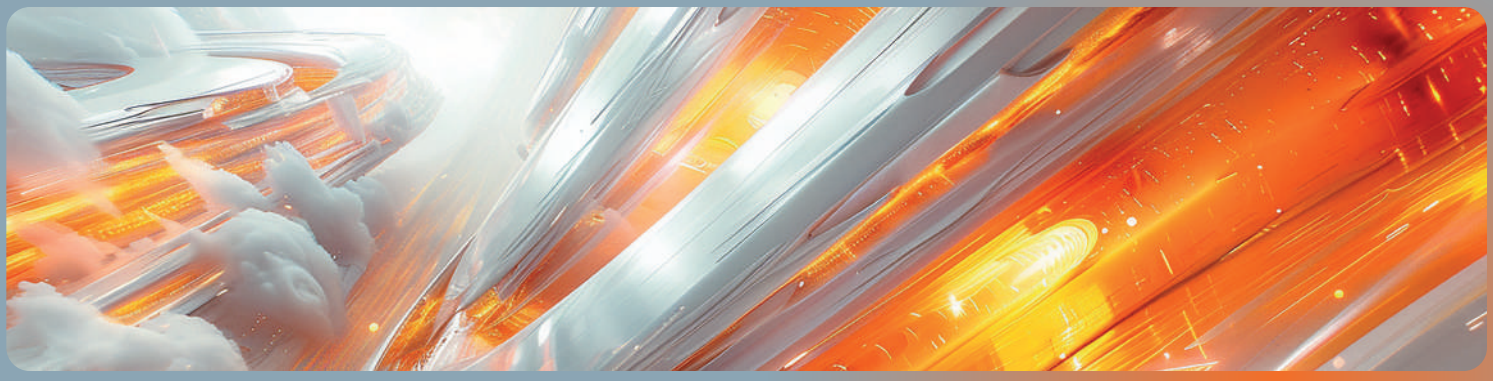
ANGARA SECURITY

ЛАНДШАФТ УГРОЗ ГЛАЗАМИ ПЕНТЕСТЕРА: ИТОГИ 2025 ГОДА

КОМАНДА ПО ПЕНТЕСТУ И АНАЛИЗУ ЗАЩИЩЕННОСТИ ANGARA SECURITY ПОДВЕЛА ИТОГИ 2025 ГОДА.

Специалисты проанализировали портфель выполненных проектов по тестированию на проникновение, чтобы на основе реального опыта выявить ключевые тенденции и найти ответы на следующие вопросы:

1. Какие услуги по пентесту и анализу защищённости были наиболее востребованы?
2. Насколько защищены инфраструктуры и насколько зрелы процессы ИБ у заказчиков?
3. Какие векторы атак и уязвимости встречались чаще всего?
4. К чему готовиться в 2026 году?



ПОРТРЕТ КЛИЕНТА

Аналитики Angara Security изучили отраслевую структуру спроса. В течение года к экспертам обращались заказчики из различных сфер бизнеса.

Наибольшую долю составили:

- Финансы и финтех
- Коммерческие организации
- Телеком и ИТ
- Ритейл
- Промышленность

Менее представленными оказались отрасли туризма, логистики, образования, медиа, а также небольшие сервисные компании. Как отмечают специалисты, в этих сегментах преобладали разовые проверки.

Таким образом, результаты анализа отражают специфику достаточно распространённых отраслей, представители которых в первую очередь заинтересованы в обеспечении высокого уровня информационной безопасности своих инфраструктур.

Особо эксперты отмечают ежегодный рост зрелости в части информационной безопасности у крупных компаний из секторов «Финансы и финтех» и «Телеком и ИТ». Эта тенденция напрямую влияет на усложнение проектов, что предъявляет высокие требования к профессиональному уровню специалистов по пентесту и их способности проявлять творческий подход к поиску и реализации векторов атак.

ПРОЕКТЫ И УСЛУГИ

Исследование показало, что основной спрос в 2025 году был сосредоточен на комплексных проектах, включающих сразу несколько услуг. Распределение проектов по типам демонстрирует, что компании всё чаще стремятся получить целостное представление о защищённости, а не ограничиваются точечной проверкой одного из периметров.

