ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ПРОВЕДЕНИЕ РАБОТ ПО ОЦЕНКЕ УРОВНЯ ЗАЩИЩЕННОСТИ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
ООО «КАПИТАЛ ЛАЙФ СТРАХОВАНИЕ ЖИЗНИ»

г. Москва
2024 г.

Оглавление

1. Термины и определения: 3
2. Общие сведения 3
3. Цели и задачи выполнения работ 3
4. Организационные ограничения проекта 4
5. Состав и содержание работ 4
6. Требования к обеспечению процесса проведения Оценки защищенности 5
7. Типы нарушителя 6
8. Требования к Оценке защищенности периметра информационной инфраструктуры 6
9. Требование к Оценке защищенности веб и мобильных приложений 7
10. Требования к отчетной документации 9
11. Требования к содержанию отчетной документации 9
12. Требования к гарантии качества 10
13. Требования к исполнителю 10

Приложение №1 11

1. Термины и определения:

1.1. Общество – Общество с ограниченной ответственностью «Капитал Лайф Страхование Жизни»

1.2. Объект оказания услуг – информационная инфраструктура Заказчика: веб-приложения, включая веб-приложение личного кабинета клиента в сети Интернет, мобильное приложение личного кабинета клиента под управлением Android и iOS, интеграционные системы и API, участвующие во взаимодействии с автоматизированными системами ДБО банка, иные функционально сопряженные инженерные подсистемы Заказчика.

1.3. Недопустимое событие – событие, возникающее в результате действий злоумышленников и делающее невозможным достижение операционных целей страховой организации или приводящее к длительному свыше 4 часов нарушению основной деятельности организации.

1.4. Brute Force - атака методом полного перебора.

1.5. CSRF (Cross-site request forgery) - межсайтовая подделка запроса.

1.6. HTTP (HyperText Transfer Protocol) – протокол передачи гипертекста.

1.7. LDAP (Lightweight Directory Access Protocol) - протокол прикладного уровня для доступа к службе каталогов.

1.8. LFI (Local File Inclusion) - подключения локальных файлов с выводом для чтения на стороне сервера.

1.9. RCE (Remote code execution) - удалённое внедрение кода на сервере.

1.10. RFI (Remote file include) - удалённое выполнение кода на сервере.

1.11. SMTP (Simple Mail Transfer Protocol) - простой протокол передачи почты.

1.12. SQL (Structured Query Language) - язык структурированных запросов.

1.13. SSI (Server Side Includes) - включения на стороне сервера.

1.14. XML (eXtensible Markup Language) - расширяемый язык разметки. Используется для хранения и передачи данных.

1.15. (XQuery) язык запросов и функциональный язык программирования, разработанный для обработки данных в формате XML.

1.16. XSS (Cross-Site Scripting) - межсайтовый скриптинг.

2. Общие сведения

2.1. Работы по оценке уровня (состояния) защищенности информационной инфраструктуры (далее – Работы, Оценка защищенности). Работы включают в себя два этапа:

- оценка защищенности,
- поиск успешных следов компрометации информационной инфраструктуры злоумышленником.

2.2. Срок выполнения работ: 4 месяца с момента заключения договора.

2.3. Работы выполняются на территории Исполнителя и объектах Заказчика, к которым будет предоставлен доступ.

2.4. Оплата осуществляется по факту оказания услуг.

3. Цели и задачи выполнения работ

3.1. Целями выполнения работ является:

- оценка уровня защищенности объектов информационной инфраструктуры Заказчика,

- обеспечение доверия к объектам информационной инфраструктуры Заказчика.
- а также выработка мер по модернизации информационной инфраструктуры.

3.2. В рамках выполнения работ по Оценке защищенности необходимо решить следующие задачи:

- выявление и консолидация недопустимых событий информационной безопасности;
- выявление уязвимостей информационной инфраструктуры, которые могут быть использованы внешними и внутренними нарушителями для осуществления несанкционированных действий, направленных на нарушение свойств конфиденциальности, целостности, доступности обрабатываемой информации, а также технических средств обработки информации, в результате которых может быть нарушен их штатный режим функционирования, что приведет к реализации недопустимых событий;
- выявление недостатков применяемых средств защиты информации и программного обеспечения, а также оценка возможности их использования нарушителем;
- проверка практической возможности использования уязвимостей (на примере наиболее критических);
- получение оценки текущего уровня защищенности на основе объективных свидетельств;
- разработка маршрутной карты по модернизации информационной инфраструктуры, предоставление рекомендаций по устранению критических уязвимостей и повышению уровня защищенности;
- идентификация риска информационной безопасности, включая случаи, когда реализация такого риска приводит к совершению операций без согласия клиента, а также описание его влияния на общую защищенность и формирование рекомендаций по минимизации риска.

