GROUP-IB

СЕКТОР: БАНКОВСКОЕ ДЕЛО / ФИНАНСЫ

РЕГИОН: РОССИЯ/СНГ

ИССЛЕДОВАНИЕ ВНЕШНЕГО ПЕРИМЕТРА

Анализ рисков, связанных с поверхностью атаки, для 50 крупнейших банков и поставщиков финансовых услуг в России и СНГ

ОКТЯБРЬ 2022

СОДЕРЖАНИЕ

КЛЮЧЕВЫЕ ВЫВОДЫ

В данном отчете специалисты Group-IB проанализировали внешнюю поверхность атаки 50 крупнейших банков и поставщиков финансовых услуг в России и странах Содружества Независимых Государств (СНГ). Собранные из общедоступных источников данные позволили оценить усредненный цифровой след финансовой организации в России и СНГ по 6 категориям внешних цифровых активов. Отчет также включает исследование проблем безопасности, распределенных по 8 категориям и 3 уровням риска.

Обычно цифровая поверхность атаки банков, находящихся в России и СНГ, немного меньше, чем в среднем по Латинской Америке, Ближнему Востоку и Северной Африке, ЕС и Азиатско-Тихоокеанскому региону. В то время как средний банк в ЕС имеет более 15 000 доступных извне цифровых активов, на банк в России или СНГ приходится в среднем лишь 3 558 активов. В Латинской Америке у банков в среднем было выявлено 7 900 активов, в Азиатско-Тихоокеанском регионе – 5 673 и в странах Ближнего Востока и Северной Африки – 2 895.

При относительно небольшой поверхности атаки по сравнению с другими регионами мира поставщики финансовых услуг в России и СНГ продемонстрировали высокий уровень защищенности. Решение Attack Surface Management от Group-IB (ASM) проводит общий скоринг безопасности компании на основе данных киберразведки, анализа возможных последствий атаки и инцидентов из реальной практики и выставляет оценку по шкале от 0 до 10, где 0 – наибольший риск, а 10 – минимальный. Согласно результатам данного исследования, общая оценка безопасности для организации в России и СНГ составила 6,7, что является вторым самым высоким показателем среди всех 5 регионов, исследованных для данного отчета. Среднее значение в ЕС составило всего 4,7 из 10, в то время как в странах Латинской Америки, Азиатско-Тихоокеанского региона и Ближнего Востока и Северной Африки общий показатель безопасности составил 5,9, 6,3 и 7,1 соответственно.

В заключительной части отчета представлены рекомендации по повышению уровня защищенности. Улучшения могут быть достигнуты прежде всего за счет концентрации усилий на фундаментальных задачах ИТ-безопасности, таких как полная и своевременная инвентаризация ресурсов, внедрение строгой политики контроля исправлений, закрытие всех ненужных портов и служб на внешних ресурсах и принудительная многофакторная авторизация на всех доступных извне страницах входа в систему.

3 558

Среднее количество внешних активов у проанализированных банков России и СНГ

6,7

Общая оценка риска для среднего банка в России и СНГ (от 0 до 10, где 10 – минимальный риск)

188

Общее количество выявленных критических проблем ИБ для среднего банка в России и СНГ

57,3

Среднее количество критических проблем на тысячу обнаруженных внешних ИТ-ресурсов

65%

Доля проанализированных банков в России и СНГ, у которых была выявлена хотя бы одна уязвимая служба удаленного доступа

ВВЕДЕНИЕ

Банки и поставщики финансовых услуг являются основными целями финансово мотивированных киберпреступников. Согласно отчету Group-IB High Tech Crime Trends Report 2021/2022: Угрозы для финансовых организаций, количество атак программ-вымогателей на финансовые учреждения увеличилось на 154% со второго полугодия 2019 года по второе полугодие 2021 года. В отчете упоминается, что за тот же период количество предложений о продаже первоначального доступа к сетям финансовых учреждений выросло на 206%. Атакующие несут все больше угроз для различных отраслей, прежде всего – для банковского и финансового секторов.

В то же время внешняя поверхность атаки организаций финансовой отрасли продолжает активно расти. Цифровая трансформация бизнеса, миграция в облако, а также слияния и поглощения — все это способствует расширению цифрового присутствия организации. В связи с постоянным увеличением количества цифровых активов, которые необходимо защищать среднестатистическому банку, становится чрезвычайно сложно поддерживать полную видимость периметра, проводить инвентаризацию ИТ-ресурсов и обеспечивать своевременное устранение уязвимостей. Многие компании сегодня внедряют инструменты класса Attack Surface Management (управление поверхностью атаки) для решения этих проблем.

В данном отчете рассматривается поверхность атаки для выборки из 50 крупнейших банков и поставщиков финансовых услуг в России и странах СНГ. Этот подход обеспечивает всесторонний взгляд на элементы цифрового следа, от количества доменов и IP-адресов до распространенности подсетей и инструментов удаленного доступа. В отчете также будет представлена подробная оценка рисков по 8 различным категориям проблем и показана разбивка по проблемам высокого и среднего уровня риска и успешно пройденным проверкам безопасности инфраструктуры. Аналогичные международные показатели добавлены для обогащения данных контекстом.

>50%

инцидентов, расследованных Лабораторией компьютерной криминалистики Group-IB, произошли в результате эксплуатации уязвимостей периметра

1/3

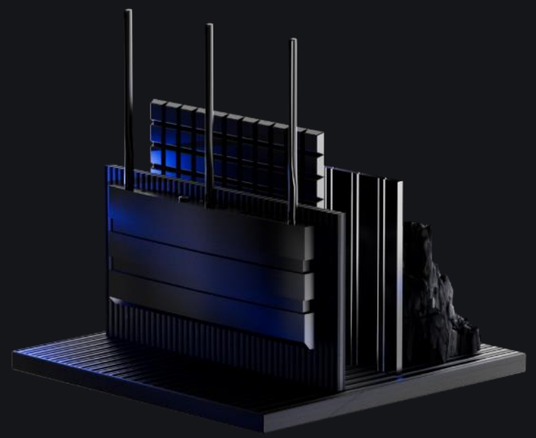
доля успешных кибератак на теневые ИТ-ресурсы (по оценке Gartner)

30%

облачных активов среднестатистической компании неизвестны ее департаментам ИБ и ИТ (по данным Forrester)

ОБЗОР ДАННЫХ О ЦИФРОВЫХ АКТИВАХ

Хотя в последние годы масштабная цифровая трансформация коснулась всех отраслей, наибольшим изменениям подвергся сектор банковских и финансовых услуг. Приведенные ниже данные характеризуют среднюю внешнюю поверхность атаки для выборки из 50 поставщиков финансовых услуг с головным офисом в России и странах СНГ.



