POSITIVE TECHNOLOGIES

ЗАО / ПОЗИТИВ ТЕКНОЛОДЖИЗ
107241 / МОСКВА / ЩЕЛКОВСКОЕ ШОССЕ / Д.23А
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

АНАЛИЗ ПРОБЛЕМ ПАРОЛЬНОЙ ЗАЩИТЫ В РОССИЙСКИХ КОМПАНИЯХ

ДМИТРИЙ ЕВТЕЕВ

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Как показывает многолетний опыт компании Positive Technologies по проведению тестирований на проникновение и аудитов информационной безопасности, зачастую, слабая парольная политика или повсеместное ее несоблюдение приводит к возможности компрометации различных участков информационной системы, и как следствие, позволяет реализовать несанкционированный доступ к информации различного уровня критичности.

Несмотря на то, что недостатки однофакторного способа аутентификации с использованием парольной фразы неоднократно озвучивались в «научно-популярной» и специализированной литературе, данный способ является простым, дешевым и наиболее распространенным методом осуществления аутентичности пользователя в большинстве современных информационных систем. Механизмы противодействия угрозам компрометации паролей пользователей также хорошо известны как системным администраторам, так и специалистам в области защиты информации. Однако, достаточно редко встречаются превентивные защитные механизмы в отношении противодействия атакам удаленного подбора паролей. Более того, при хранении паролей в информационных системах, зачастую не используются защитные механизмы, затрудняющие их локальное восстановление[1]. Также эпизодически встречаются Web-приложения, хранение паролей в которых реализовано в виде открытого текста.

Вероятность реализации различного рода угроз ИБ в информационных системах, базирующихся на однофакторной модели аутентификации с использованием парольной фразы, во многом усугубляет присутствие человеческого фактора. Проводимые за рубежом исследования [1] показывают, что в большинстве случаев пользователи используют простые и легко угадываемые пароли для доступа к информационным ресурсам. Данное исследование рассматривает аналогичные проблемы, характерные для Российского пользователя.

2. МЕТОДИКА

Публикация содержит статистику по используемым паролям сотрудниками российских компаний, полученную в ходе работ по тестированиям на проникновение, аудитов безопасности и других работ, выполненных экспертами компании Positive Technologies в 2007-2009 году. Всего в статистику вошли данные более чем о 185 тысячах паролей пользователей.

В зависимости от типа выполняемых работ были задействованы различные методики компрометации учетных записей. От автоматизированного удаленного перебора пароля по словарям методом «черного ящика» (black-box, blind) с использованием сканеров безопасности XSpider и MaxPatrol, до проведения локального аудита используемых паролей на основе полученных значений хешей Microsoft Active Directory, сетевого оборудования Cisco и других хранилищ паролей с использованием rainbow tables [2,3].

[1] Например, повсеместно в Microsoft Active Directory хранятся значения LanManager от используемых пользователями паролей, что позволяет с меньшими усилиями и за короткое время восстановить пароли.

При анализе паролей учитывались следующие характеристики:

- длина пароля;
- используемый набор символов (см. Приложение 1);
- полное или частичное совпадение пароля с именем пользователя (логином);
- наличие пароля в публично распространяемых словарях [4,5].

Помимо этого при анализе паролей учитывались привилегии пользователя в информационной системе и пол человека, использующего анализируемый пароль. Привилегии пользователя оценивались на основе групп безопасности, участником которых являлась учетная запись пользователя на момент проведения соответствующих работ. А пол человека оценивался по используемому логину (имени пользователя) там, где это было возможно.

3. ИСТОЧНИКИ ДАННЫХ

Распределение источников данных для исследования приведено в Табл. 1 и на Рис. 1. При формировании базы для исследования использовались как внешние источники данных, доступные со стороны сети Интернет, так и внутренние информационные ресурсы, доступные только со стороны внутренних сетей. Примером внешних источников данных являются Web-приложения, сетевые сервисы (POP, IMAP и др.) и сетевое оборудование (коммутаторы, маршрутизаторы и т.п.). Примером внутренних источников данных, помимо уже перечисленных, также являются службы каталогов Microsoft Active Directory.

Таблица 1. Распределение источников

Источник	Доля, %
Web-приложения	59
Службы каталогов Microsoft Active Directory	35
Сетевые сервисы (POP, IMAP и др.)	1
Сетевое оборудование	1
Другие	4

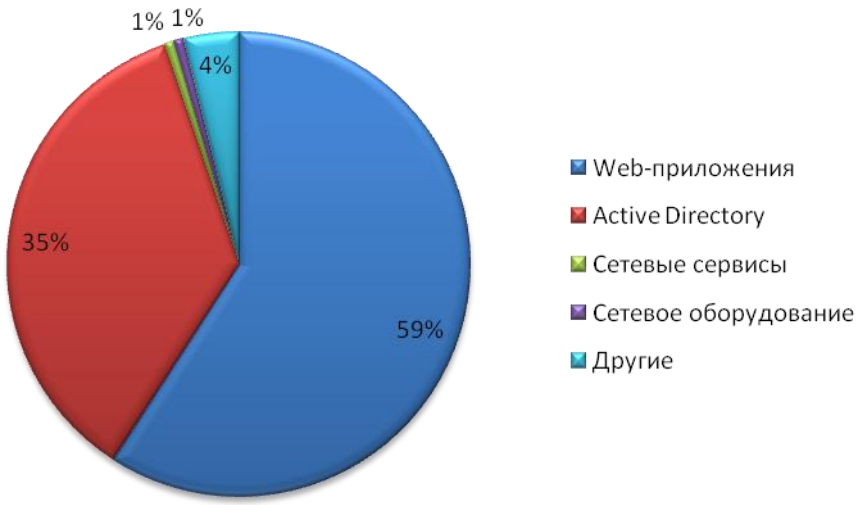

Рисунок 1. Распределение источников

Подобное распределение источников связано с тем, что во многих исследуемых Web-приложениях при проведении тестирований на проникновение, было обнаружено хранение паролей пользователей без применения какой-либо криптографии, т.е. все пароли хранились в виде открытого текста. Также большой объем данных для исследования был получен в рамках проведения парольных аудитов Active Directory с использованием rainbow tables [2].

4. СТАТИСТИКА ПАРОЛЕЙ, ИСПОЛЬЗУЕМЫХ ПОЛЬЗОВАТЕЛЯМИ

Всего в представленную статистику вошли данные более чем о 185 тысячах паролей пользователей. TOP 10 наиболее часто используемых паролей Российскими пользователями приведен в Табл. 2.

Таблица 2. TOP 10 наиболее часто используемых паролей Российскими пользователями

Пароль	Позиция	Доля, %
1234567	1	3,36%
12345678	2	1,65%
123456	3	1,02%
Пустая строка	4	0,72%
12345	5	0,47%
7654321	6	0,31%

qweasd	7	0,27%
123	8	0,25%
qwerty	9	0,25%
123456789	10	0,23%

Проводя параллель между данными исследований, проводимых за рубежом, [1] и полученными результатами проведенного исследования в отношении используемых паролей российскими пользователями можно отметить, что результаты обоих исследований во многом расходятся. Так, полюбившийся пароль «password» (вторая позиция наиболее распространенных паролей) зарубежному пользователю, содержится на 135-й позиции по результатам исследования паролей российских пользователей. А популярное слово в качестве пароля «pussy», которое по данным Марка Бернетта занимает пятую строчку наиболее распространенных паролей, не используется российскими пользователями вообще. С другой стороны, пользователи российских компаний предпочитают использовать в качестве паролей наборы, расположенных рядом символов на клавиатуре, такие как 1234567, 12345678, qweasd, qwerty и т.д. Также было замечено, что в случае, когда информационная система никак не ограничивала пользователя в творческом процессе создания пароля (ограничение на длину и сложность задаваемого пароля), то пользователи с успехом использовали пустые строки в качестве своего пароля. Таким образом, пустая строка занимает четвертое место в рейтинге данного исследования.

4.1. Суммарная статистика

Суммарная статистика по используемым наборам символов в паролях приведена в Табл. 3 и на Рис. 2 (полностью таблица с суммарной статистикой приведена в Приложении 2). Принадлежность пароля к определенному набору символов оценивалась по наборам, приведенным в Приложении 1.