4. Организационные ограничения проекта

4.1. Все действия Исполнителя, которые могут привести к нарушению функционирования или другим негативным последствиям для Заказчика, согласовываются с Заказчиком заблаговременно.

4.2. После выполнения работ все средства проведения Оценки уровня защищенности, применявшиеся в рамках выполнения работ, удаляются из инфраструктуры.

4.3. Исполнитель предоставляет полную информацию о действиях, выполнявшихся в ходе Оценке защищенности, применявшихся методах атаки, выявленных недостатках и причинах, результатах использования наиболее серьезных недостатков и объективных свидетельствах, подтверждающих как наличие недостатков, так и результаты их использования специалистами Исполнителя.

4.4. При проведении работ Исполнителю со стороны Заказчика не предоставляется доступ к персональным данным клиентов, а также иной информации, составляющей коммерческую тайну, сопряженной с основной деятельностью Заказчика.

4.5. Исполнитель обязан во время проведения работ, а также после их выполнения обеспечить защиту сведений, полученных в рамках выполнения работ по данному ТЗ, в соответствии с законодательством Российской Федерации.

5. Состав и содержание работ

5.1. В целях проведения Оценки защищенности Исполнитель должен выполнить следующие виды работ:

- создание, совместно с Заказчиком, реестра недопустимых событий;
- оценка возможности реализации недопустимых событий путем моделирования целевых атак (тестирование на проникновение);
- оценка мер противодействия моделированию атак со стороны системы защиты информации информационной инфраструктуры Заказчика;
- разработка маршрутной карты по модернизации информационной инфраструктуры с целью повышения уровня защищенности;
- разработка отчетных материалов в соответствии с требованиями к отчетной документации.

5.2. Тестирование на проникновение проводится следующими методами:

- методом «черного ящика», при котором оценщик не владеет информацией об объектах информационной инфраструктуры,
- методом «серого ящика», при котором оценщик владеет частичной информацией об объектах информационной инфраструктуры.

5.3. При проведении тестирования на проникновение Исполнителю рекомендуется использовать базы данных угроз безопасности информации и иные информационные источники для идентификации уязвимостей и формализованного представления результатов (например, БДУ ФСТЭК России[1], CAPEC[2], MITRE ATT&CK[3], OWASP[4], STIX[5], WASC[6], CWE[7], CVE[8] и иные).

5.4. В процессе проведения Оценки защищенности требуется фиксировать фактические результаты выполнения тестирования на проникновение и исследовать причины возникновения любых непредвиденных ситуаций.

5.5. В случае выявления уязвимостей Исполнителю требуется предусмотреть повторное тестирование на проникновение после устранения выявленных уязвимостей. Повторное тестирование на проникновение допускается проводить только для тех объектов информационной инфраструктуры, в которых были выявлены уязвимости.

6. Требования к обеспечению процесса проведения Оценки защищенности

6.1. Для обеспечения выполнения работ по Оценке защищенности Заказчик предоставляет информацию с описанием внешнего периметра информационной инфраструктуры, путем перечисления внешних сервисов компании: не более 20 публичных IP адресов, не более 5 веб-приложений, 2 мобильных приложения личного кабинета клиента под управлением Android и iOS.

6.2. Заказчик обеспечивает Исполнителя беспрепятственной возможностью выполнять работы в режиме 24/7 на протяжении всего срока реализации Оценки защищенности.

6.3. Исполнитель имеет право выполнять работы с любых IP-адресов, расположенных на территории Российской Федерации.