3 558

среднее количество внешних активов у проанализированных банков России и СНГ

650

доменов и поддоменов

1 910

IP-адресов

6

подсетей

912

ПО и сервисов

52

SSL-сертификатов

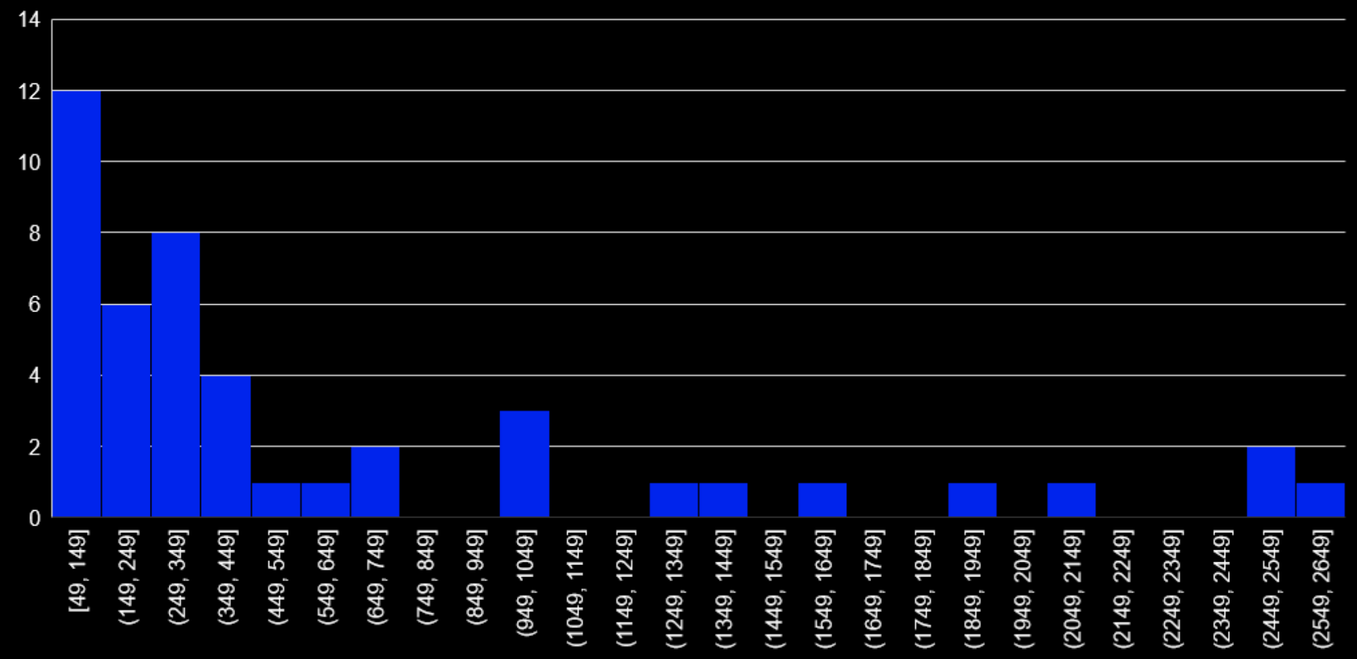
28

служб удаленного доступа

ДОМЕНЫ И ПОДДОМЕНЫ

У представленных в выборке банков России и СНГ в среднем было выявлено по 650 доменов и поддоменов, относящихся к поверхности атаки. Это меньше половины среднего показателя для европейских банков, но больше, чем в среднем по Азиатско-Тихоокеанскому региону, Ближнему Востоку и Северной Африке или Латинской Америке. Свыше половины банков, включенных в выборку, имели менее 350 доменов и поддоменов.

Количество доменов и поддоменов на один банк



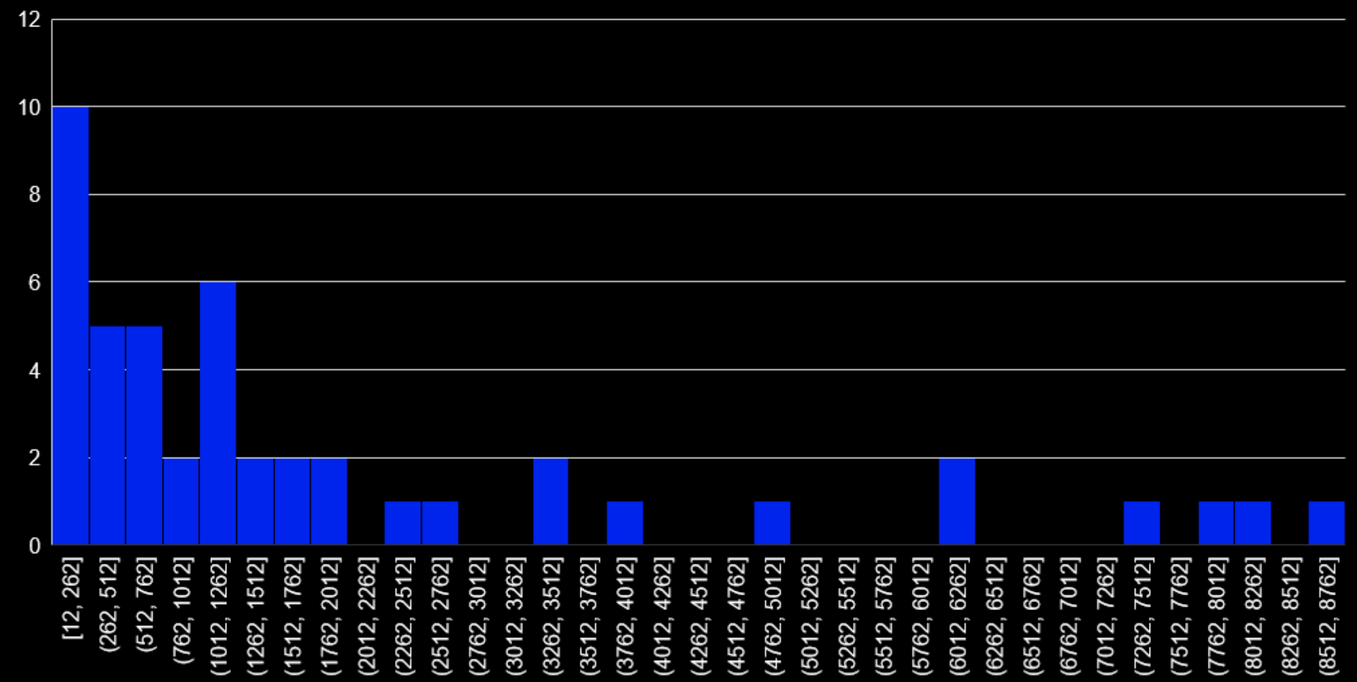
Международные показатели

Регион	Среднее кол-во доменов на один банк
Европа	1 516,67
Россия и СНГ	**649,72**
Азиатско-Тихоокеанский регион	617,02
Ближний Восток и Северная Африка	534,53
Латинская Америка	529,83

IP-АДРЕСА

В среднем у попавших в выборку банков из России и СНГ было выявлено по 1910 IP-адресов. При этом у нескольких крупных организаций были огромные поверхности атаки, что исказило среднее значение. Более 50% банков России и СНГ в выборке имели менее 1300 IP-адресов. Хотя средний показатель оказался выше, чем в странах Ближнего Востока и Северной Африки, поверхность атаки у банков из России и СНГ оказалась относительно небольшой по сравнению с другими регионами мира.