Распределение проектов по типам по данным аналитиков Angara Security:

- Внешний пентест – 14%
- Внутренний пентест – 12%
- Комплексные проекты – 51%
- Анализ защищенности веб-приложений – 23%

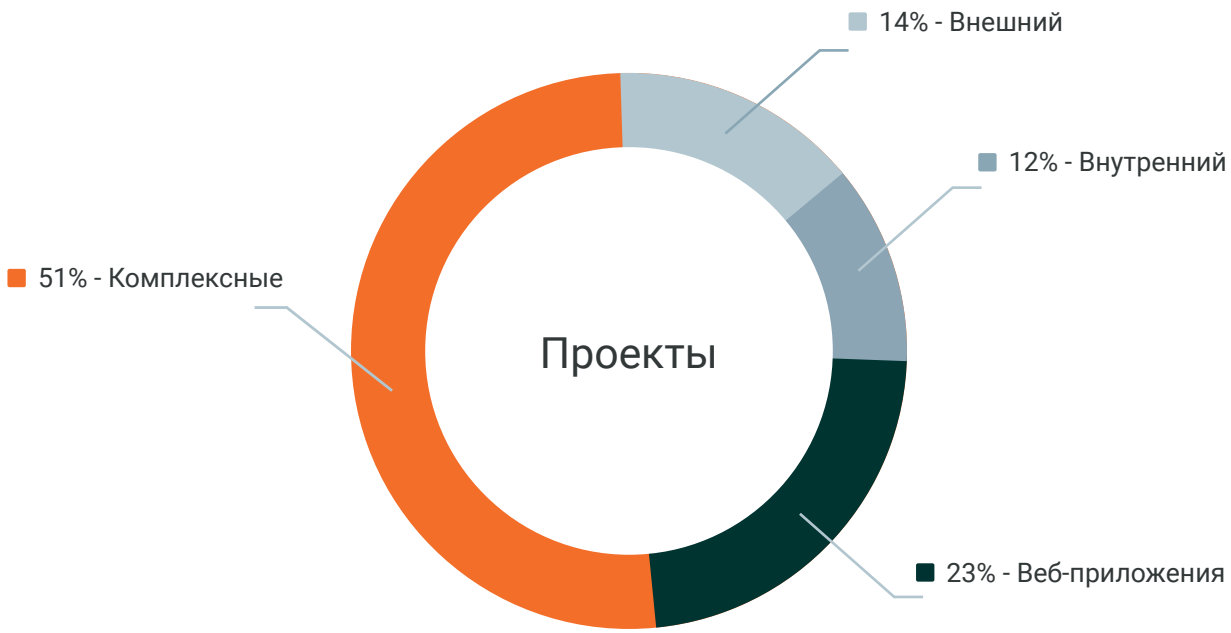


Рисунок 1. Распределение проектов по типам

Как отмечают эксперты, комплексные проекты были наиболее востребованы компаниями из секторов «Финансы и финтех», тогда как представители «Ритейла» и коммерческих организаций чаще выбирали анализ защищенности веб-приложений, для которых характерны различные интеграции и личные кабинеты.

В состав комплексных проектов входили:

- внешнее и внутреннее тестирование на проникновение как базовые составляющие;
- анализ защищенности веб-приложений;
- социотехническое тестирование;
- анализ защищенности беспроводных сетей.

Распределение услуг по всем типам проектов:

- Внешнее тестирование на проникновение – 47%
- Внутреннее тестирование на проникновение – 27%
- Анализ защищенности веб-приложений – 17%
- Социотехническое тестирование – 9%

Рисунок 2. Распределение услуг по всем типам проектов

Внутреннее тестирование на проникновение в 90% проектов проводилось экспертами компании очно на территории заказчика и в половине случаев требовало проведения анализа защищённости беспроводных сетей.