6.4. Исполнитель обязан обеспечить нахождение специалистов автоматизированных средств, используемых для проведения тестирования на проникновение и анализа уязвимостей объектов информационной инфраструктуры, на

[1] Банк данных угроз безопасности информации ФСТЭК России по адресу https://bdu.fstec.ru/threat
[2] Common Attack Pattern Enumerations and Classifications по адресу https://capec.mitre.org
[3] MITRE ATT&CK по адресу https://attack.mitre.org
[4] Open Web Application Security Project по адресу https://owasp.org
[5] Security Threat Information Expression по адресу https://stixproject.github.io
[6] Web Application Security Consortium по адресу https://www.webappsec.org
[7] Common Weakness Enumeration по адресу https://cwe.mitre.org
[8] Common Vulnerabilities and Exposures по адресу https://cve.mitre.org

территории Российской Федерации при проведении тестирования на проникновение и анализа уязвимостей объектов информационной инфраструктуры.

6.5. Сканирование объектов информационной инфраструктуры на наличие уязвимостей информационной безопасности 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. Допускается и рекомендуется применение нескольких средств анализа защищенности от разных производителей.

6.6. Рекомендуется для выявления и описания уязвимостей, информация о которых не включена в средства анализа защищенности, а также для формализованного представления результатов использовать банк данных угроз безопасности информации ФСТЭК России (далее – БДУ ФСТЭК России) и иные базы данных, содержащие сведения об уязвимостях объектов информационной инфраструктуры.

6.7. Дополнительные ограничения могут быть согласованы в рабочем порядке.

7. Типы нарушителя

7.1. В рамках выполнения работ по Оценке защищенности должен моделироваться тип потенциального злоумышленника – нарушитель, не имеющий права доступа в контролируемую (охраняемую) зону и не имеющий физического доступа к средствам автоматизации оцениваемой информационной инфраструктуры (имитация действий внешнего нарушителя).

7.2. При определении и оценке возможностей внешних нарушителей, Исполнитель должен руководствоваться следующим уровнем возможностей нарушителей, предусмотренным Методикой оценки угроз безопасности информации, утвержденной ФСТЭК России от 5 февраля 2021 г., - нарушитель, обладающий средними возможностями.

8. Требования к Оценке защищенности периметра информационной инфраструктуры

8.1. Исполнитель совместно с Заказчиком формирует и согласовывает «Реестр недопустимых событий» путем интервьюирования ответственных лиц.

8.2. Оценка возможности реализации недопустимых событий проводится путем моделирования целевой атаки на инфраструктуру Заказчика, включая следующие действия:

- сбор информации об инфраструктуре для последующего анализа и уточнения областей поиска уязвимостей;
- получение информации о топологии веб-приложений, используемых решений, версиях программного обеспечения, логике работы;
- определение текущего уровня защищённости;
- сканирование узлов сетевого периметра;
- идентификация уязвимостей сетевых служб. Должен быть осуществлен анализ данных, полученных в результате сканирования доступных ресурсов. Должны быть выявлены возможности доступа к ресурсам с использованием интерфейсов управления, удаленного доступа или доступа к СУБД, которые не должны быть доступны пользователям сети, в которой выполняется работа. Должны быть выявлены сетевые службы, использование которых позволяет перехватывать сетевой трафик или осуществлять другие атаки;

- анализ защищенности инфраструктурных служб и приложений (DNS, электронная почта и т. д.). Должно быть установлено наличие или отсутствие уязвимостей инфраструктурных служб и приложений;
- поиск и анализ информации из открытых источников, содержащей «чувствительные» сведения, способствующие проведению атак на рассматриваемые ИС (информация из баз утечек аутентификационных данных, информация о выявленных ранее уязвимостях, конфигурационные файлы и файлы журналов аудита, размещенные на общедоступных ресурсах и др.);
- оценка защищенности сети от атак на канальном уровне. Должно быть установлено наличие или отсутствие недостатков в реализации сетевой инфраструктуры, а также в использовании протоколов канального и сетевого уровней, которые могут быть использованы для проведения атак;
- подбор паролей. Должен быть осуществлен подбор словарных паролей пользователей;
- анализ технологий и средств защищённого обмена информацией между пользователями;
- определение возможных векторов атак на основании выявленных уязвимостей;
- проверка возможных векторов атак реализации недопустимых событий.

