	+
СВИ.1.3	Поиск уязвимостей, связанных с отсутствием ограничений на количество ресурсов, выделяемых виртуальным машинам (CPU, память)	+
СВИ.1.4	Поиск уязвимостей, связанных с использованием общих каталогов для хранения информации разного уровня конфиденциальности	+

Условное обозначение и номер	Наименование работы	Вид анализа
		С2
СВИ.1.5	Поиск бесконтрольного использования снимков состояний (снапшотов) виртуальных машин	+
СВИ.1.6	Поиск отсутствия изоляции между виртуальными машинами	+
СВИ.1.7	Поиск уязвимостей конфигурации виртуальных коммутаторов и маршрутизаторов	+
СВИ.1.8	Поиск отсутствия фильтрации трафика между виртуальными машинами	+
СВИ.1.9	Поиск иных уязвимостей конфигурации средств виртуализации	+
СВИ.1.10	Поиск уязвимостей программного обеспечения средств виртуализации	+
СКО	Средства контейнеризации	+
СКО.1	Поиск уязвимостей конфигурации средств контейнеризации	+
СКО.1.1	Поиск уязвимостей, связанных с возможностью запуска контейнеров с флагом --privileged	+
СКО.1.2	Поиск уязвимостей, связанных с возможностью монтирования чувствительных директорий хостовой операционной системы (/etc, /var/run/docker.sock)	+
СКО.1.3	Поиск уязвимостей, связанных с возможностью запуска процессов внутри контейнера от имени привилегированных учетных записей (root)	+
СКО.1.4	Поиск уязвимостей, связанных с применением образов контейнеров, содержащих уязвимости	+
СКО.1.5	Поиск уязвимостей, связанных с отсутствием у контейнеров ограничений по ресурсам (--cpus, --memory)	+
СКО.1.6	Поиск уязвимостей, связанных с возможностью запуска контейнеров в hostNetwork/hostPID режиме	+
СКО.1.7	Поиск уязвимостей, связанных с отсутствием политик сетевого взаимодействия между контейнерами	+
СКО.1.8	Поиск уязвимостей, связанных с отсутствием ограничений по доступу к сервисам, содержащимся в контейнерах (NodePort/LoadBalancer)	+
СКО.1.9	Поиск иных уязвимостей конфигурации средств контейнеризации	+
СКО.2	Поиск уязвимостей программного обеспечения средств контейнеризации	+

Условное обозначение и номер	Наименование работы	Вид анализа
		С2
ВЕБ	Веб-серверы	
ВЕБ.1	Поиск уязвимостей конфигурации веб-приложений	+
ВЕБ.1.1	Поиск уязвимостей идентификации и аутентификации пользователей	+
ВЕБ.1.2	Поиск уязвимостей управления доступом пользователей к ресурсам	+
ВЕБ.1.3	Поиск уязвимостей, связанных с возможностью запуска произвольного программного кода	+
ВЕБ.1.4	Поиск уязвимостей в управлении ресурсами, доступными веб-приложению	+
ВЕБ.1.5	Поиск уязвимостей, связанных с недостатками проверки вводимых данных	+
ВЕБ.1.6	Поиск уязвимостей реализации криптографических механизмов	+
ВЕБ.1.7	Поиск уязвимостей, связанных с неправильной конфигурацией приложения (например, включенный режим отладки)	+
ВЕБ.1.8	Поиск небезопасной конфигурации веб-сервера	+
ВЕБ.1.9	Поиск иных уязвимостей конфигурации веб-приложений	+
ВЕБ.2	Поиск уязвимостей в программном обеспечении веб-приложений (например, в веб-сервере, CMS, фреймворках и иных компонентах)	+
ПРИ	Прикладное программное обеспечение	
ПРИ.1	Поиск уязвимостей конфигурации прикладного программного обеспечения (офисные программы, интернет-браузеры, системы электронного документооборота и другое программное обеспечение)	+
ПРИ.2	Поиск уязвимостей прикладного программного обеспечения	+
МИИ	Модели машинного обучения	
МИИ.1	Поиск уязвимостей конфигурации модели машинного обучения	+
МИИ.1.1	Поиск ошибок, позволяющих исказить поведение обученной модели машинного обучения путем формирования специальных запросов (промптов)	+