Аналитики обращают внимание, что доля услуг по анализу защищённости веб-приложений остаётся относительно небольшой. С одной стороны, это может свидетельствовать о признаках зрелости процессов безопасной разработки и формировать мнение, что анализ защищённости веб-приложений является избыточным. Однако специалисты предлагают и другую версию: заказчики выбирают менее затратный подход и ограничиваются базовым анализом веб-приложений в рамках внешнего тестирования периметра вместо полноценного анализа, который включает расширенные проверки и исследование бизнес-логики.

Социотехническое тестирование в комплексных проектах, по наблюдениям экспертов, было ограничено проверкой осведомлённости сотрудников и не использовалось для фишинга с целью проникновения во внутренний периметр.

Помимо этого, специалистами Angara Security были выполнены отдельные запросы на оказание нестандартных услуг, таких как:

- анализ защищённости средств разработки;
- выявление нестойких паролей;
- повышение уровня осведомлённости сотрудников о фишинге.

ВНЕШНИЙ ПЕРИМЕТР. ВЫСОКИЙ УРОВЕНЬ ЗАЩИТЫ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Результаты 2025 года демонстрируют высокий уровень защищенности внешних периметров.

Рисунок 3. Уровень защищенности внешнего периметра

В условиях отсутствия возможности применения социальной инженерии и с учётом возросшего уровня кибербезопасности заказчиков пробиться через внешний периметр исключительно техническими методами удавалось крайне редко.

Успешные кейсы, как правило, были связаны:

- с невнимательностью администраторов;
- с ошибками конфигурации сервисов;
- с забытыми или некорректно защищёнными компонентами инфраструктуры.

При этом примерно в 25% проектов экспертам удавалось достичь альтернативных целей внешнего тестирования, например получить доступ к чувствительным данным или обнаружить уязвимости, которые могут быть использованы потенциальными злоумышленниками в сложных сценариях с применением социальной инженерии.

По наблюдениям аналитиков, в основном встречались массовые, хорошо известные классы уязвимостей, критические уязвимости фиксировались крайне редко.

Рисунок 4. Уровень риска уязвимостей внешнего периметра

Наиболее распространённые уязвимости:

1. перечисление пользователей домена через Outlook Web Access;
2. раскрытие служебной информации и деталей конфигурации;
3. ошибки конфигурации веб-сервисов, сетевых сервисов и баз данных;
4. недостаточная защита механизмов аутентификации.

Топ реализованных векторов атак на внешнем периметре:

1. компрометацией учетных данных (Password Spraying, получение паролей пользователей, в том числе доменных учетных данных);
2. получение удалённого доступа через виртуальную частную сеть (VPN);
3. эксплуатация уязвимостей пограничных сервисов, включая уязвимые службы, веб-приложения и базы данных.

Результаты анализа проектов по внешнему периметру показывают, что наиболее результативными векторами атак по-прежнему остаются компрометация учётных данных и ошибки конфигурации сервисов удалённого доступа. Эксперты подчеркивают: даже при высоком уровне технической защищённости периметра человеческий фактор и контроль доступа продолжают играть ключевую роль.

ВНУТРЕННИЙ ПЕРИМЕТР ПО-ПРЕЖНЕМУ ЗОНА ПОВЫШЕННОГО РИСКА

Во внутреннем периметре наблюдается совершенно иная ситуация:

- В **70%** проектов получены привилегии администратора домена Active Directory.
- Только в **7%** случаев не удалось добиться повышения привилегий в инфраструктуре.
- В остальных случаях были достигнуты цели, не связанные с доменной инфраструктурой.

Несмотря на рост зрелости инфраструктур и процессов информационной безопасности, уровень защищённости внутреннего периметра остаётся достаточно низким. Это особенно важно учитывать компаниям, которые привлекают подрядчиков, аутсорсеров и иные категории временных сотрудников для работы с внутренними сервисами.