8.3. В рамках выполнения работ по оценке защищенности периметра должны быть решены следующие задачи:

- проверка возможности эксплуатации наиболее опасных уязвимостей с целью выхода за границы заданного сегмента ИС. Должна быть установлена возможность или невозможность получения доступа специалистами Исполнителя к критически важным ИС. Данный этап заканчивается проверкой возможности получения доступа к одному или нескольким компонентам ИС или исчерпанием Исполнителем применимых методов развития атаки.
- сбор информации. Должен быть составлен перечень узлов внутренней сети, доступных из определенного Заказчика и подведомственных учреждений для выполнения работ сегмента сети ИС. Должен быть проведен анализ механизма получения IP-адреса в сети и возможности подключения сторонних устройств. Должен быть осуществлен анализ сегментации сети;
- инвентаризация узлов, доступных из текущего сегмента ИС, без сканирования на наличие уязвимостей, определение типов устройств, операционных систем, приложений по реакции на внешнее воздействие. Должен быть составлен перечень идентифицированных сервисов на узлах, вошедших в границы выполняемых работ;
- выявление недостатков в управлении доступом. Должны быть выявлены ресурсы, к которым удалось получить доступ с использованием согласованного вектора атаки.

9. Требование к Оценке защищенности веб и мобильных приложений

9.1. В процессе выполнения работ Исполнителю рекомендуется руководствоваться пунктом 7.2.6 «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, а также 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).

9.2. Для веб-приложений должен быть выполнен поиск следующих типов известных уязвимостей:

9.2.1. некорректная обработка пользовательского ввода, которая позволяет проводить следующие виды атак:

- внедрение операторов языка SQL (англ. SQL injection), в том числе межмодульное (англ. Second order);
- межсайтовое выполнение сценариев (Cross-Site Scripting);
- подделка межсайтового запроса (Cross-Site Request Forgery);
- включение локальных и удаленных файлов (англ. LFI/RFI/RCE);
- внедрение кода на языке, интерпретируемом на стороне клиента (англ. XSS), в том числе межмодульное (англ. Stored) и клиентское (англ. DOM-based);
- внедрение команд, интерпретируемых средой выполнения (англ. Eval injection);
- внедрение команд, интерпретируемых ОС сервера (англ. OS command injection);
- внедрение SMTP-команд;
- внедрение директив SSI;
- внедрение конструкций языка запросов LDAP;
- внедрение конструкций языка запросов XPath/XQuery;
- внедрение разметки на языке XML;
- внедрение заголовков (Header Injection), в том числе позволяющие разделить HTTP-ответ;
- подключение внешних XML-сущностей (англ. XML External Entity);
- прочие атаки, целью которых является выполнение кода на стороне сервера;
- атака на переполнение буфера применяемых программных и программно-аппаратных компонентов ИС;

9.2.2. небезопасная реализация загрузки пользовательских файлов на сервер (англ. Unrestricted Upload of File with Dangerous Type);

9.2.3. отсутствие проверки или некорректная проверка привилегий пользователя при доступе к закрытым функциям или ресурсам (англ. Insufficient authorization);

9.2.4. ошибки в протоколе проверки подлинности пользователей (англ. Insufficient authentication);

9.2.5. уязвимости в процедуре восстановления доступа при утере учетных данных (англ. Insufficient password recovery);

9.2.6. уязвимости в организации безопасного соединения (англ. Insufficient Transport Layer Protection);

9.2.7. уязвимости, связанные с некорректным управлением сеансами (англ. Insufficient Session Expiration);

9.2.8. возможность несанкционированного выполнения запросов от имени пользователей (англ. CSRF);

9.2.9. возможность вызвать отказ в обслуживании (англ. Denial of Service) без применения методов валовой посылки запросов;

9.2.10. некорректная обработка исключительных ситуаций, приводящая к утечке информации о приложении (англ. Information Leakage);

9.2.11. выявление общеизвестных уязвимостей в ИС;

9.2.12. выявление ошибок конфигурации в ИС;

9.2.13. поиск уязвимостей в ИС, связанных с некорректной обработкой входных данных от пользователей;

9.2.14. выявление уязвимостей, связанных с логикой работы ИС;

9.2.15. расщепление запроса HTTP, сокрытие ответа HTTP;

9.2.16. открытое перенаправление;

9.2.17. раскрытие информации о директориях/сценариях;

9.2.18. предсказуемое расположение ресурсов;

9.2.19. идентификация приложений;

9.2.20. чтение произвольных файлов;

9.2.21. обратный путь в директориях;

9.2.22. раскрытие защищаемой информации;

9.2.23. загрузка и выполнение произвольного кода;

9.2.24. подмена контента;

9.2.25. недостатки защиты от атак типа Clickjacking;

9.2.26. недостатки защиты от атак на функции форматирования строк;

9.2.27. уязвимости клиентских плагинов;

9.2.28. выявление других свойств ИС, негативно влияющих на безопасность (hardening);

9.2.29. прочие ошибки, позволяющие изменить логику работы ИС.