Количество IP-адресов на один банк



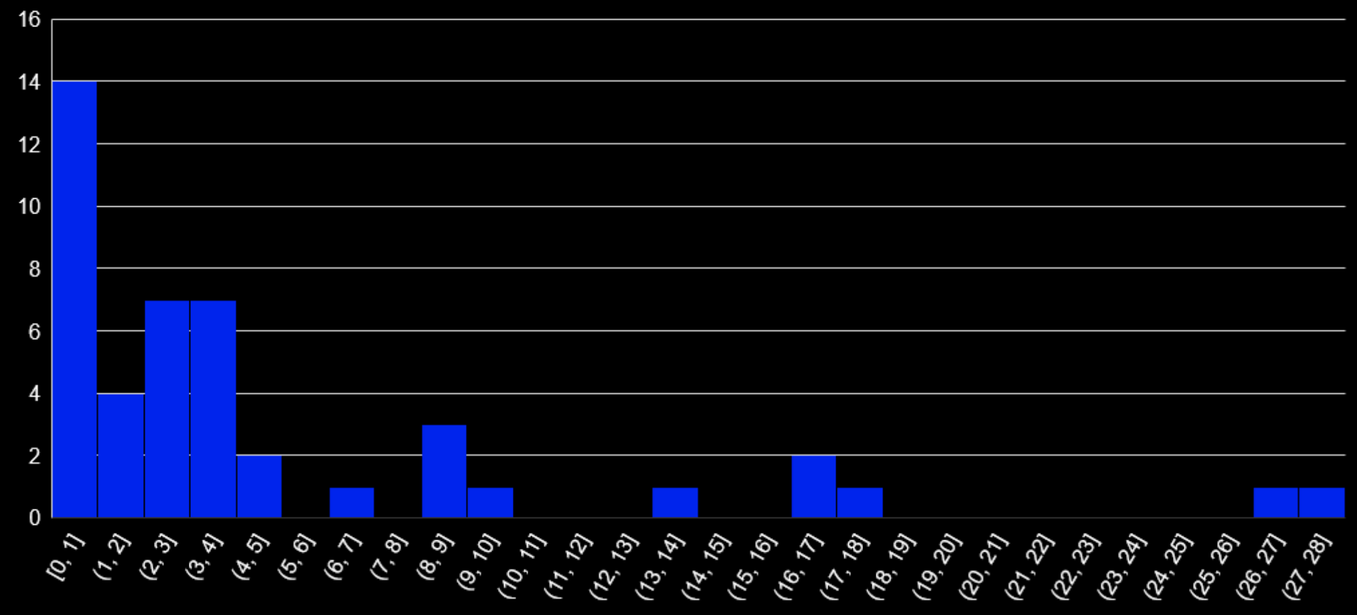
Международные показатели

Регион	Среднее кол-во IP-адресов на один банк
Европа	9 668,24
Латинская Америка	5 117,42
Азиатско-Тихоокеанский регион	2 290,77
Россия и СНГ	**1 910,17**
Ближний Восток и Северная Африка	1 105,80

ПОДСЕТИ

Подсеть — это типичный компонент архитектуры корпоративной сети. В мире на один банк в среднем приходится 8,3 подсети. Для финансовых учреждений в России и СНГ этот показатель составил 5,9, что ниже среднемирового уровня и соответствует третьему месту в рейтинге исследуемых в данном отчете регионов.

Количество подсетей на один банк



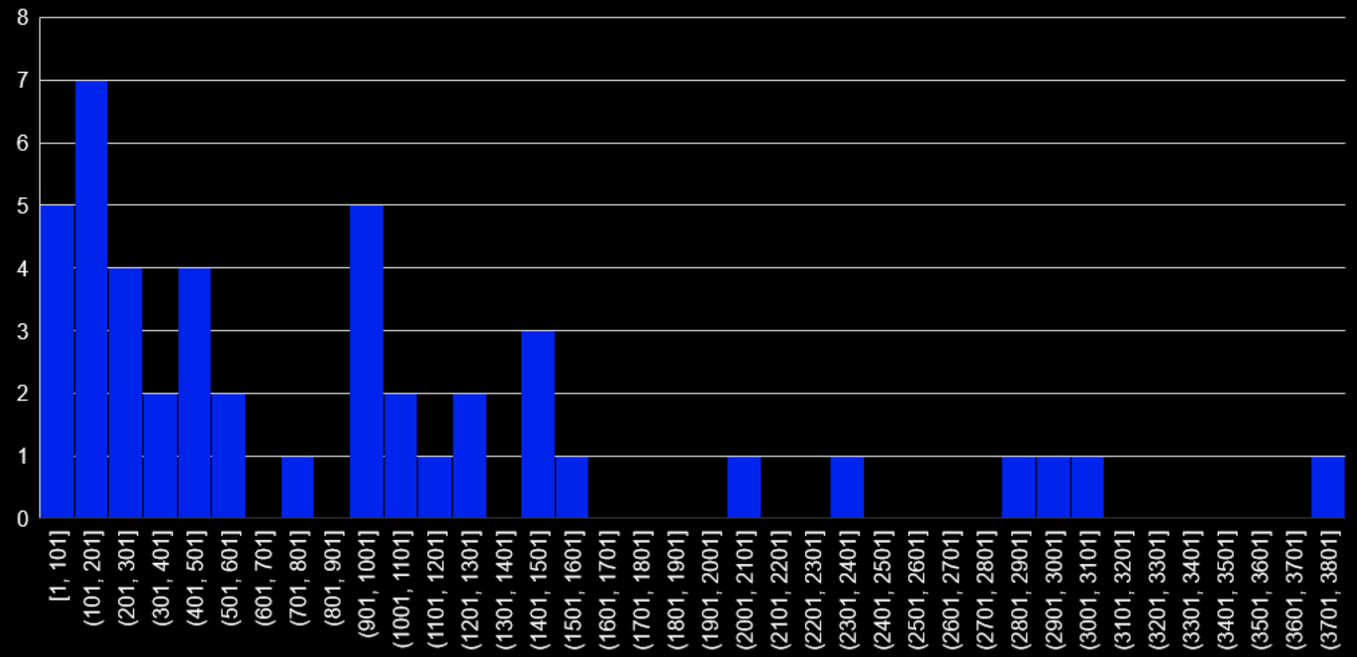
Международные показатели

Регион	Среднее кол-во подсетей на один банк
Европа	16,04
Латинская Америка	12,52
Россия и СНГ	**5,85**
Азиатско-Тихоокеанский регион	5,36
Ближний Восток и Северная Африка	1,55

ПО И СЕРВИСЫ

Устаревшее программное обеспечение и незакрытые бреши в сервисах могут создавать уязвимости в периметре организации и поэтому являются важной частью поверхности атаки. В среднем на банк в России и СНГ приходится только 912 потенциально уязвимых программ и сервисов, что является самым низким показателем среди всех исследованных регионов.