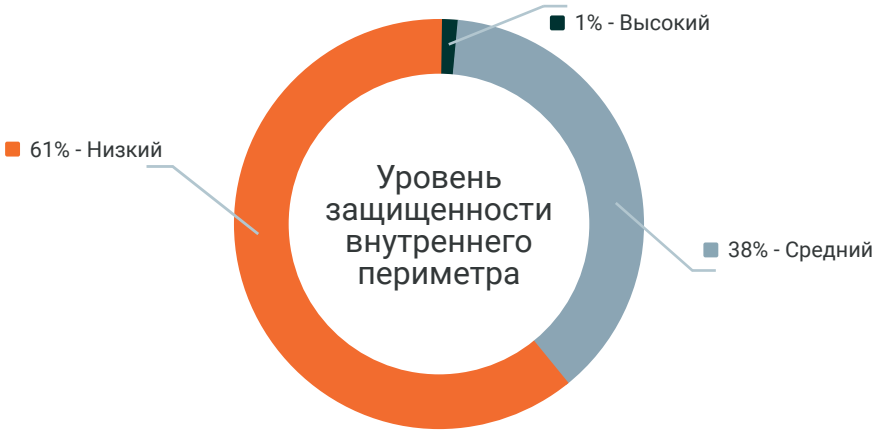


Рисунок 5. Уровень защищенности внутреннего периметра

Внутренний периметр, в отличие от внешнего, богат уязвимостями с высоким уровнем риска, которые встречаются в большинстве проектов уже не первый год.

Рисунок 6. Уровень риска уязвимостей внутреннего периметра

Наиболее распространённые уязвимости во внутреннем периметре:

1. отсутствие подписи (signing) для протоколов LDAP и SMB;
2. перенаправление NTLM-аутентификации (например, CVE-2025-33073);
3. нестойкие и повторно используемые пароли (в том числе учётных записей администраторов и служб);
4. керберос с восстановлением паролей в открытом виде;
5. ошибки конфигурации AD CS (Active Directory Certificate Services).

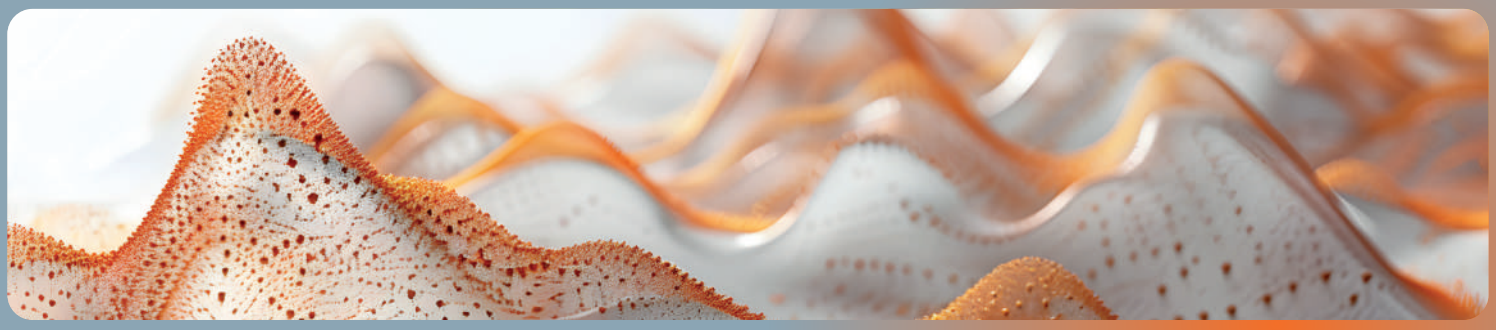
Успешные векторы атак во внутреннем периметре:

- компрометация Active Directory (Kerberoasting, уязвимости Veeam, SCCM, серверы 1С);
- злоупотребление доверенными внутренними сервисами (Confluence, 1С);
- обход механизмов защиты рабочих станций (AppLocker, локальное повышение привилегий);
- сетевые атаки внутри сегментов (mDNS, WPAD, DHCPv6 spoofing);
- случаи, где нашим экспертам удалось получить права администратора домена через МФУ Kyocera и AD CS в первые часы работ.