Таблица 3. Суммарная статистика по используемым наборам символов в паролях

Набор символов	Доля, %
Только цифры (numeric)	52,73%
Символы английского алфавита в нижнем регистре (loweralpha)	17,96%
Символы английского алфавита в нижнем регистре и цифры (loweralpha-numeric)	17,51%
Символы английского алфавита в разных регистрах и цифры (mixalpha-numeric)	3,4%
Символы английского алфавита в разных регистрах (mixalpha)	1,63%
Символы английского алфавита в верхнем регистре и цифры (alpha-numeric)	1,35%
Символы русского алфавита в нижнем регистре (loweralpha-rus)	1,12%

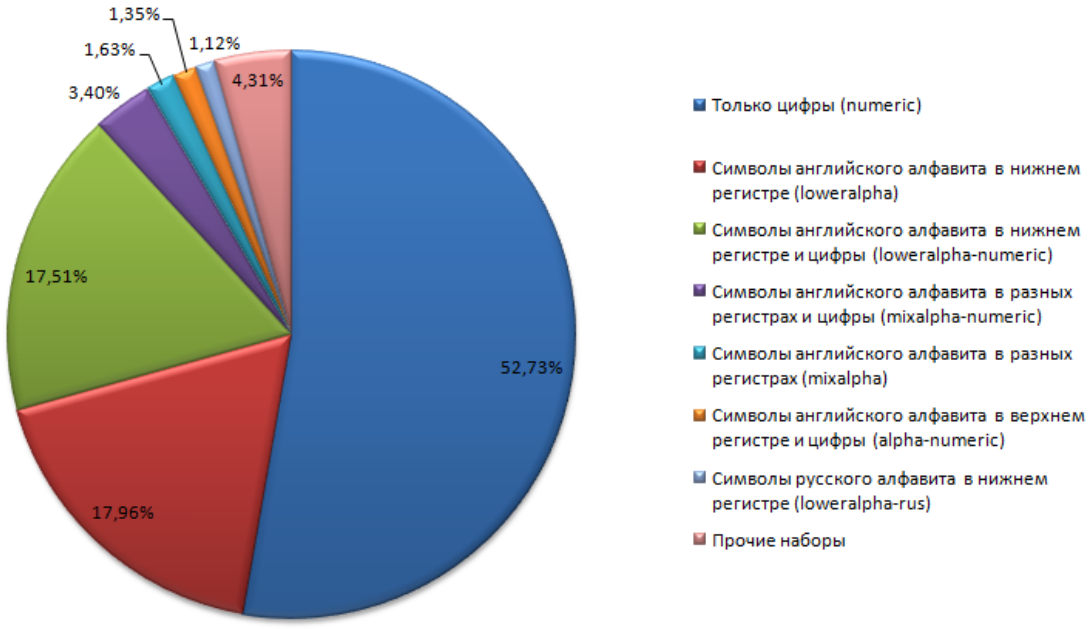

Рисунок 2. Суммарная статистика по используемым наборам символов в паролях

Наиболее распространенными паролями у российских пользователей являются цифровые пароли, на долю которых приходится около 53% от числа всех проанализированных паролей. Забегая немного вперед, хочется добавить, что анализ длины используемых паролей показывает, что в большинстве случаев пароли не превышают восьми символов. Подобная ситуация позволяет с высокой долей вероятности успешно проводить атаки типа «Удаленный перебор паролей» (Brute-force) в тех случаях, когда не используются различного рода превентивные механизмы, затрудняющие реализацию этой атаки.

Вторым по популярности набором используемых символов в своих паролях является набор из символов английского алфавита в нижнем регистре, на долю которого приходится до 18% от числа всех проанализированных паролей.

С небольшим отрывом по популярности следуют аналогичные предыдущему набору символов пароли, состоящие из символов английского алфавита в нижнем регистре, но с усложнением пароля за счет использования в нем цифр. Пароли, состоящие из символов английского алфавита в нижнем регистре и цифр, встретились в 17% от числа всех проанализированных паролей.

Таким образом, около 88% паролей, используемых сотрудниками российских компаний – это пароли, содержащие в себе либо цифры, либо символы английского алфавита в нижнем регистре, либо и то и другое.

Стоит отметить, что из всех проанализированных паролей, не было замечено ни одного пароля, который бы соответствовал следующим наборам символов:

- Символы русского алфавита в верхнем регистре и пробел (alpha-space-rus);
- Символы русского алфавита в верхнем регистре, цифры и пробел (alpha-numeric-space-rus);
- Символы русского алфавита в верхнем регистре, цифры, спец. символы и пробел (alpha-numeric-symbol14-space-rus);

- Символы русского алфавита в нижнем регистре, цифры, спец. символы и пробел (loweralpha-numeric-symbol14-space-rus);
- Символы русского алфавита в разных регистрах и пробел (mixalpha-numeric-space-rus).

Если же рассматривать суммарную статистику по длине используемых паролей, то будут получены данные, приведенные в Табл. 4, на Рис. 3 и на Рис. 4.

Таблица 4. Суммарная статистика по длине используемых паролей

Количество символов	Доля, %	Вероятность компрометации пароля длинной N[1], %	Вероятность компрометации пароля по словарю от 0-N символов[2], %
0	0,71%	100%	0,71%
1	0,26%	99,29%	0,97%
2	0,39%	99,03%	1,36%
3	1,37%	98,64%	2,73%
4	2,03%	97,27%	4,76%
5	4,86%	95,24%	9,62%
6	27,22%	90,38%	36,84%
7	21,75%	63,16%	58,59%
8	25,22%	41,41%	83,81%
9	6,5%	16,19%	90,31%
10	4,42%	9,69%	94,73%
11	2,83%	5,27%	97,56%
12	1,33%	2,44%	98,89%
13	0,4%	1,11%	99,29%
14	0,34%	0,71%	99,63%

[1] Под вероятностью компрометации пароля длинной N символов подразумевается оценка вероятности компрометации пароля в реальных условиях.

[2] Под вероятностью компрометации пароля по словарю от 0 до N символов подразумевается теоретическая вероятность компрометации пароля при использовании словаря от 0 до N символов без учета фактора времени, потраченного на подбор.

15	0,1%	0,37%	99,73%
16	0,09%	0,27%	99,82%
17	0,02%	0,18%	99,84%
18	0,01%	0,16%	99,85%
19	0,01%	0,15%	99,86%
20	0,008%	0,14%	99,87%
>20	0,02%	0,13%	99,89%

* При расчетах использовалось математическое округление до двух знаков.

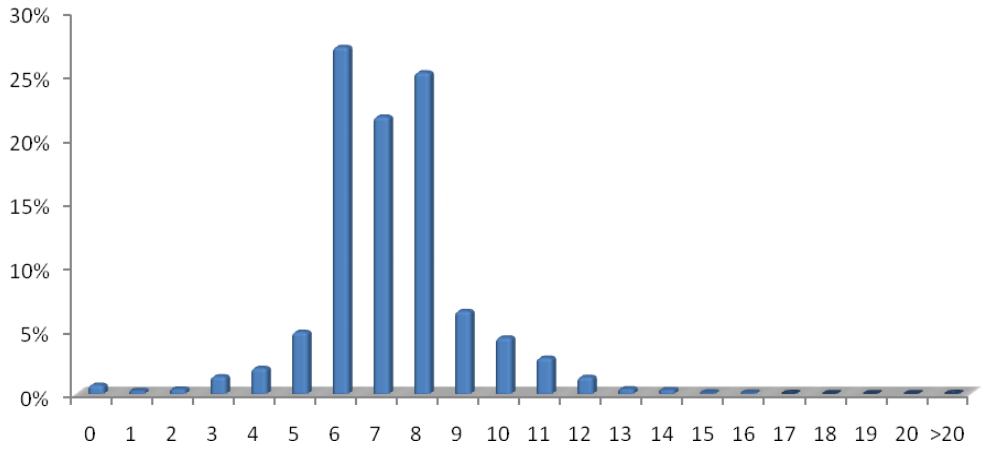

Рисунок 3. Суммарная статистика по длине используемых паролей

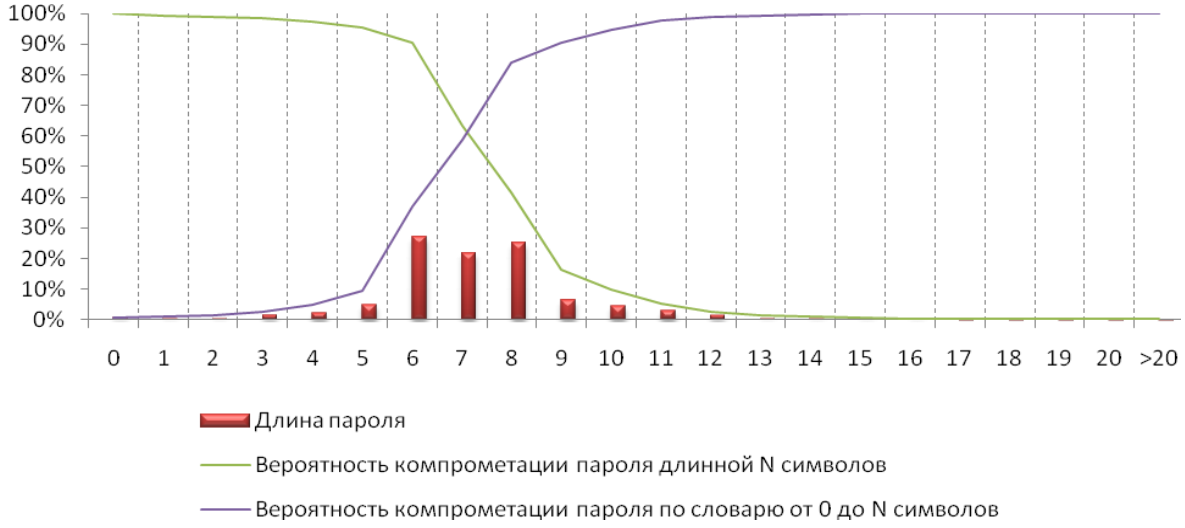

Рисунок 4. Суммарная статистика по длине используемых паролей с вероятностью их компрометации

То есть, используемые пароли российскими пользователями в большинстве случаев не превышают 8-ми символов, и лишь единицы используют пароли длиннее 12-ти символов. Также стоит отметить, что используемые пароли до 8-ми символов с высокой долей вероятности могут быть скомпрометированы в реальных условиях.

Если же рассматривать наиболее «слабые пароли», то будут получены данные, представленные в Табл. 5 и на Рис. 5.