Количество доступных извне ПО и сервисов на один банк



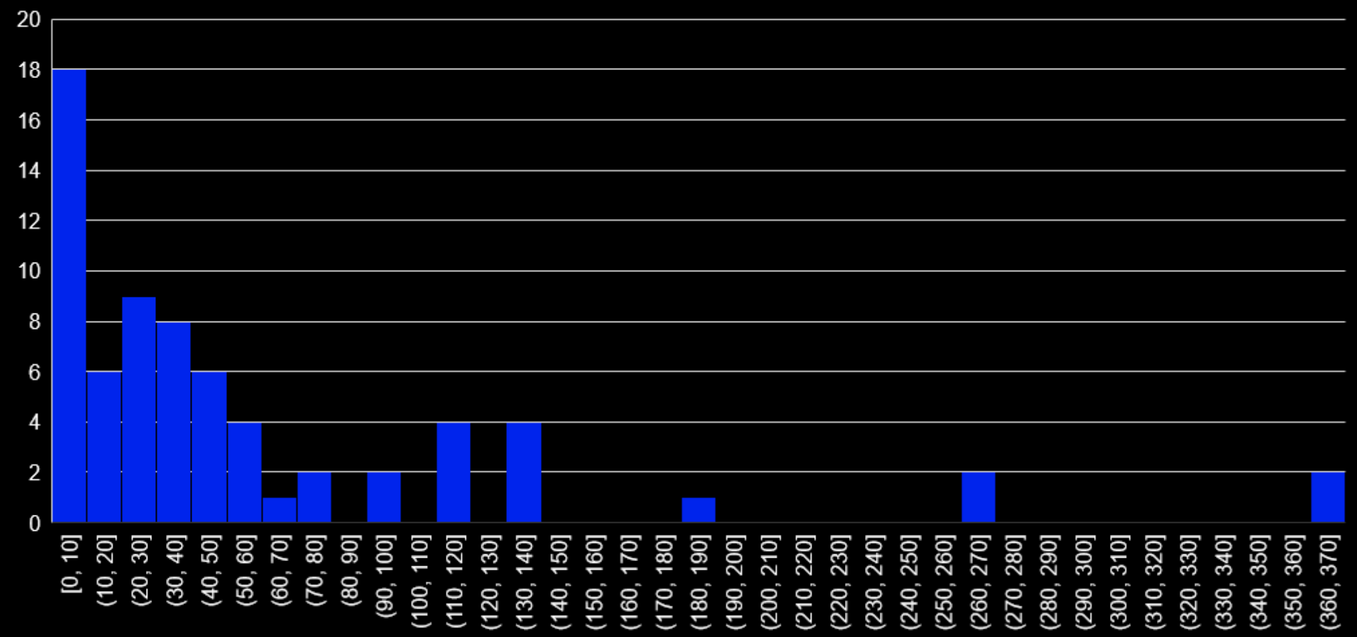
Международные показатели

Регион	Среднее кол-во ПО и сервисов на один банк
Европа	3 855,37
Азиатско-Тихоокеанский регион	2 688,79
Латинская Америка	2 190,21
Ближний Восток и Северная Африка	1 205,14
Россия и СНГ	**912,11**

SSL-сертификаты

SSL-сертификаты являются важным элементом поверхности атаки, так как подтверждают подлинность веб-сайтов, приложений и других цифровых активов, доступных для клиентов. В банках России и СНГ в среднем используется почти в два раза больше SSL-сертификатов, чем в банках Ближнего Востока и Северной Африки (регион с наименьшим средним количеством сертификатов в выборке), но более чем вдвое меньше, чем у европейских банков.

Количество SSL-сертификатов на один банк



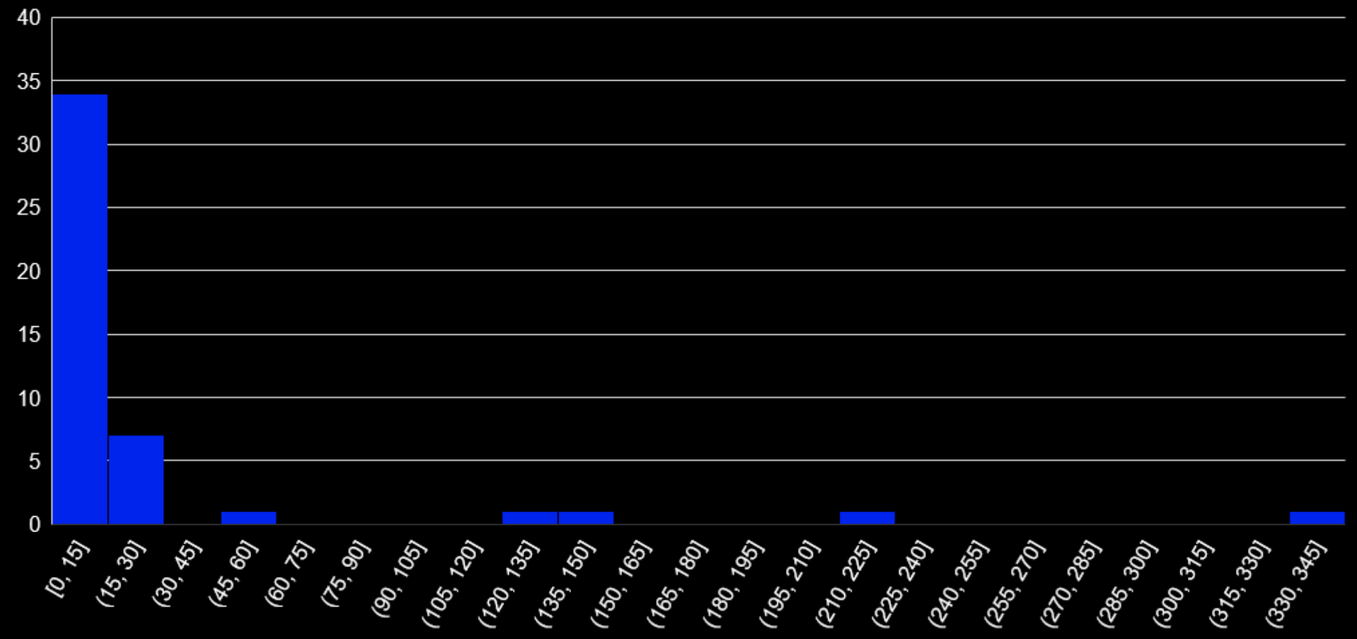
Международные показатели

Регион	Среднее кол-во SSL-сертификатов на один банк
Европа	122,55
Азиатско-Тихоокеанский регион	63,38
Россия и СНГ	**51,89**
Латинская Америка	47,31
Ближний Восток и Северная Африка	29,43

ИНСТРУМЕНТЫ УДАЛЕННОГО ДОСТУПА

Инструменты удаленного доступа (RDP, SSH, VPN и др.) часто используются злоумышленниками как вектор компрометации. У финансовых учреждений в России и странах СНГ среднее количество доступных извне средств удаленного доступа намного выше, чем в других регионах мира, за исключением Европы. 65% проанализированных банков России и СНГ имели по крайней мере один открытый для веб-доступа порт.

Количество доступных извне средств удаленного доступа на один банк



Международные показатели

Регион	Среднее кол-во средств удаленного доступа на один банк
Европа	47,78
Россия и СНГ	**27,80**
Ближний Восток и Северная Африка	18,37
Азиатско-Тихоокеанский регион	7,62
Латинская Америка	2,92

СВОДКА РИСКОВ ПО КАТЕГОРИЯМ ПРОБЛЕМ

Group-IB Attack Surface Management проверяет различные проблемы безопасности и присваивает им оценки рисков. В среднем оценка защищенности банков в России и странах СНГ немного выше среднемирового показателя: 6,7 из 10, где 0 — самый высокий риск, а 10 — самый низкий. Для Европы этот показатель составил 4,9, для Латинской Америки – 5,9, для Азиатско-Тихоокеанского региона – 6,3, для стран Ближнего Востока и Северной Африки – 7,1.

6,7

Средняя общая оценка защищенности поверхности атаки для банков России и СНГ, включенных в выборку

6,3

Уязвимости

7,4

Сетевая безопасность

6,6

Утечки учетных данных

8,6

Упоминания в дарквебе

9,3

Вредоносное ПО

5,4

Безопасность электронной почты

6,2

Безопасность SSL/TLS

7,7

DNS/домены

СВОДНЫЕ РЕЗУЛЬТАТЫ ВСЕХ ПРОВЕРОК

Помимо инвентаризации внешних активов организаций, в рамках исследования на основе общедоступных данных были проведены пассивные проверки безопасности для выявления распространенных проблем, с которыми сталкиваются многие банки в России и СНГ.

57,3 Среднее количество проблем высокого уровня риска на 1000 активов

289,1 Среднее количество проблем среднего уровня риска на 1000 активов

11 228 Среднее количество успешно пройденных проверок безопасности на 1000 активов

Результаты проверок на 1000 цифровых активов

ОБЗОР ПРОБЛЕМ ВЫСОКОГО УРОВНЯ РИСКА

Среднее общее количество проблем высокой степени риска сильно варьировалось в зависимости от категории проблемы. В среднем на одно вошедшее в выборку финансовое учреждение пришлось всего 0,7 критических угроз, связанных с вредоносным ПО, и только 1,5 критических рисков, связанных с сетевой безопасностью. В то же время среднее количество угроз для электронной почты составило 119, а среднее количество уязвимостей — 43.