Условное обозначение и номер	Наименование работы	Вид анализа
		С2
МИИ.1.2	Поиск уязвимостей, связанных с использованием для обучения модели машинного обучения модифицированных данных или наборов данных	+
МИИ.1.3	Поиск уязвимостей, позволяющих в результате ответа модели машинного обучения получить конфиденциальную информацию	+
МИИ.1.4	Поиск уязвимостей контроля и управления данными, используемыми моделью машинного обучения	+
МИИ.1.5	Поиск уязвимостей, позволяющих модифицировать обучающие наборы данных	+
МИИ.1.6	Поиск уязвимостей управления доступом к модели машинного обучения	+
МНИ.1.7	Поиск уязвимостей механизмов фильтрации и контроля входных и выходных данных модели машинного обучения	+
МИИ.1.8	Поиск прочих уязвимостей конфигурации модели машинного обучения	+
МИИ.2	Поиск уязвимостей модели машинного обучения	+
МИИ.2.1	Поиск уязвимостей программного обеспечения библиотек, фреймворков, используемых для разработки модели машинного обучения	+
МИИ.2.2	Поиск уязвимостей программного обеспечения модели машинного обучения	+

Знаком «+» отмечены необходимые работы для каждого из видов анализа.

3.4. Оценка выявленных уязвимостей

3.4.1. На этапе оценки выявленных уязвимостей проводится оценка уровня критичности выявленных уязвимостей информационной системы и возможности реализации с их использованием угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий.

3.4.2. В случае если по результатам проведенного анализа не выявлено уязвимостей информационной системы, исполнителем выдается положительное заключение по результатам анализа уязвимостей в информационной системе заказчика (оператора).

3.4.3. В случае если по результатам проведенного анализа выявлены уязвимости информационной системы, исполнителем совместно с заказчиком (оператором) проводится оценка уровня критичности выявленных уязвимостей информационной системы в соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30 июня 2025 г.

3.4.4. Заказчиком (оператором) в ходе проведения анализа уязвимостей должны быть приняты меры по устранению всех уязвимостей критического и высокого уровней опасности.

3.4.5. В отношение уязвимостей среднего и низкого уровней опасности исполнитель совместно с заказчиком (оператором) проводит экспертную оценку возможности использования указанных уязвимостей потенциальным нарушителем для реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий.

Экспертная оценка возможности эксплуатации выявленных уязвимостей проводится с учетом способов реализации угроз безопасности и возможностей нарушителей, содержащихся в модели угроз безопасности информации информационной системы, а также структурно-функциональных характеристик и особенностей функционирования информационной системы.

Для проведения оценки выявленных уязвимостей заказчик (оператор) представляет исполнителю сведения о способах реализации угроз безопасности информации, сценариях реализации угроз безопасности информации, возможностях нарушителей, а также негативных последствиях от реализации угроз безопасности информации (при наличии).

Заказчиком (оператором) в ходе проведения анализа уязвимостей должны быть приняты меры по устранению уязвимостей среднего и низкого уровней опасности, которые по результатам экспертной оценки могут быть использованы потенциальным нарушителем для реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий.

3.4.6. Уязвимости среднего и низкого уровней опасности, которые по результатам экспертной оценки не могут быть использованы потенциальным нарушителем для реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий, подлежат устранению заказчиком (оператором) после проведения анализа уязвимостей в порядке, установленном в Руководстве по организации процесса управления уязвимостями в органе (организации), утвержденном ФСТЭК России 17 мая 2023 г.

3.4.7. Исполнителем формируются рекомендации по устранению выявленных в ходе анализа уязвимостей, подлежащих устранению в ходе анализа, и принятию мер защиты информации в части:

обновления программного обеспечения;

изменения архитектуры и конфигурации информационной системы;

реализации дополнительных мер защиты информации и (или) установки дополнительных средств защиты информации.