Таблица 5. Суммарная статистика по паролям низкой стойкости

Причина низкой стойкости	Доля, %
Полное совпадение пароля с именем пользователя	3,94%
Частичное совпадение пароля с именем пользователя	0,7%
Пароль содержится в публично распространяемых словарях	14,69%
Пароль является пустой строкой	0,7%

Рисунок 5. Суммарная статистика по паролям низкой стойкости

Таким образом, до 4% от числа всех проанализированных паролей полностью совпадают с используемым логином, а около 15% содержатся в публично распространяемых словарях [4,5]. Подобная ситуация в значительной степени упрощает процесс реализации несанкционированного доступа злоумышленнику, действующему удаленно.

Если же рассматривать вероятность компрометации пароля пользователя с использованием словарей, то будут получены данные, представленные на Рис. 6. А для случая, когда используется стандартная политика требований сложности задаваемых паролей в ОС Microsoft (Windows 2000 и выше), вероятность компрометации пароля пользователя с использованием словарей будет выглядеть, как показано на Рис. 7.

Под стандартной политикой сложности задаваемых паролей подразумевается включенный параметр «Пароль должен отвечать требованиям сложности» [6], настраиваемый в групповых политиках ОС. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:

- Не должен содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;
- Иметь длину не менее 6 знаков;

Содержать знаки трех из четырех перечисленных ниже категорий:

- Латинские заглавные буквы (от A до Z);
- Латинские строчные буквы (от a до z);
- Цифры (от 0 до 9);
- Отличающиеся от букв и цифр знаки (например, !, $, #, %).

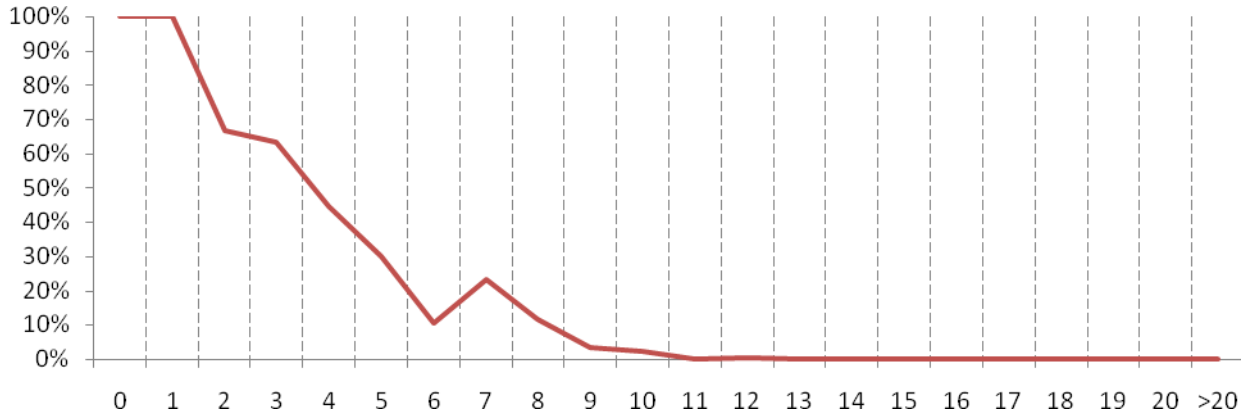

Рисунок 6. Вероятность компрометации паролей определенной длины по словарям

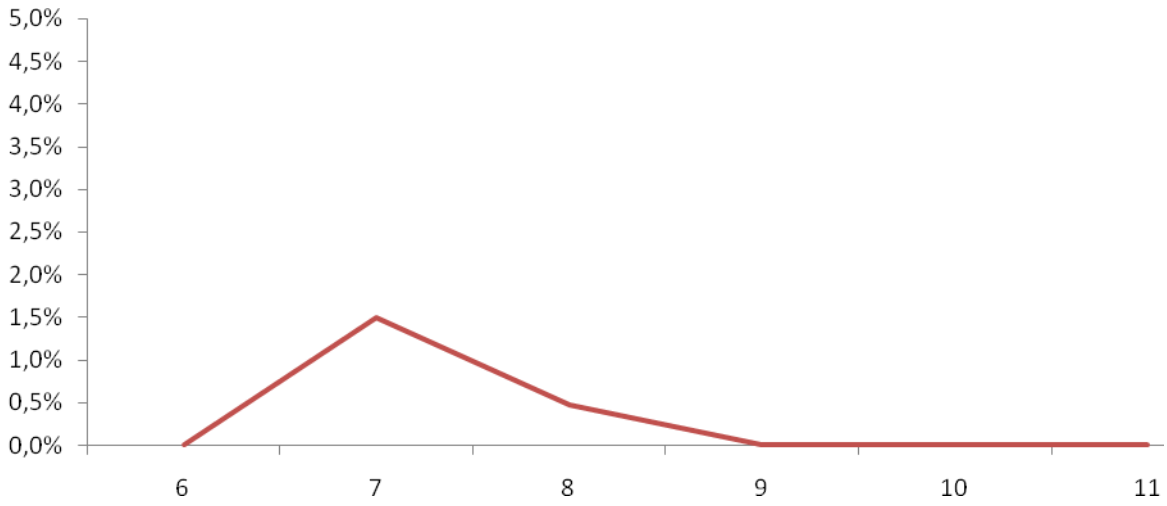

Рисунок 7. Вероятность компрометации паролей определенной длины по словарям с учетом требований сложности к паролям

То есть, использование стандартной политики требований сложности задаваемых паролей в ОС Microsoft, в значительной степени затрудняет компрометацию учетных записей удаленным злоумышленником с использованием словарей.

Если же рассматривать вероятность компрометации пароля пользователя по разным наборам символов с использованием тех же словарей, то будут получены данные, представленные на Рис. 8.

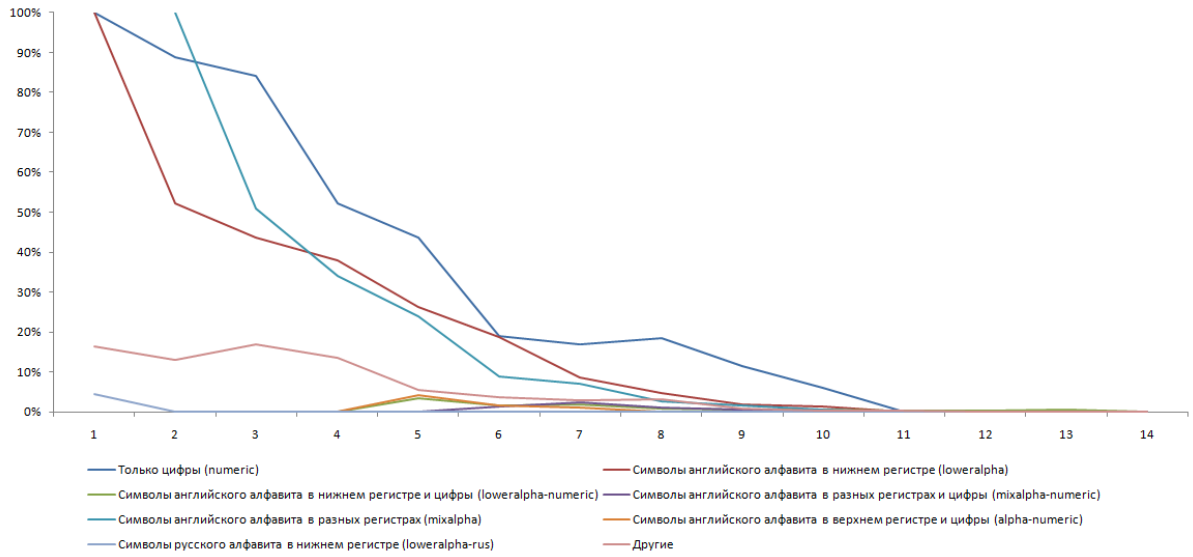

Рисунок 8. Вероятность компрометации паролей определенной длины для разного набора символов по словарям

Таким образом, для атаки по словарю, наиболее стойким паролем по Рис. 8 оказался пароль, состоящий из символов русского алфавита в нижнем регистре (loweralpha-rus). Маловероятна и компрометация паролей, в которых используются символы английского алфавита в разных регистрах и цифры (mixalpha-numeric), и символы английского алфавита в верхнем регистре и цифры (alpha-numeric), что по большому счету было ожидаемым результатом.

Если же брать во внимание, что 6-ти символьный цифровой пароль – это всего 1.000.000 всех возможных комбинаций, то логично было бы предположить высокую эффективность осуществления удаленной атаки на цифровые пароли по всем возможным комбинациям. Учитывая этот факт, вероятность компрометации цифрового пароля состоящего из N-символов с использованием цифровых словарей будет иметь вид, как показано на Рис. 9.