188

Среднее общее количество проблем высокого уровня риска на один банк

57,3

Среднее количество проблем высокого уровня риска на 1000 активов

0,52%

Доля проверок, выявивших проблемы высокого уровня риска

42,7

Уязвимости высокого уровня риска в среднем на один банк

1,5

Угрозы сетевой безопасности высокого уровня риска в среднем на один банк

12

Утечки учетных данных высокого уровня риска в среднем на один банк

4,2

Угрозы в даркевебе с высоким уровнем риска в среднем на один банк

0,7

Вредоносное ПО с высоким уровнем угрозы в среднем на один банк

118,9

Угрозы для электронной почты высокого уровня риска в среднем на один банк

5,7

Проблемы безопасности SSL/TLS высокого уровня риска в среднем на один банк

3

Проблемы безопасности DNS/доменов высокого уровня риска в среднем на один банк

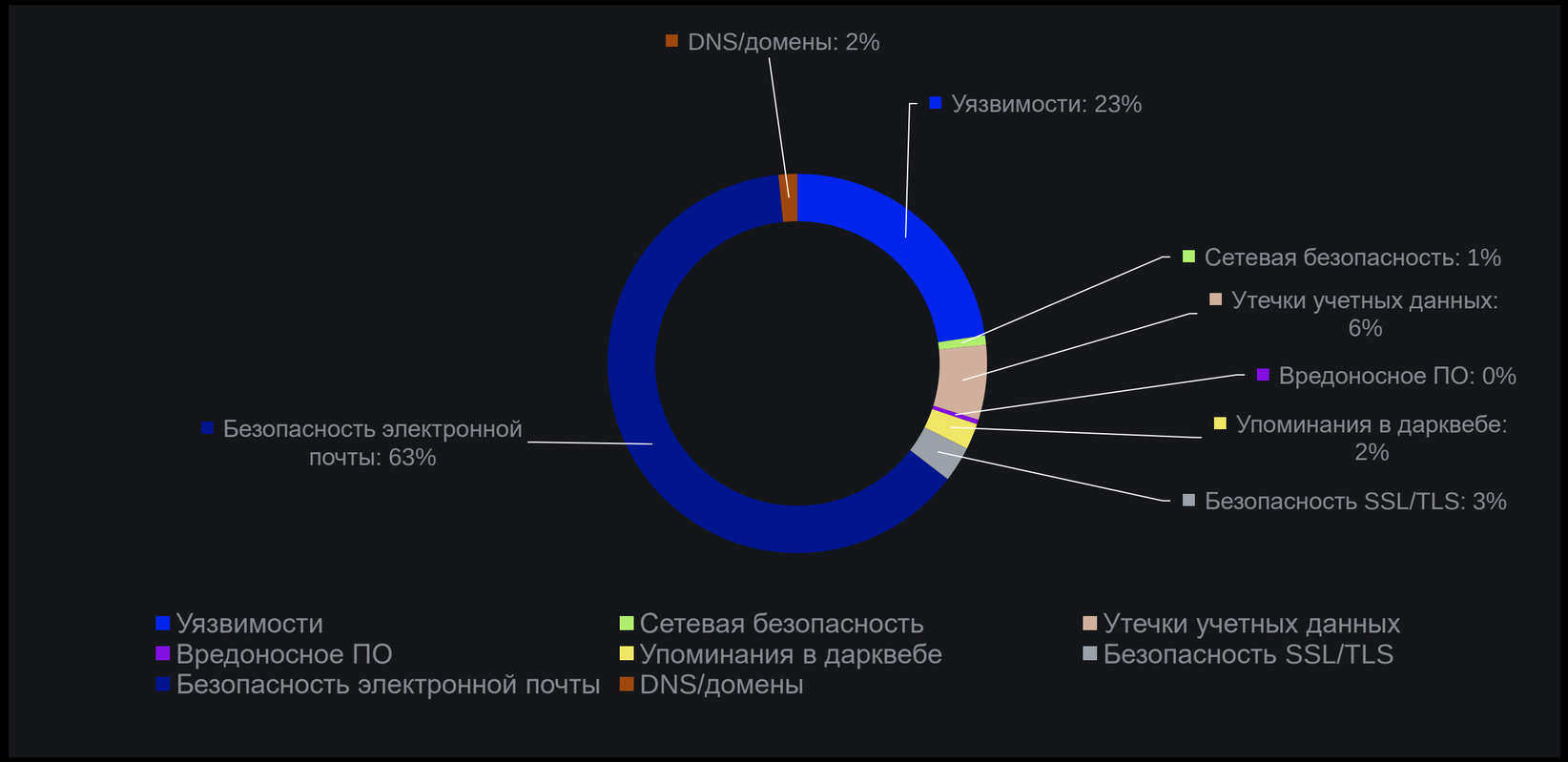
АНАЛИЗ ПРОБЛЕМ ВЫСОКОГО УРОВНЯ РИСКА

Угрозы безопасности электронной почты составляют в среднем 63% обнаруженных проблем высокой степени риска. Это связано с тем, что злоумышленники постоянно обходят механизмы защиты DKIM и DMARC. Значительную долю проблем высокого уровня риска составляют уязвимости – 23%. Хотя на утечки учетных данных приходится всего 6% от общего количества проблем высокого уровня риска, нахождение учетных данных в дарквебе представляет критическую угрозу для организаций.

Международные показатели

Регион	Среднее кол-во проблем с высоким уровнем риска на 1000 активов
Ближний Восток и Северная Африка	121,1
Азиатско-Тихоокеанский регион	105,0
Латинская Америка	61,9
Россия и СНГ	**57,3**
Европа	41,4

Проблемы высокого уровня риска по категориям



ОБЗОР ПРОБЛЕМ СРЕДНЕГО УРОВНЯ РИСКА

Угрозы сетевой безопасности составляют значительную часть проблем среднего уровня риска, выявляемых среди банков России и СНГ. Уязвимости, проблемы с безопасностью SSL/TLS и проблемы с DNS/доменами также составляют значительную долю обнаруженных проблем среднего уровня риска.