По результатам анализа проектов по внутреннему тестированию на проникновение можно сделать вывод, что комбинация слабого контроля клиентских автоматизированных рабочих мест (АРМ), небезопасных настроек доменной инфраструктуры, избыточных привилегий и плоской сетевой архитектуры по-прежнему приводит к успешной компрометации домена Active Directory.

Практика анализа беспроводных сетей в рамках проектов внутреннего тестирования показывает, что беспроводные сети создают критический канал утечки данных и несанкционированного доступа в сеть компании.

Подробнее с угрозами и рекомендациями можно ознакомиться в материале эксперта Angara Security: «Миф о безопасности Wi-Fi: как злоумышленники обходят стандартную защиту и проникают в корпоративную сеть».



ВЕБ-ПРИЛОЖЕНИЯ: ВОЗМОЖНО ЛИ СЭКОНОМИТЬ НА АНАЛИЗЕ БИЗНЕС-ЛОГИКИ?

Тестирование веб-приложений в 2025 году в основном проводилось по моделям «серого» и «белого ящика». Практика показывает, что развитие процессов безопасной разработки и внедрение безопасного жизненного цикла разработки действительно повышают общий уровень защищённости приложений.

Рисунок 7. Уровень защищённости веб-приложений

Тем не менее уязвимости продолжают выявляться.

Рисунок 8. Уровень риска уязвимостей веб-приложений

Чаще всего, по наблюдениям аналитиков, они связаны с логическими ошибками и классическими для веб-приложений уязвимостями, такими как:

1. недостатки в механизмах контроля доступа;
2. различные виды инъекций;
3. недостатки конфигурации компонентов приложения;
4. использование устаревших компонентов.

Это подтверждает, что даже при зрелых процессах разработки анализ безопасности веб-приложений остаётся необходимым и оправданным.

Специалисты Angara Security часто сталкиваются с вопросами о целесообразности проведения анализа защищённости отдельных веб-приложений в случаях, когда заказчики обращаются за услугой внешнего тестирования на проникновение.

Эксперты поясняют: методика внешнего тестирования включает поиск и эксплуатацию только тех уязвимостей, которые позволяют достичь цели и проникнуть во внутренний периметр.

Анализ веб-приложения в ходе внешнего тестирования:

- не учитывает все доступные во внешнем периметре веб-приложения;
- не затрагивает сложную бизнес-логику;
- небезопасные прямые ссылки на объекты (IDOR), некорректные сценарии авторизации;
- не отражает реальные риски злоупотребления функциональностью приложения.

Результаты полноценного анализа защищённости веб-приложений наглядно демонстрируют различия между услугами и подтверждают, что экономия за счёт анализа веб-приложений в рамках внешнего тестирования может создавать ложное ощущение защищённости.

ИТОГИ И ПРОГНОЗ

Одним из заметных итогов 2025 года, по оценке экспертов Angara Security, стал рост уровня зрелости информационной безопасности и защищённости периметров крупных компаний из финтеха, телекома и ИТ-сектора.

Это выражается сразу в нескольких аспектах:

- в сокращении количества «типовых» уязвимостей;
- в более безопасной сегментации сетей периметров;
- в повышении качества внутренних процессов реагирования и мониторинга.