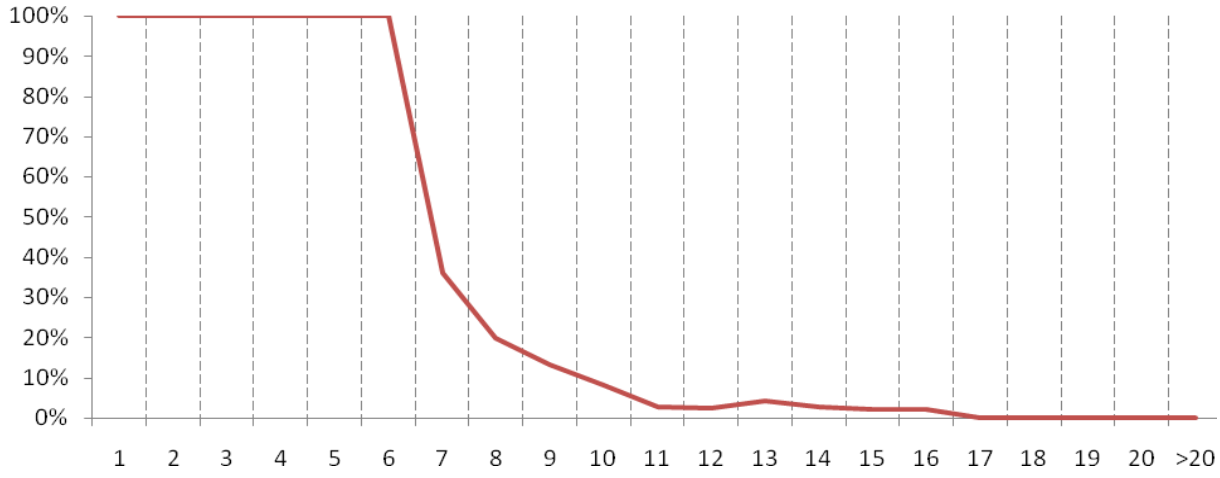

Рисунок 9. Вероятность компрометации цифровых паролей определенной длины для разного набора символов по словарям

Таким образом, удаленная атака по словарям позволяет скомпрометировать 37% из числа всех анализируемых паролей.

4.2. Статистика по паролям, используемым администраторами ИС

В данном разделе рассматриваются используемые пароли администраторами информационных систем, в том числе:

- пароли администраторов с привилегиями «Администратора домена» (Domain Admins) в контексте Microsoft Active Directory;
- пароли локальных администраторов в операционных системах (Windows/*nix);
- пароли учетных записей к сетевому оборудованию (коммутаторы, маршрутизаторы и т.п.);
- пароли администраторов в Web-приложениях.

Статистика по используемым наборам символов в паролях учетных записей с повышенными привилегиями в информационных системах приведена в Табл. 6 и на Рис. 10.

Таблица 6. Статистика по используемым наборам символов в паролях администраторов

Набор символов	Доля, %
Символы английского алфавита в нижнем регистре (loweralpha)	26,11%
Символы английского алфавита в нижнем регистре и цифры (loweralpha-numeric)	22,29%
Символы английского алфавита в разных регистрах и цифры (mixalpha-numeric)	17,83%
Только цифры (numeric)	9,55%
Символы английского алфавита в нижнем регистре, цифры и спец. символы (loweralpha-numeric-symbol14)	8,28%
Символы английского алфавита в разных регистрах, цифры и спец. символы (mixalpha-numeric-symbol14)	4,46%
Символы английского алфавита в разных регистрах (mixalpha)	3,18%
Символы английского алфавита в верхнем регистре, цифры и спец. символы (alpha-numeric-symbol14)	1,91%
Пустая строка (NULL)	1,91%
Символы английского алфавита в нижнем регистре, цифры, спец. Символы и пробел (loweralpha-numeric-symbol32-space)	1,27%
Символы английского алфавита в разных регистрах, цифры, спец. символы и пробел (mixalpha-numeric-all-space)	1,27%

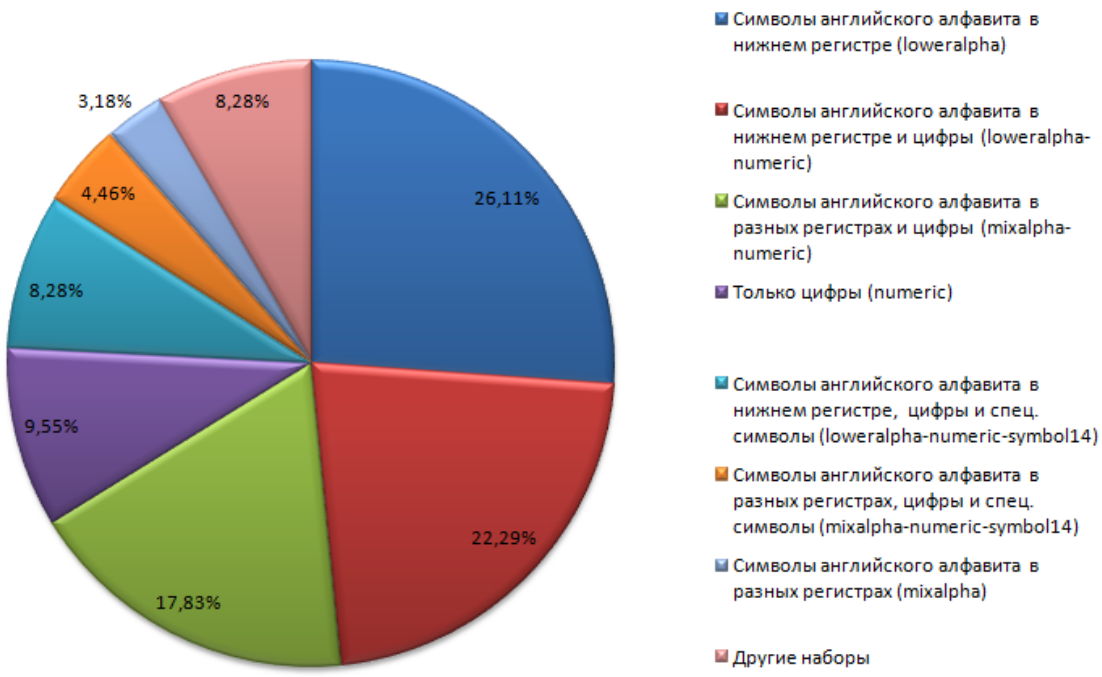

Рисунок 10. Статистика по используемым наборам символов в паролях администраторов

В отличие от непривилегированных учетных записей, пользователи с административными привилегиями в информационных системах используют более сложные пароли. Так, цифровые пароли используются администраторами в 9% случаев, а пароли, содержащие символы английского алфавита и/или усложнены цифрами, в 48% случаев. И, около 34% паролей, используемых администраторами информационных систем, содержат в себе наборы символов, которые в значительной степени затрудняют проведение удаленной атаки по перебору таких паролей.

Примечателен также факт использования администраторами пустых паролей для доступа к информационным системам. Это связано с тем, что наибольшее число проблем, связанных с несоблюдением парольной политики во внутренних сетях, встречается в сетевом оборудовании (коммутаторы, маршрутизаторы и др.), для доступа к которым аутентификация, зачастую, не используется вовсе [7].

Статистика по длине паролей учетных записей с повышенными привилегиями в информационных системах приведена в Табл. 7, на Рис. 11 и на Рис. 12.

Таблица 7. Статистика по длине паролей используемых администраторами

Количество символов	Доля, %	Вероятность компрометации пароля длинной N[1], %	Вероятность компрометации пароля по словарю от 0-N символов[2], %
0	1,91%	100%	1,91%
1	0%	98,09%	1,91%
2	0,63%	98,09%	2,54%
3	0,63%	97,46%	3,17%
4	3,18%	96,83%	6,35%
5	10,82%	93,65%	17,17%
6	8,91%	82,83%	26,08%
7	8,28%	73,92%	34,36%
8	19,1%	65,64%	53,46%
9	11,46%	46,54%	64,92%
10	11,46%	35,08%	76,38%
11	9,55%	23,62%	85,93%
12	3,82%	14,07%	89,75%
13	4,45%	10,25%	94,2%
14	2,54%	5,8%	96,74%
15	0%	3,26%	96,74%
16	0,63%	3,26%	97,37%
17	0%	2,63%	97,37%
18	0,63%	2,63%	98%

[1] Под вероятностью компрометации пароля длинной N символов подразумевается оценка вероятности компрометации пароля в реальных условиях.

[2] Под вероятностью компрометации пароля по словарю от 0 до N символов подразумевается теоретическая вероятность компрометации пароля при использовании словаря от 0 до N символов без учета фактора времени, потраченного на подбор.

19	1,27%	2%	99,27%
20	0%	0,73%	99,27%
>20	0,63%	0,73%	99,9%

* При расчетах использовалось математическое округление до двух знаков.