9.3. При проведении оценки защищенности мобильных приложений необходимо организовать проведение следующих мероприятий:

9.3.1. проверка наличия защищаемой информации в файлах данных, журналах регистрации событий, в оперативной памяти устройства, а также передачи защищаемой информации в незашифрованном виде;

9.3.2. проверка возможности чтения ключей шифрования и электронной подписи, а также записи и замены сертификатов ключей;

9.3.3. идентификация протоколов взаимодействия и проверка возможности принудительного навязывания устройству использования незащищенных версий протоколов (HTTP вместо HTTPS, TELNET вместо SSH, SSH1 вместо SSH2);

9.3.4. проверка корректности обработки мобильным приложением входящих параметров, в том числе с использованием значений различной длины, дублирование отдельных параметров с присвоением им разных значений, включение в значения параметров специальных символов, команд операционной системы, операторов интерпретируемых языков программирования;

9.3.5. проверка наличия в мобильном приложении средств защиты от исследования и возможность неавторизованного доступа к интерфейсу программирования приложений.

10. Требования к отчетной документации

10.1. Комплект отчетной документации должен быть предоставлен Заказчику в двух экземплярах: один утвержденный экземпляр на бумажном носителе, второй экземпляр в электронном виде, подписанный электронно-цифровой подписью. Отчет, оформленный в электронном виде, должен быть представлен в формате, не допускающем его редактирования, и снабжен усиленной квалифицированной электронной подписью руководителя организации, сертификат ключа проверки которой действует не менее 5 лет.

10.2. Вся разрабатываемая отчетная документация должна быть выполнена на русском языке.

11. Требования к содержанию отчетной документации

11.1. Результаты тестирования на проникновение и анализа уязвимостей оформляются отчетом, рекомендуемая форма которого приведена в приложении к настоящему техническому заданию.

12. Требования к гарантии качества

14.1. Срок предоставления гарантии качества выполненных работ составляет 12 месяцев со дня подписания документа о приемке выполненных работ (оказанных услуг).

14.2. Исполнитель в течение срока предоставления гарантии должен обеспечить своевременное (в срок не более 10 рабочих дней после предоставления Заказчиком всей необходимой для устранения ошибок информации) устранение недочетов и ошибок, выявленных после выполнения работ.

14.3. Факт регистрации заявки о гарантийном случае подтверждается Исполнителем письмом в адрес ответственного представителя Заказчика, в котором указывается дата и время принятия заявки в работу.

13. Требования к исполнителю

14.1. В соответствии с законодательством (Федеральный закон от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации») организация, выполняющие работы по анализу защищенности ИС должна обладать действующей лицензией Федеральной службы по техническому и экспортному контролю России на деятельность по технической защите конфиденциальной информации, включая услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.

14.2. Исполнитель должен обладать необходимым опытом в проведении тестирования на проникновение не менее 3 лет в организациях финансового рынка, подтвержденного не менее чем тремя соответствующими завершенными договорами.

14.3. Исполнитель должен обладать необходимыми кадровыми ресурсами соответствующей квалификации для реализации данной работы. Исполнитель обязан подтвердить наличие опыта не менее 3 лет привлекаемых специалистов в проведении тестирования на проникновение.

14.4. Квалификация специалистов и архитекторов информационной безопасности подтверждается наличием профильного образования и опытом реализации.

Приложение №1
к Техническому заданию

Рекомендуемая форма отчета о тестировании на проникновение и анализе уязвимостей

Отчет по результатам тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры ООО «Капитал Лайф Страхование Жизни»

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;

реквизиты Заказчика и Исполнителя;

Ф.И.О. и должности исполнителей тестирования на проникновение;

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

дополнительная информация, предоставленная для проведения тестирования на проникновение;

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 успешной эксплуатации уязвимостей;

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

виды тестирования на проникновение с указанием объектов тестирования;

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

2. Раздел «Методология проведения тестирования на проникновение»:

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

описание условий и обобщенных результатов проведения тестирования на проникновение.

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;

IP-адрес объекта сканирования, DNS-имя (при наличии) и любая дополнительная информация, позволяющая однозначно идентифицировать информационную систему или ее 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.