В случае выявления по результатам инвентаризации исполнителем не используемых (не идентифицированных) заказчиком (оператором) сетевых адресов, портов, служб и сервисов, доменных имен, интерфейсов, заказчик (оператор) принимает меры по ограничению доступа к таким сетевым адресам из сети «Интернет», а также по отключению неиспользуемых служб и сервисов.

3.4.8. С учетом выданных исполнителем рекомендаций заказчик (оператор) проводит работы по реализации мер защиты информации, направленных на устранение выявленных уязвимостей, или приводит обоснования невозможности эксплуатации уязвимостей для реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий.

Для устранения уязвимостей информационной системы в приоритетном порядке заказчиком (оператором) принимаются меры по обновлению программного обеспечения.

3.4.9. Исполнитель повторно проводит анализ уязвимостей информационной системы с целью подтверждения устранения заказчиком (оператором) выявленных уязвимостей информационной системы.

3.4.10. В случае, если исполнителем подтверждено, что заказчиком (оператором) приняты меры по устранению выявленных уязвимостей информационной системы, исполнителем выдается положительное заключение по результатам анализа уязвимостей информационной системы.

3.4.11. Если по результатам оценки принятых заказчиком (оператором) мер по устранению выявленных уязвимостей выявлена хотя бы одна уязвимость, эксплуатация которой может привести к реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий, исполнителем выдается отрицательное заключение по результатам анализа уязвимостей в информационной системе заказчика (оператора).

4. Документирование результатов анализа уязвимостей

4.1. По результатам проведения анализа уязвимостей исполнителем разрабатывается отчет или протокол (при проведении аттестационных испытаний) (далее – отчет (протокол)), в котором содержатся сведения о порядке проведения работ, их результатах, а также информация об информационной системе, целях, условиях и границах проведения работ, используемых для анализа методах и средствах.

4.2. Отчет (протокол) должен содержать:

а) сведения об основании для проведения работ, наименования заказчика и исполнителя работ, сроки проведения работ, их цели и задачи;

б) информация об используемых средствах выявления уязвимостей, а также инструментальных средствах;

в) результаты инвентаризации информационной системы, включающие перечень адресов, портов, сетевых служб, сервисов, интерфейсов, а также перечень программного обеспечения, содержащегося в информационной системе;

г) краткое описание процесса проведения внешнего и внутреннего тестирования;

д) перечень выявленных уязвимостей информационной системы, а также описание выявленных уязвимостей с приложением отчетов, сформированных средствами выявления уязвимостей;

е) результаты оценки критичности выявленных уязвимостей информационной системы;

ж) перечень выявленных уязвимостей информационной системы, подлежащих устранению в ходе анализа уязвимостей, с обоснованием необходимости их устранения для предотвращения реализации угроз безопасности информации (векторов атак), приводящих к возникновению негативных последствий;

з) рекомендации исполнителя по устранению выявленных уязвимостей информационной системы;

и) результаты повторного анализа уязвимостей информационной системы, проводимого с целью подтверждения устранения заказчиком (оператором) выявленных уязвимостей информационной системы;

к) ограничения, которые заказчик (оператор) накладывает на действия исполнителя в ходе анализа уязвимостей информационной системы (например, запреты на определенные виды работ, исключение объектов информационной системы из границ проведения работ, непредставление требуемой информации или доступа для подключения к информационной системе).

4.3. Состав и содержание информации в отчете (протоколе) должны обеспечивать заказчику (оператору) возможность установить перечень выявленных уязвимостей информационной системы, определить состав и сроки проведенных работ по выявлению и устранению уязвимостей, а также методов анализа уязвимостей в соответствии с настоящей Методикой. Описанные действия должны быть подтверждены документированными материалами, указывающими на поиск уязвимостей информационной системы (отчетами, скриншотами, текстовыми описаниями).

4.4. Отчет (протокол) подписывается специалистами исполнителя, которые проводили анализ уязвимостей. Организация и руководитель структурного

подразделения, проводившие анализ уязвимостей и разработавшие отчет (протокол), несут ответственность за качество и объективность проведенных работ.