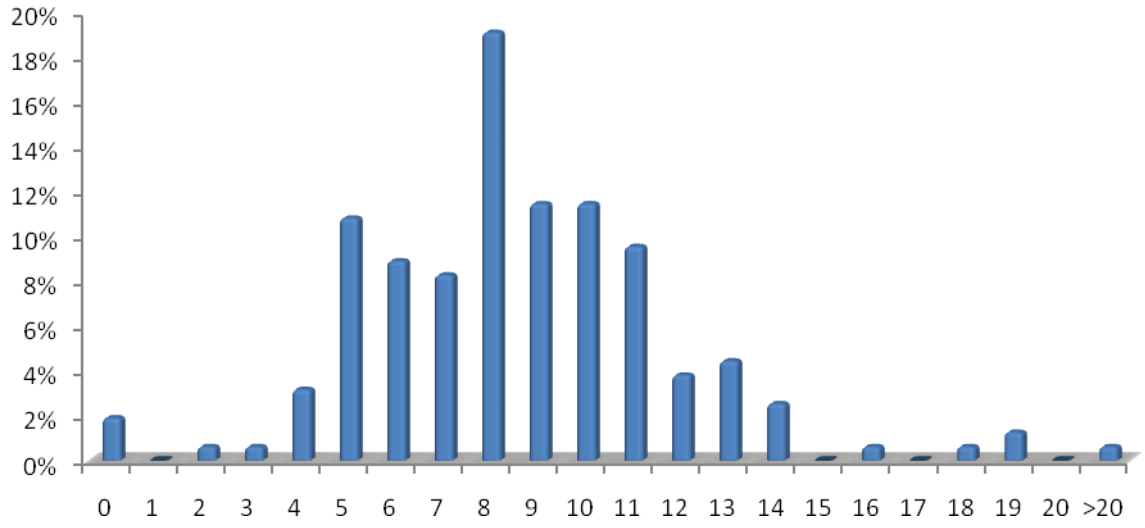

Рисунок 11. Статистика по длине паролей используемых администраторами

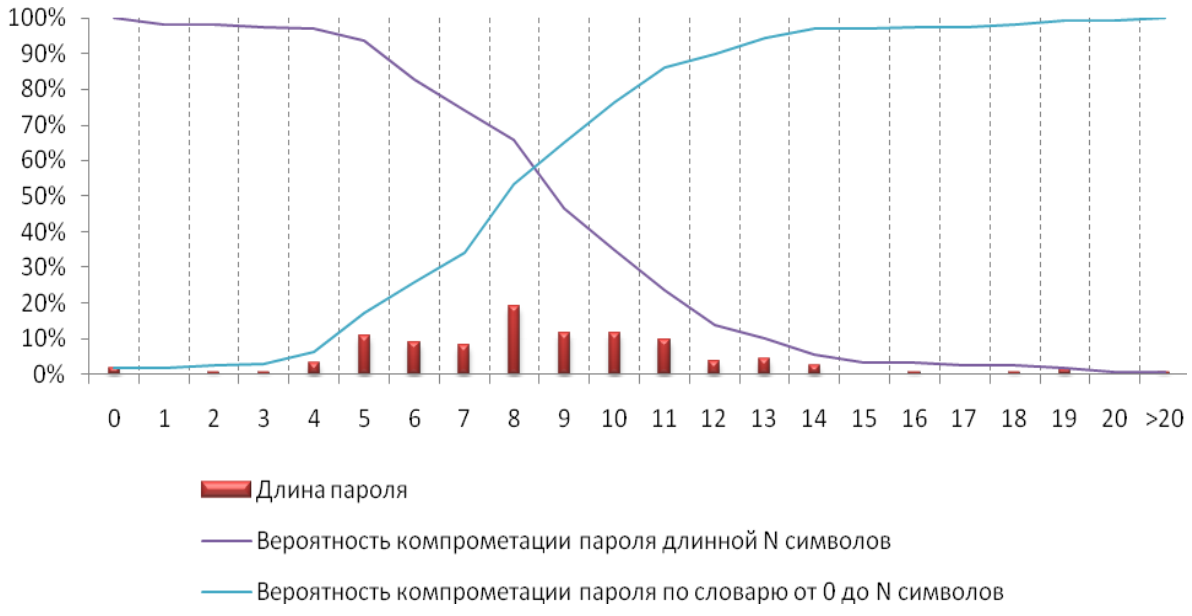

Рисунок 12. Статистика по длине паролей используемых администраторами с вероятностью их компрометации

То есть, в большей степени, администраторами используются пароли, состоящие от 8-ми до 10-ти символов. В совокупности с широкими наборами символов (см. Рис. 10), подобные пароли являются достаточно стойкими как для удаленного перебора, так и для их локального восстановления при проведении атаки по перебору всех возможных значений «в лоб».

Если же рассматривать наиболее слабые пароли, используемые администраторами, то будут получены данные, приведенные в Табл. 8 и на Рис. 13.

Таблица 8. Статистика по паролям низкой стойкости у администраторов

Причина низкой стойкости	Доля, %
Полное совпадение пароля с именем пользователя	10,19%
Частичное совпадение пароля с именем пользователя	0,63%
Пароль содержится в публично распространяемых словарях	15,28%
Пароль является пустой строкой	1,91%

Рисунок 13. Статистика по паролям низкой стойкости у администраторов

Таким образом, в 28% случаев для учетных записей с повышенными привилегиями используются пароли низкой стойкости. Это позволяет злоумышленнику, действующему удаленно, за короткое время скомпрометировать атакуемую информационную систему, и, возможно, воспользоваться полученными данными для проведения атак на другие ресурсы исследуемой сети. Вероятность наступления подобного события приведена на Рис. 14.

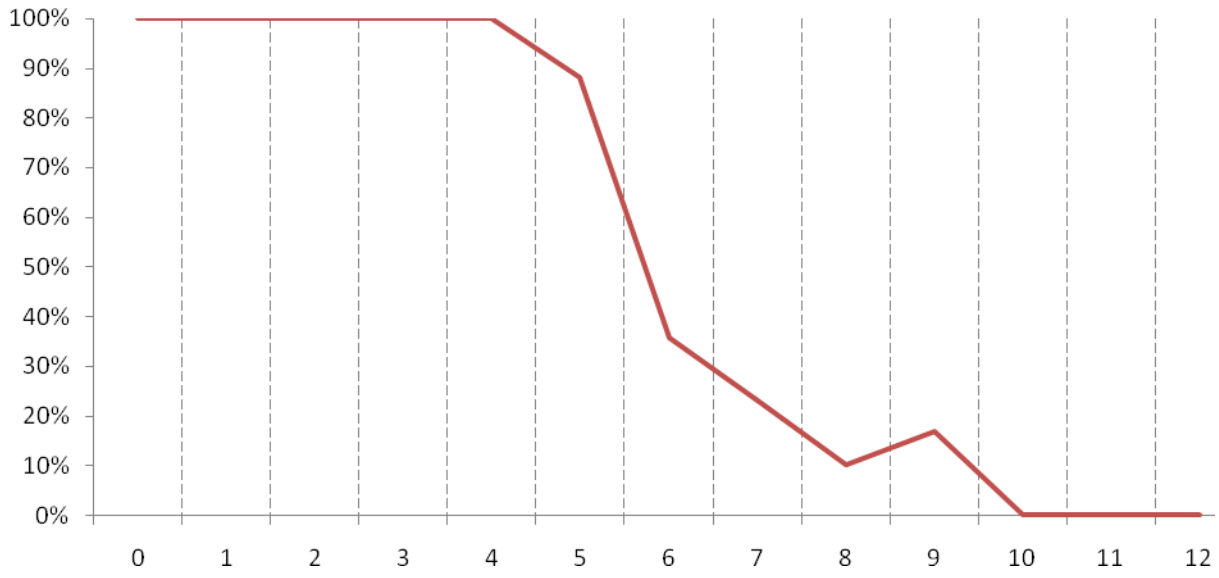

Рисунок 14. Вероятность компрометации пароля администратора длинной N-символов

4.3. Оценка используемых паролей в соответствие с требованиями PCI DSS

Рассматривая проблему использования «слабых» паролей в контексте соответствия требованиям стандарта по защите информации в индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard) [8], можно выделить требования, приведенные в Табл. 9, регламентирующие использование стойких паролей в информационной системе.

Таблица 9. Требования PCI DSS, регламентирующие правила использования паролей

Требование PCI DSS v.1.2	Процедура
2.1 До подключения системы к сети должны быть изменены параметры, заданные производителем по умолчанию (например, пароли, SNMP-строки), а также удалены не используемые учетные записи	Определить выборку системных компонентов, критичных серверов и беспроводных точек доступа и попытаться выполнить процедуру входа на этих устройствах (при поддержке системного администратора) с использованием учетных записей и паролей, заданных производителем, для того чтобы удостовериться, что учетные записи и пароли, заданные производителем по умолчанию, изменены (для поиска учетных записей и паролей, заданных производителем по умолчанию, можно использовать документацию производителя и сеть Интернет)
8.5.10 Длина паролей должна составлять не менее 7 символов	Для выборки системных компонентов просмотреть конфигурационные настройки систем и убедиться, что настройки парольной политики пользователей установлены таким образом, что длина паролей должна составлять не менее 7 символов. Только для сервис-провайдеров: ознакомиться с внутренними процессами и документацией для пользователей/клиентов и убедиться, что пароли клиентов должны удовлетворять требованиям к минимальной длине пароля.
8.5.11 Пароли должны содержать как цифры, так и буквы	Для выборки системных компонентов просмотреть конфигурационные настройки систем и убедиться, что настройки парольной политики пользователей установлены таким образом, что пароли должны содержать как цифры, так и буквы. Только для сервис-провайдеров: ознакомиться с внутренними процессами и документацией для пользователей/клиентов и убедиться, что пароли клиентов должны содержать как цифры, так и буквы.

Оценивая полученную статистику используемых паролей сотрудниками российских компаний по приведенным критериям в Табл. 9, будут получены данные, представленные в Табл. 10, на Рис. 15 и на Рис. 16.