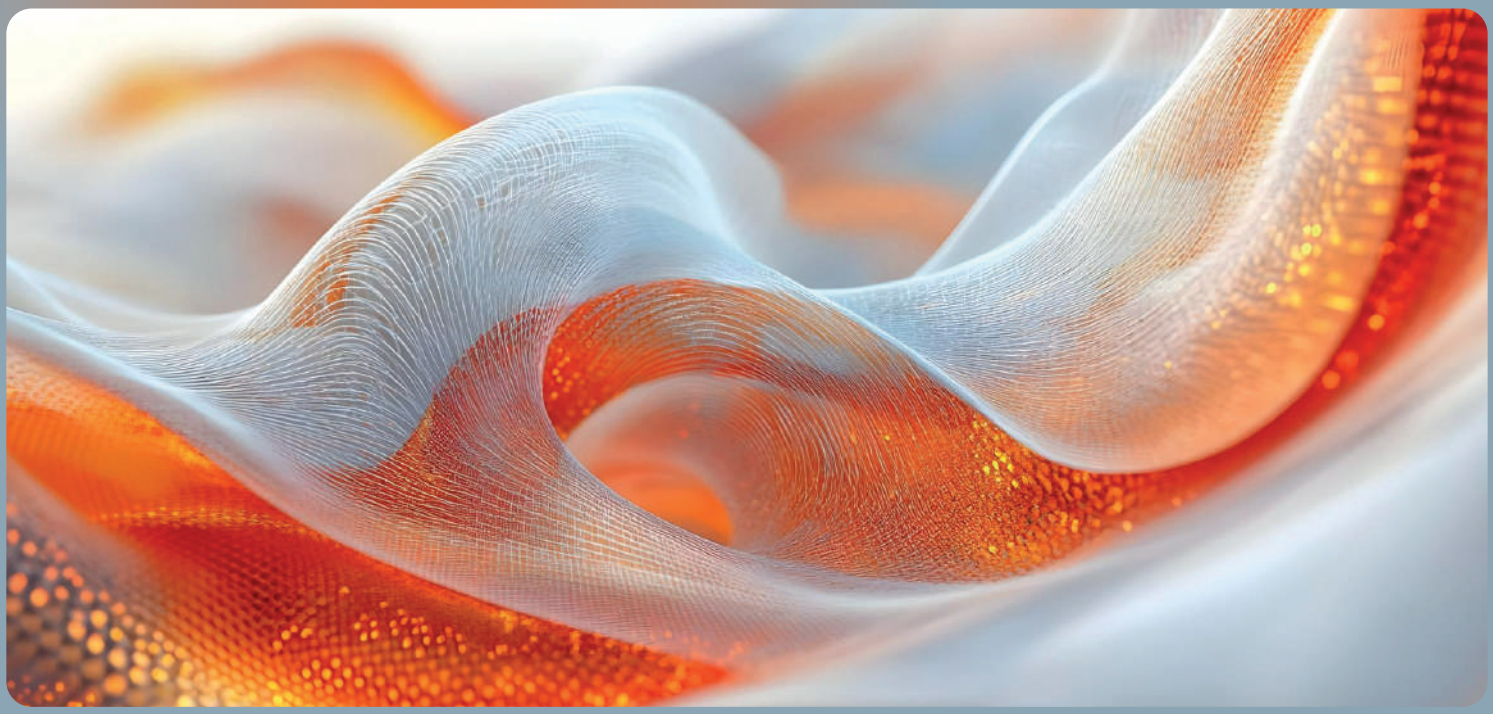
Это свидетельствует о том, что всё больше заказчиков и компаний-интеграторов в сфере ИБ действительно инвестируют в безопасность, а не в формальное соответствие требованиям заданий и регуляторов. Данная тенденция позитивна как для всей отрасли, так и для заказчиков. Накопленный опыт в сочетании с развитием нестандартных подходов будет и дальше помогать экспертам находить слабые места в инфраструктурах и давать честные оценки уровня их защищённости.

2025 год также показал, что, несмотря на необходимость проведения «рутинных» проверок, заказчики всё чаще заинтересованы в эффективности взаимодействия в ходе проекта. Такой подход положительно отразился не только на поиске реальных слабых мест периметров инфраструктур, но и позволил заказчикам оценить эффективность ранее внедрённых средств защиты и систем мониторинга.

В 2026 году пентест как услуга будет неизбежно расширяться и усложняться, что повысит требования к квалификации экспертов и качеству взаимодействия с заказчиком.

ANGARA SECURITY

ОБЕРЕГАЯ ДЕЙСТВИТЕЛЬНО ЦЕННОЕ



СВЯЗАТЬСЯ С НАМИ

angarasecurity.ru

+7 (495) 269 26 06

info@angarasecurity.ru
response@angarasecurity.ru