909,2

Среднее общее количество проблем среднего уровня риска на один банк

289,1

Среднее количество проблем среднего уровня риска на 1000 активов

2,7%

Доля проверок, выявивших проблемы среднего уровня риска

176,7

Уязвимости среднего уровня риска в среднем на один банк

383,4

Угрозы сетевой безопасности среднего уровня риска в среднем на один банк

11,9

Утечки учетных данных среднего уровня риска в среднем на один банк

3

Угрозы в даркевебе со средним уровнем риска в среднем на один банк

62,7

Вредоносное ПО со средним уровнем риска в среднем на один банк

10,7

Угрозы для электронной почты среднего уровня риска в среднем на один банк

150,9

Проблемы безопасности SSL/TLS среднего уровня риска в среднем на один банк

109,8

Проблемы безопасности DNS/доменов среднего уровня в среднем на один банк

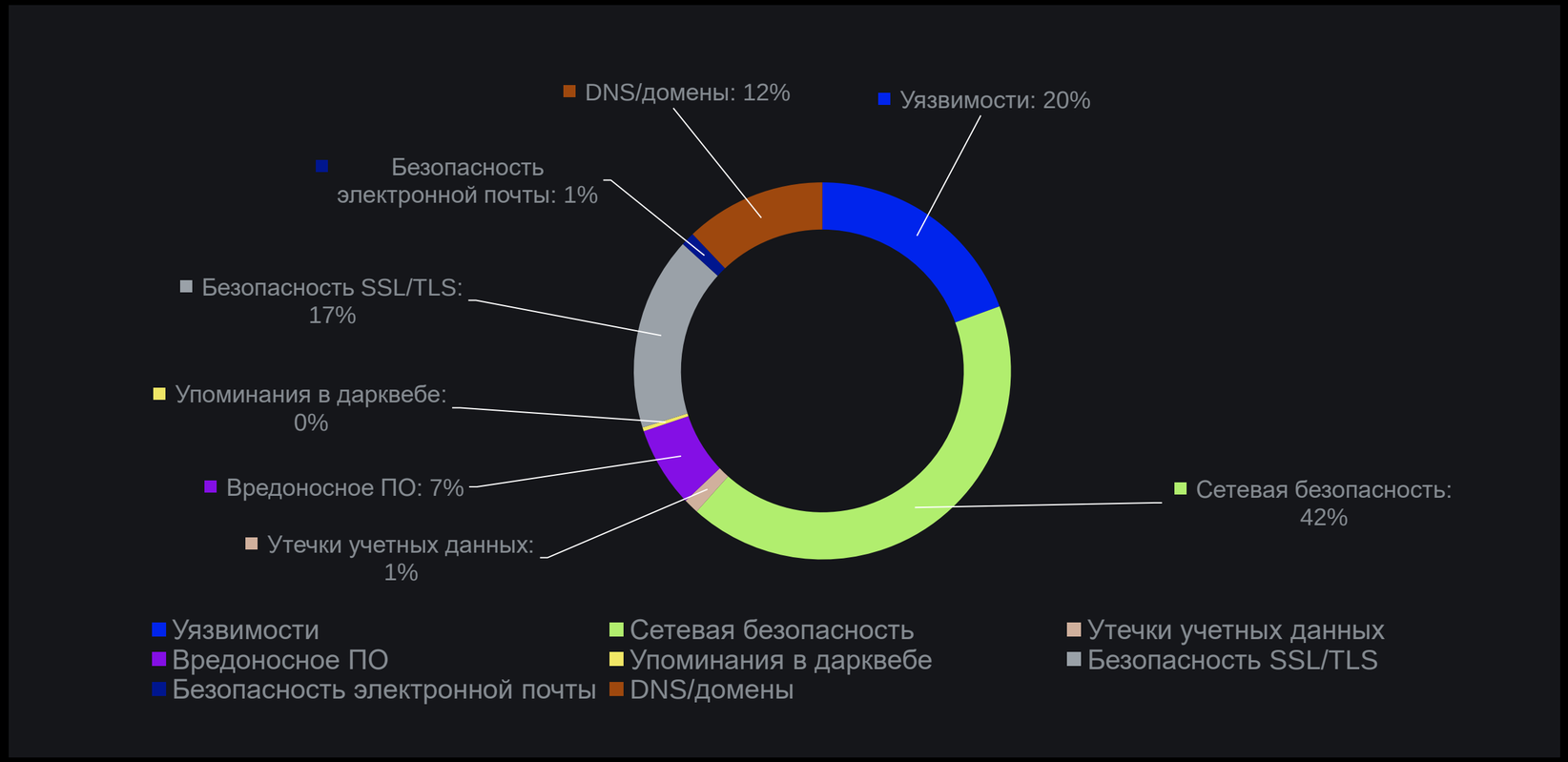
АНАЛИЗ ПРОБЛЕМ СРЕДНЕГО УРОВНЯ РИСКА

Более 90% проблем среднего уровня риска составили проблемы с сетевой безопасностью (42%), уязвимостями (20%), безопасностью SSL/TLS (17%) и DNS/доменами (12%). Это говорит о сложности поддержания высокого уровня кибергигиены в масштабной и сложной ИТ-инфраструктуре. Хотя угрозы безопасности электронной почты составили 63% от всех проблем высокой степени риска, из проблем средней степени риска с электронной почтой был связан только 1%.

Международные показатели

Регион	Среднее кол-во проблем среднего уровня риска на 1000 активов
Азиатско-Тихоокеанский регион	439,5
Ближний Восток и Северная Африка	348,9
Латинская Америка	346,1
Россия и СНГ	**289,1**
Европа	263,7

Проблемы среднего уровня риска по категориям



УЯЗВИМОСТИ

6,3

Средняя общая оценка риска для проверок, связанных с **уязвимостями**

Международные показатели

Регион	Средняя оценка риска для уязвимостей
Ближний Восток и Северная Африка	7,78
Россия и СНГ	**6,34**
Азиатско-Тихоокеанский регион	6,21
Латинская Америка	5,93
Европа	4,45

Уязвимости высокого уровня риска	Уязвимости среднего уровня риска	Успешно пройденные проверки безопасности
42,7 Среднее общее кол-во проблем на один банк	**176,7** Среднее общее кол-во проблем на один банк	**14 005** Среднее общее кол-во проверок безопасности, пройденных одним банком
7,9 Среднее кол-во проблем на 1000 активов на один банк	**44,5** Среднее кол-во проблем на 1000 активов на один банк	**3 824** Среднее кол-во пройденных проверок безопасности на 1000 активов
0,21% Средняя доля проверок, выявивших проблемы высокого уровня риска	**1,26%** Средняя доля проверок, выявивших проблемы среднего уровня риска	**98,5%** Средняя доля успешно пройденных проверок

СЕТЕВАЯ БЕЗОПАСНОСТЬ

7,4

Средняя общая оценка риска для проверок, связанных с **сетевой безопасностью**

Международные показатели

Регион	Средняя оценка риска для сетевой безопасности
Ближний Восток и Северная Африка	8,08
Россия и СНГ	**7,38**
Латинская Америка	5,49
Азиатско-Тихоокеанский регион	5,53
Европа	3,88

Проблемы сетевой безопасности высокого уровня риска	Проблемы сетевой безопасности среднего уровня риска	Успешно пройденные проверки безопасности
1,5 Среднее общее количество проблем на один банк	**383,4** Среднее общее кол-во проблем на один банк	**17 111** Среднее общее кол-во проверок безопасности, пройденных одним банком
0,5 Среднее кол-во проблем на 1000 активов на один банк	**124,9** Среднее кол-во проблем на 1000 активов на один банк	**4 077** Среднее кол-во пройденных проверок безопасности на 1000 активов
0,02% Средняя доля проверок, выявивших проблемы высокого уровня риска	**4,54%** Средняя доля проверок, выявивших проблемы среднего уровня риска	**95,4%** Средняя доля успешно пройденных проверок

УТЕЧКИ УЧЕТНЫХ ДАННЫХ

6,6

Средняя общая оценка риска для проверок, связанных с **утечками учетных данных**

Международные показатели

Регион	Средняя оценка риска для утечек учетных данных
Россия и СНГ	**6,62**
Азиатско-Тихоокеанский регион	5,07
Ближний Восток и Северная Африка	4,64
Европа	4,20
Латинская Америка	3,81