Таблица 10. Оценка используемых паролей в соответствие с требованиями PCI DSS

Требование PCI DSS v.1.2	Суммарная доля не соответствия, %	Доля не соответствия для паролей администраторов, %
2.1 До подключения системы к сети должны быть изменены параметры, заданные производителем по умолчанию (например, пароли, SNMP-строки), а также удалены не используемые учетные записи[1]	1%	10%
8.5.10 Длина паролей должна составлять не менее 7 символов	37%	26%
8.5.11 Пароли должны содержать как цифры, так и буквы	74%	39%

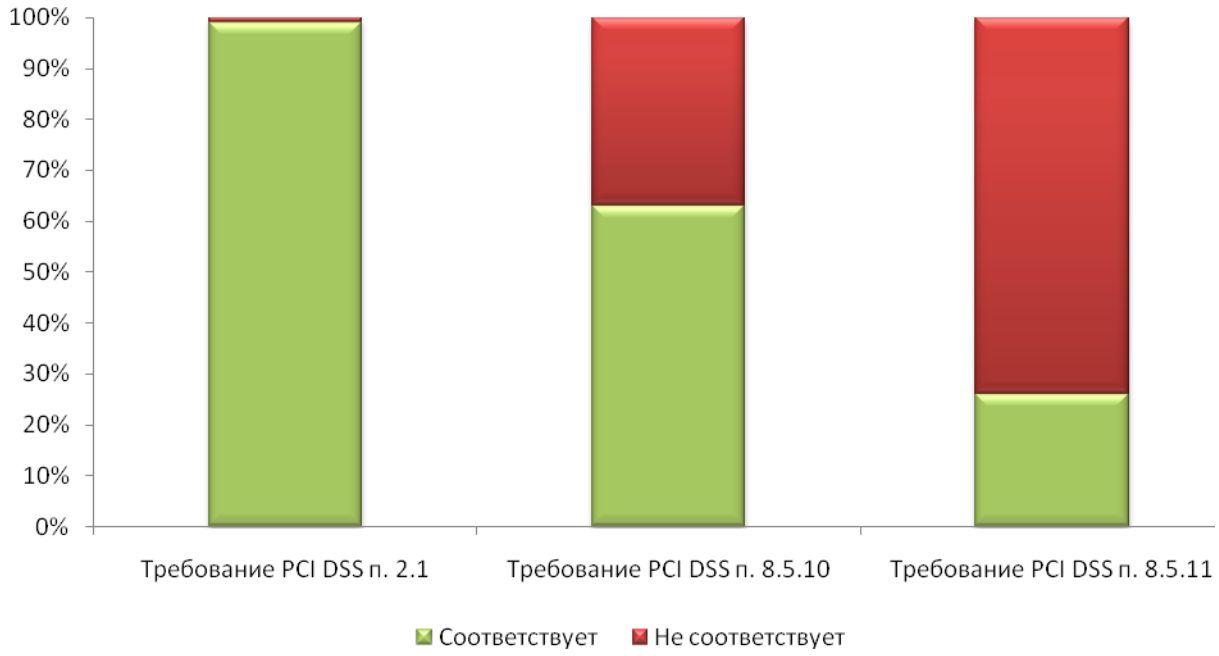

Рисунок 15. Оценка соответствия требованиям PCI DSS в отношении всех анализируемых паролей

[1] Требование оценивалось по списку паролей, доступных на странице: http://www.phenoelit-us.org/dpl/dpl.html

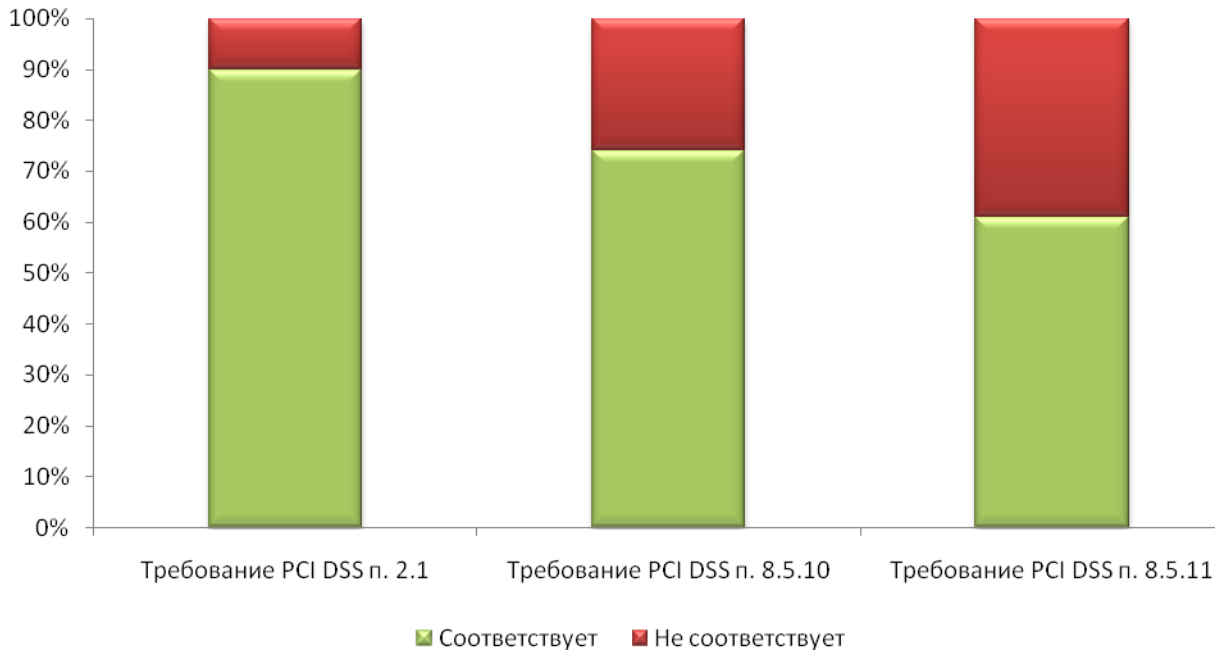

Рисунок 16. Оценка соответствия требованиям PCI DSS в отношении паролей администраторов

То есть, 74% используемых паролей пользователями в корпоративном секторе не соответствуют требованиям стандарта PCI DSS.

4.4. Анализ используемых паролей в зависимости от пола пользователя

При проведении исследования используемых паролей российскими пользователями в зависимости от имени пользователя (логина) делалось предположение о половой принадлежности человека, использующего анализируемый пароль. В данный раздел не вошли сервисные учетные записи и учетные записи общего пользования (например, admin, test и т.д.).

Статистика по используемым наборам символов в своих паролях в зависимости от пола пользователя приведена в Табл. 11, на Рис. 17 и на Рис. 18.

Таблица 11. Статистика по используемым наборам символов в зависимости от пола пользователя

Набор символов	Доля, % у мужчин	Доля, % у женщин
Только цифры (numeric)	57,98%	60,76%
Символы английского алфавита в нижнем регистре и цифры (loweralpha-numeric)	17,05%	14,11%
Символы английского алфавита в нижнем регистре (loweralpha)	16,37%	17,27%
Символы английского алфавита в разных регистрах и цифры (mixalpha-numeric)	2,11%	1,96%

Символы русского алфавита в нижнем регистре (loweralpha-rus)	1,33%	1,63%
Символы английского алфавита в разных регистрах (mixalpha)	1,33%	1,02%