Утечки учетных данных высокого уровня риска	Утечки учетных данных среднего уровня риска	Успешно пройденные проверки безопасности
12 Среднее общее количество проблем на один банк	**11,9** Среднее общее количество проблем на один банк	**1 255** Среднее общее кол-во проверок безопасности, пройденных одним банком
4,8 Среднее кол-во проблем на 1000 активов на один банк	**5,8** Среднее кол-во проблем на 1000 активов на один банк	**428,9** Среднее кол-во пройденных проверок безопасности на 1000 активов
1,2% Средняя доля проверок, выявивших проблемы высокого уровня риска	**1,5%** Средняя доля проверок, выявивших проблемы среднего уровня риска	**97,3%** Средняя доля успешно пройденных проверок

ВРЕДОНОСНОЕ ПО

9,3

Средняя общая оценка риска для проверок, связанных с **вредоносным ПО**

Международные показатели

Регион	Средняя оценка риска для вредоносного ПО
Россия и СНГ	**9,27**
Ближний Восток и Северная Африка	9,26
Ближний Восток и Северная Африка	9,06
Латинская Америка	8,88
Европа	8,61

Проблемы высокого уровня риска, связанные с вредоносным ПО	Проблемы среднего уровня риска, связанные с вредоносным ПО	Успешно пройденные проверки безопасности
0,7 Среднее общее количество проблем на один банк	**62,7** Среднее общее кол-во проблем на один банк	**7 016** Среднее общее кол-во проверок безопасности, пройденных одним банком
0,2 Среднее кол-во проблем на 1000 активов на один банк	**16,3** Среднее кол-во проблем на 1000 активов на один банк	**2 013** Среднее кол-во пройденных проверок безопасности на 1000 активов
0,01% Средняя доля проверок, выявивших проблемы высокого уровня риска	**0,7%** Средняя доля проверок, выявивших проблемы среднего уровня риска	**99,3%** Средняя доля успешно пройденных проверок

УПОМИНАНИЯ В ДАРКВЕБЕ

8,6

Средняя общая оценка риска для проверок, связанных с **упоминаниями в дарквебе**

Международные показатели

Регион	Средняя оценка риска для упоминаний в дарквебе
Латинская Америка	9,55
Ближний Восток и Северная Африка	9,53
Азиатско-Тихоокеанский регион	9,46
Европа	9,22
Россия и СНГ	**8,55**

Упоминания в дарквебе высокого уровня риска	Упоминания в дарквебе среднего уровня риска	Успешно пройденные проверки безопасности
4,2 Среднее общее количество проблем на один банк	**3** Среднее общее кол-во проблем на один банк	**1 272** Среднее общее кол-во проверок безопасности, пройденных одним банком
1,8 Среднее кол-во проблем на 1000 активов на один банк	**1** Среднее кол-во проблем на 1000 активов на один банк	**436,9** Среднее кол-во пройденных проверок безопасности на 1000 активов
0,44% Средняя доля проверок, выявивших проблемы высокого уровня риска	**0,26%** Средняя доля проверок, выявивших проблемы среднего уровня риска	**99,3%** Средняя доля успешно пройденных проверок

БЕЗОПАСНОСТЬ SSL/TLS

6,2

Средняя общая оценка риска для проверок, связанных с **безопасностью SSL/TLS**

Международные показатели

Регион	Средняя оценка риска для безопасности SSL/TLS
Ближний Восток и Северная Африка	8,36
Азиатско-Тихоокеанский регион	6,84
Латинская Америка	6,75
Россия и СНГ	**6,15**
Европа	6,03

Проблемы безопасности SSL/TLS высокого уровня риска	Проблемы безопасности SSL/TLS среднего уровня риска	Успешно пройденные проверки безопасности
5,7 Среднее общее количество проблем на один банк	**150,9** Среднее общее кол-во проблем на один банк	**270,1** Среднее общее кол-во проверок безопасности, пройденных одним банком
2,3 Среднее кол-во проблем на 1000 активов на один банк	**46,2** Среднее кол-во проблем на 1000 активов на один банк	**85,9** Среднее кол-во пройденных проверок безопасности на 1000 активов
2,7% Средняя доля проверок, выявивших проблемы высокого уровня риска	**34,6%** Средняя доля проверок, выявивших проблемы среднего уровня риска	**62,7%** Средняя доля успешно пройденных проверок

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

5,4

Средняя общая оценка риска для проверок, связанных с **безопасностью электронной почты**

Международные показатели

Регион	Средняя оценка рисков для безопасности электронной почты
Ближний Восток и Северная Африка	5,91
Азиатско-Тихоокеанский регион	5,51
Ближний Восток и Северная Африка	5,50
Европа	5,40
Россия и СНГ	**5,38**

Проблемы с безопасностью электронной почты высокого уровня риска	Проблемы с безопасностью электронной почты среднего уровня риска	Успешно пройденные проверки безопасности
118,9 Среднее общее количество проблем на один банк	**10,7** Среднее общее кол-во проблем на один банк	**59,2** Среднее общее кол-во проверок безопасности, пройденных одним банком
38,9 Среднее кол-во проблем на 1000 активов на один банк	**3** Среднее кол-во проблем на 1000 активов на один банк	**21,6** Среднее кол-во пройденных проверок безопасности на 1000 активов
62,5% Средняя доля проверок, выявивших проблемы высокого уровня риска	**4,6%** Средняя доля проверок, выявивших проблемы среднего уровня риска	**32,9%** Средняя доля успешно пройденных проверок

DNS/ДОМЕНЫ

7,7

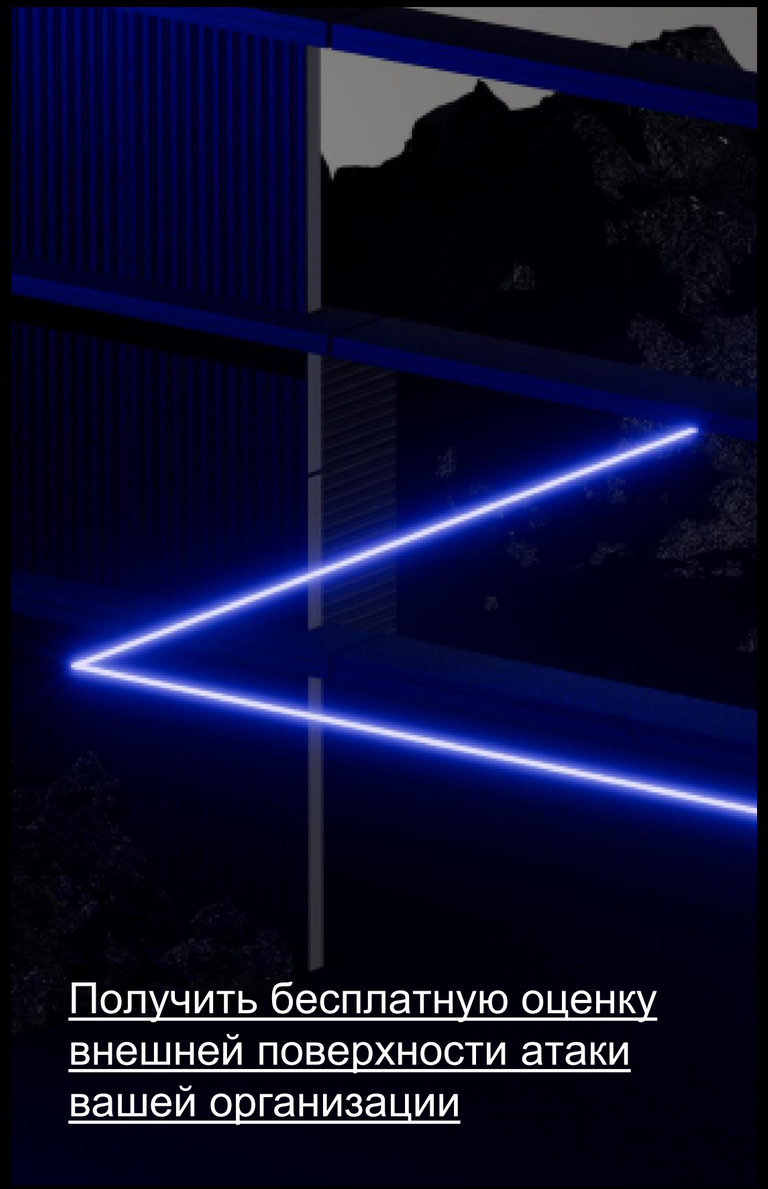
Средняя общая оценка риска для проверок, связанных с **DNS/доменами**

Международные показатели

Регион	Средняя оценка рисков для DNS/доменов
Азиатско-Тихоокеанский регион	7,66
Россия и СНГ	**7,65**
Латинская Америка	7,05
Ближний Восток и Северная Африка	5,99
Европа	3,21

Проблемы высокого уровня риска, связанные с DNS/доменами	Проблемы среднего уровня риска, связанные с DNS/доменами	Успешно пройденные проверки безопасности
3 Среднее общее количество проблем на один банк	**109,8** Среднее общее кол-во проблем на один банк	**883,3** Среднее общее кол-во проверок безопасности, пройденных одним банком
1,1 Среднее кол-во проблем на 1000 активов на один банк	**47,5** Среднее кол-во проблем на 1000 активов на один банк	**343,8** Среднее кол-во пройденных проверок безопасности на 1000 активов
0,36% Средняя доля проверок, выявивших проблемы высокого уровня риска	**11,3%** Средняя доля проверок, выявивших проблемы среднего уровня риска	**88,3%** Средняя доля успешно пройденных проверок

РЕКОМЕНДАЦИИ



Получить бесплатную оценку внешней поверхности атаки вашей организации

РЕГУЛЯРНЫЙ МОНИТОРИНГ ЦИФРОВЫХ АКТИВОВ

Проводите своевременную инвентаризация всей внешней поверхности атаки организации.

НЕПРЕРЫВНЫЙ ПОИСК ТЕНЕВЫХ ИТ

Регулярно сканируйте внешнюю поверхность атаки для выявления теневых ИТ, некорректных конфигураций и других скрытых рисков.

ЗАКРЫТИЕ НЕИСПОЛЬЗУЕМЫХ ПОРТОВ

Закройте все неиспользуемые порты удаленного доступа. Внедрите многофакторную аутентификации для тех портов, которые останутся открытыми, и тщательно отслеживайте их работу.

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ И УПРАВЛЕНИЕ ДОСТУПНЫМИ ИЗВНЕ РЕСУРСАМИ

Обеспечьте своевременное обновление всех доступных из Интернета цифровых активов и устранение всех известных уязвимостей и рисков.

ПАРОЛЬНАЯ ПОЛИТИКА И МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Внедрите строгую парольную политику для предотвращения брутфорс-атак и словарных атак и используйте многофакторную аутентификацию для обеспечения безопасности служб и приложений.

МОНИТОРИНГ ДАРКВЕБА ДЛЯ ПРЕВЕНТИВНОЙ ЗАЩИТЫ ОТ УГРОЗ

Используйте данные киберразведки для проактивного снижения рисков, включая утечки учетных данных, упоминания в даркнебе и целевые атаки.

ЗАКЛЮЧЕНИЕ

Атаки нулевого дня и другие сложные угрозы, за которыми стоят прогосударственные злоумышленники, широко освещаются в СМИ. Однако этот тип инцидентов составляет лишь незначительную часть от всех успешных взломов, которые встречаются на практике. Подавляющее большинство киберпреступников обладают низкой квалификацией и предпочитают использовать автоматизированные способы поиска легко эксплуатируемых уязвимостей, таких как открытые порты RDP, которые можно взломать с помощью словаря или брутфорс-атаки. Если они не находят недостатков безопасности, позволяющих без значительных усилий взломать инфраструктуру организации, то просто переключаются на следующую жертву.

У большинства поставщиков финансовых услуг есть зрелая стратегия кибербезопасности, которая позволяет успешно защитить известные ИТ-активы. При этом серьезные риски могут исходить от неизвестных компонентов инфраструктуры. Массовая цифровизация бизнеса неизбежно приводит к потере контроля над некоторыми доступными извне активами организации. Со временем компании перестают отслеживать такие активы, управлять их уровнем защищенности и устранять уязвимости. Таким образом, теневые активы становятся критической угрозой для организаций и привлекательным вектором атаки для киберпреступников.

Выявление и устранение скрытых рисков должно быть для компании приоритетной целью, ведь ее достижение позволяет усилить защищенность инфраструктуры и повысить барьер для несанкционированного проникновения в корпоративную сеть. Устранение неуправляемых активов – либо путем их удаления и перевода в автономный режим, либо путем их обновления и приведения в соответствие с требованиями – значительно сокращает риски и заметно повышает уровень безопасности. Управление поверхностью атаки – важнейшая задача, которая из-за непрерывного увеличения количества цифровых активов будет оставаться в центре внимания организаций еще долгие годы.

МЕТОДОЛОГИЯ

Исследования, которые легли в основу этого отчета, проводились 18–31 июля 2022 г. Все проанализированные и опубликованные в рамках отчета данные были собраны пассивным методом и находятся в публичном доступе на различных веб-ресурсах и интернет-сервисах.

Group-IB Attack Surface Management анализирует все пространство IPv4, выявляет все доступные из Интернета цифровые активы и собирает публично доступные данные о каждом из них. Например, решение фиксирует данные об используемой операционной системе, запущенных службах и программном обеспечении, открытых портах и т. д. При помощи других открытых источников данных, включая регистраторов доменных имен, Whois-сервис, записи DNS и SSL-сертификаты, Group-IB Attack Surface Management устанавливает цифровые связи между различными доменами, IP-адресами и другими доступными из сети активами. При этом конфиденциальная и засекреченная информация не собирается ни при каких обстоятельствах.

Команда Group-IB ASM проанализировала поверхность атаки 250 банков и поставщиков финансовых услуг из разных стран. Выборки из 50 крупнейших компаний были составлены для пяти регионов: Латинская Америка, Европа, Ближний Восток и Северная Африка, Евразия и Центральная Азия, а также Азиатско-Тихоокеанский регион (не включая организации со штаб-квартирами в Китае).

Приведенные в отчете статистические данные отражают среднюю картину для выборки из 50 банков России и стран СНГ. Для целей отчета в выборку были отобраны организации из следующих стран: Армения, Азербайджан, Беларусь, Грузия, Казахстан, Кыргызстан, Молдова, Россия, Таджикистан, Туркменистан, Украина и Узбекистан.

Для определения глобальных эталонных показателей между собой сравнивались средние показатели выборок по каждому из пяти регионов. В каждую выборку было включено 50 крупнейших банков и поставщиков финансовых услуг в соответствующем регионе.

GROUP-IB

СВЯЖИТЕСЬ С КОМАНДОЙ GROUP-IB ДЛЯ ПОЛУЧЕНИЯ ПОЛНОЙ ВИДИМОСТИ ПОВЕРХНОСТИ АТАКИ

GROUP-IB

ПРЕДОТВРАЩЕНИЕ И ИССЛЕДОВАНИЕ КИБЕРПРЕСТУПЛЕНИЙ С 2003 ГОДА

GROUP-IB.RU
INFO@GROUP-IB.COM
BLOG.GROUP-IB.RU
+7 495 984 33 64