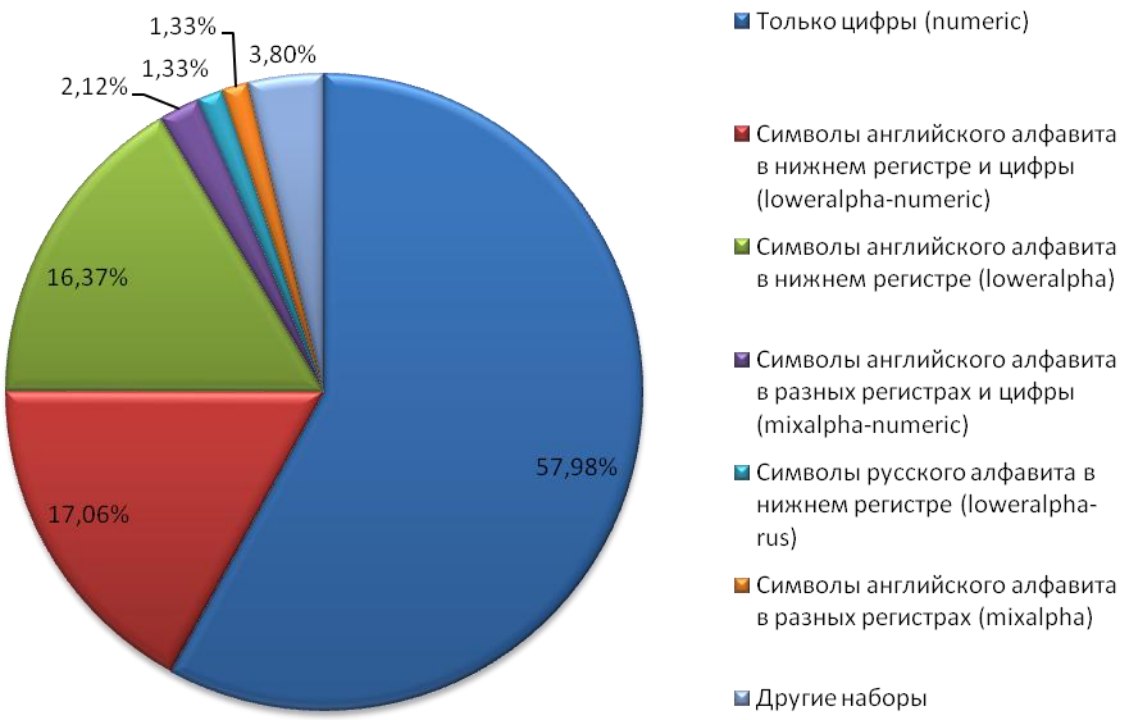

Рисунок 17. Статистика по используемым наборам символов у мужчин

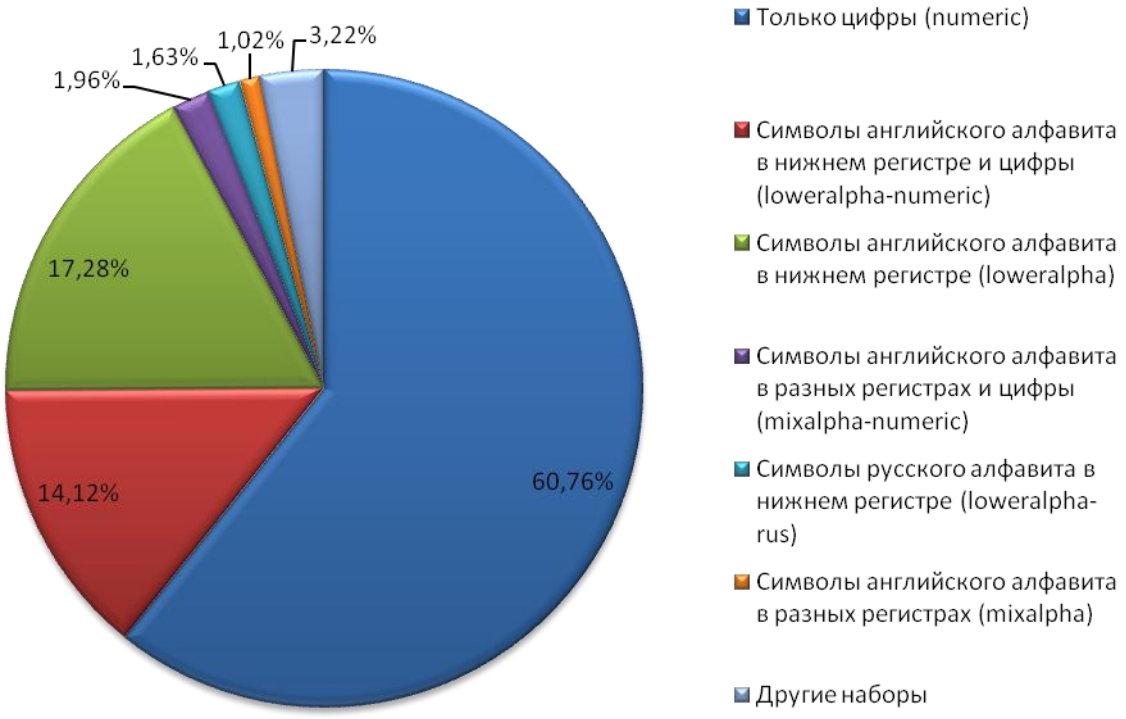

Рисунок 18. Статистика по используемым наборам символов у женщин

Таким образом, разница между выбираемыми символами при создании пароля между разными полами практически не прослеживается. Наиболее распространенными как у мужчин, так и у женщин, являются цифровые пароли, на долю которых приходится приблизительно 58-60% от числа всех проанализированных паролей.

Статистика по длине используемых паролей в зависимости от пола пользователя приведена в Табл. 11, на Рис. 19 и на Рис. 20.

Таблица 11. Статистика по длине используемых паролей в зависимости от пола пользователя

Количество символов	Доля, % у мужчин	Вероятность компрометации пароля длинной N у мужчин, %[1]	Вероятность компрометации пароля по словарю от 0-N символов у мужчин, %[2]	Доля, % у женщин	Вероятность компрометации пароля длинной N у женщин, %	Вероятность компрометации пароля по словарю от 0-N символов у женщин, %
0	0%	100%	0%	0,02%	100%	0,02%
1	0,02%	100%	0,02%	0%	100%	0,02%
2	0,07%	99,98%	0,09%	0,02%	100%	0,04%
3	0,06%	99,91%	0,15%	0,1%	99,98%	0,14%
4	0,18%	99,85%	0,33%	2,52%	99,88%	0,28%
5	4,56%	99,67%	4,89%	3,76%	97,36%	4,04%
6	35,23%	95,11%	40,12%	39,41%	93,6%	43,45%
7	20,22%	59,88%	60,34%	17,03%	54,19%	60,48%
8	21,97%	39,66%	82,31%	20,65%	37,16%	81,13%
9	6,25%	17,69%	88,56%	5,92%	16,51%	87,05%
10	5,15%	11,44%	93,71%	4,9%	10,59%	91,95%
11	3,7%	6,29%	97,41%	3,24%	5,69%	95,19%
12	1,53%	2,59%	98,94%	1,17%	2,45%	96,36%
13	0,4%	1,06%	99,34%	0,3%	1,28%	96,66%
14	0,27%	0,66%	99,61%	0,34%	0,98%	97%

[1] Под вероятностью компрометации пароля длинной N символов подразумевается оценка вероятности компрометации пароля в реальных условиях.

[2] Под вероятностью компрометации пароля по словарю от 0 до N символов подразумевается теоретическая вероятность компрометации пароля при использовании словаря от 0 до N символов без учета фактора времени, потраченного на подбор.

15	0,12%	0,39%	99,73%	0,13%	0,64%	97,13%
16	0,11%	0,27%	99,84%	0,32%	0,51%	97,45%
17	0,02%	0,16%	99,86%	0,04%	0,19%	97,49%
18	0,02%	0,14%	99,88%	0,02%	0%	97,51%
19	0,01%	0,12%	99,89%	0%	0%	97,51%
20	0,01%	0,11%	99,9%	0%	0%	97,51%
>20	0,01%	0,1%	99,91%	0,02%	0%	97,53%

* При расчетах использовалось математическое округление до двух знаков.

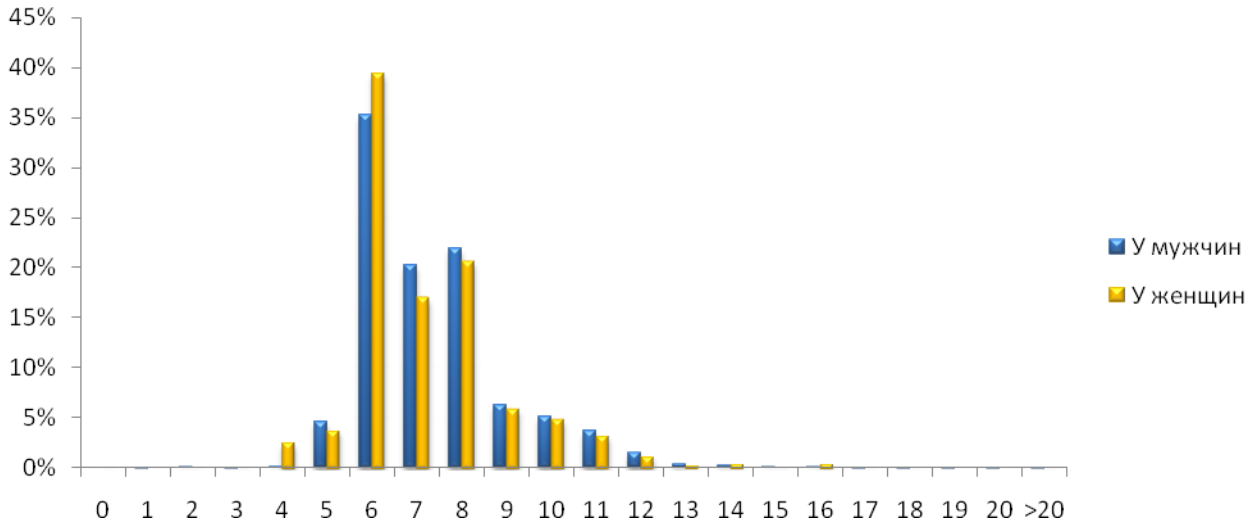

Рисунок 19. Статистика по длине используемых паролей в зависимости от пола пользователя

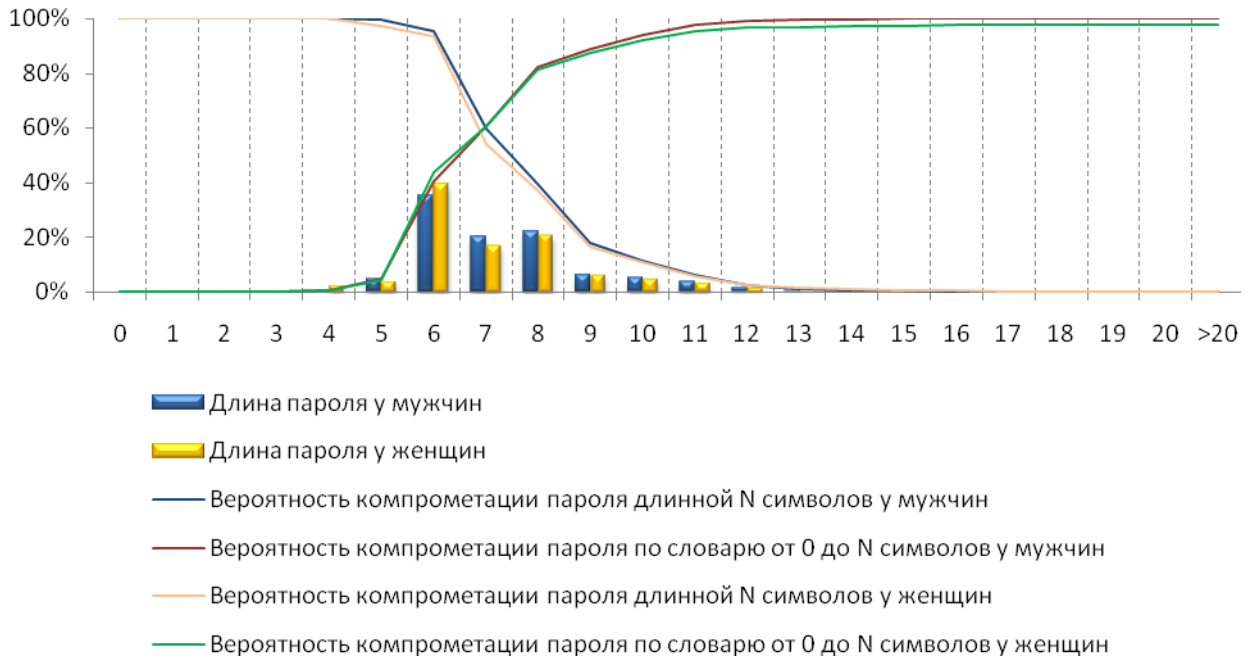

Рисунок 20. Статистика по длине используемых паролей в зависимости от пола пользователя с вероятностью их компрометации

Аналогичным образом разница в используемой длине пароля разными полами также не прослеживается. И те и другие предпочитают использовать пароли от 6-ти и до 8-ми символов.

Статистика по паролям низкой стойкости в зависимости от пола пользователя приведена в Табл. 12 и на Рис. 21.

Таблица 12. Статистика по паролям низкой стойкости в зависимости от пола пользователя

Причина низкой стойкости	Доля, % у мужчин	Доля, % у женщин
Полное совпадение пароля с именем пользователя	4,47%	3,94%
Частичное совпадение пароля с именем пользователя	0,85%	0,74%
Пароль содержится в публично распространяемых словарях	2,3%	13,11%

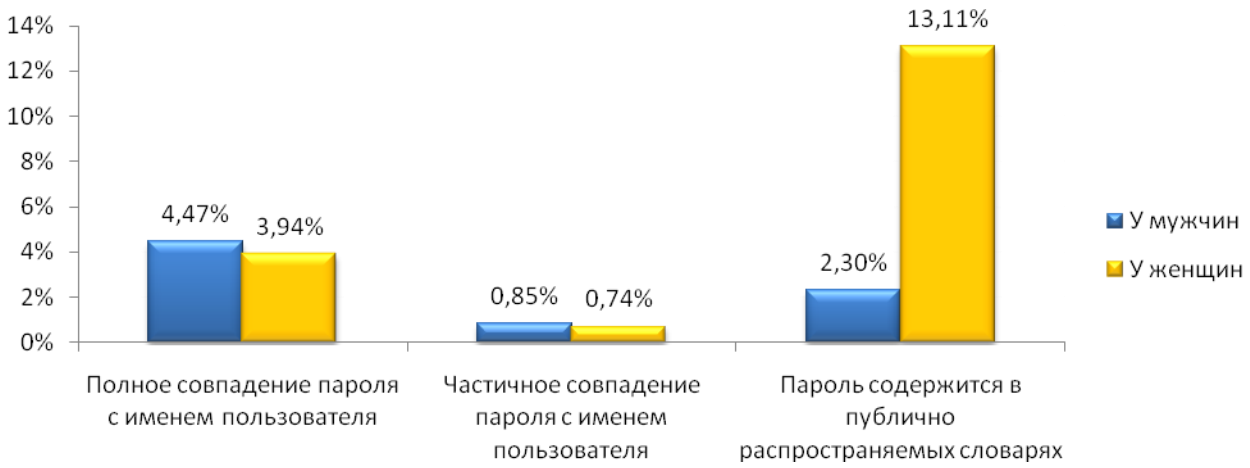

Рисунок 21. Статистика по паролям низкой стойкости в зависимости от пола пользователя

То есть, пароли, используемые женщинами, являются несколько более уязвимыми для атакующего. Благодаря более частому использованию женщинами словарных паролей удаленному злоумышленнику в среднем требуется меньше времени на их подбор.

Резюмируя результаты этого раздела можно сделать вывод, что женщины в большей степени склонны к использованию словарных паролей, таких как имена, даты и пр. Это стоит учитывать при составлении парольной политики в компании и при проведении программ повышения осведомленности сотрудников в вопросах обеспечения информационной безопасности на предприятии.

5. ВЫВОДЫ

На основании полученных данных можно сделать следующие выводы:

- В целом результаты аналогичных исследований, проводимых за рубежом, отличаются от полученных результатов проведенного исследования в отношении используемых паролей российскими пользователями;
- Наиболее распространенными паролями у российских пользователей являются пароли, состоящие только из цифр, на долю которых приходится приблизительно 53% от числа всех проанализированных паролей;
- 88% используемых паролей – это пароли, содержащие в себе либо цифры, либо символы английского алфавита в нижнем регистре, либо и то и другое;
- Используемые пароли российскими пользователями в большинстве случаев не превышают 8-ми символов и лишь единицы используют пароли длиннее 12-ти символов;
- Удаленная атака по словарям позволяет скомпрометировать 37% учетных записей;
- 74% используемых паролей пользователями в корпоративном секторе не соответствуют требованиям стандарта PCI DSS;
- Администраторами информационных систем зачастую используются незамысловатые пароли низкой стойкости, которые могут содержаться в публично распространяемых словарях (15%), полностью совпадать с логином (10%) или вовсе отсутствовать (2%);
- Используемые женщинами пароли, являются несколько более уязвимыми для атакующего, чем пароли, используемые мужчинами. Женщины в большей степени склонны к использованию словарных паролей, таких как имена, даты и пр. Благодаря более частому использованию словарных паролей удаленному злоумышленнику в среднем требуется меньше времени на их подбор.

6. ОБ АВТОРЕ

Дмитрий Евтеев, эксперт по информационной безопасности отдела консалтинга и аудита компании Positive Technologies. Специализируется в вопросах проведения тестирований на проникновение, аудита информационных систем и анализа защищенности Web-приложений. Имеет профессиональные звания и сертификаты (MCSE:Security, MCTS).

7. О КОМПАНИИ

«Позитив Текнолоджиз» (Positive Technologies) - лидирующая компания на рынке информационной безопасности.

Основные направления деятельности компании:

- разработка систем комплексного мониторинга информационной безопасности (XSpider, MaxPatrol);
- оказание консалтинговых услуг в области ИБ;
- предоставление сервисных услуг в области ИБ;
- развитие ведущего российского портала по ИБ Securitylab.ru.

Компания «Позитив Текнолоджиз» (Positive Technologies) – это команда квалифицированных разработчиков и консультантов. Эксперты компании имеют большой практический опыт, являются членами международных организаций, активно участвуют в развитии отрасли.

8. ССЫЛКИ

[1] Марк Бернетт (Mark Burnett), http://xato.com/, http://www.whatsmypass.com/?p=415

[2] HAK5 Rainbow Tables Project, http://wiki.hak5.org/wiki/Community_Rainbow_Tables

[3] Free Rainbow Tables Project, http://www.freerainbowtables.com/

[4] Словарь от InsidePro, http://www.insidepro.com/download/dictionary_insidepro_big.zip

[5] Словари от Underground InformatioN Center (UINC),
http://www.uinc.ru/forum/faqs/wordlist.shtml

Использовались следующие словари:
Список дат от 01/01/1950 до 31/12/1999
Список русских имен
Список наиболее употребляемых глаголов русского языка
Список наиболее употребляемых существительных русского языка
Список наиболее употребляемых наречий русского языка
Список наиболее употребляемых прилагательных русского языка
Список часто употребляемых слов в разговорном в "живом" русском языке
Список слов, характеризующих настроение и эмоции

[6] Microsoft TechNet, http://technet.microsoft.com/en-us/library/cc786468.aspx

[7] Дмитрий Евтеев, «Безопасность языком цифр #3»
http://devteev.blogspot.com/2009/05/3.html

[8] Payment Card Industry Data Security Standard, https://www.pcisecuritystandards.org/,
http://www.pcisecurity.ru/files/

9. ПРИЛОЖЕНИЕ 1: ИСПОЛЬЗУЕМЫЕ НАБОРЫ СИМВОЛОВ

numeric = [0-9]

alpha = [A-Z]

alpha-space = [A-Z]

alpha-numeric = [A-Z0-9]

alpha-numeric-space = [A-Z0-9]

alpha-numeric-symbol14 = [A-Z0-9!@#$%^&*()-_+=]

alpha-numeric-symbol14-space = [A-Z0-9!@#$%^&*()-_+=]

alpha-numeric-symbol32-space = [A-Z0-9!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

loweralpha = [a-z]

loweralpha-space = [a-z]

loweralpha-numeric = [a-z0-9]

loweralpha-numeric-space = [a-z0-9]

loweralpha-numeric-symbol14 = [a-z0-9!@#$%^&*()-_+="]

loweralpha-numeric-symbol14-space = [a-z0-9!@#$%^&*()-_+="]

loweralpha-numeric-symbol32-space = [a-z0-9!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

mixalpha = [a-zA-Z]

mixalpha-space = [a-zA-Z]

mixalpha-numeric = [a-zA-Z0-9]

mixalpha-numeric-space = [a-zA-Z0-9]

mixalpha-numeric-symbol14 = [a-zA-Z0-9!@#$%^&*()-_+=]

mixalpha-numeric-all-space = [a-zA-Z0-9!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

alpha-rus = [А-Я]

alpha-space-rus = [А-Я]

alpha-numeric-rus = [А-Я0-9]

alpha-numeric-space-rus = [А-Я0-9]

alpha-numeric-symbol14-rus = [А-Я0-9!@#$%^&*()-_+=]

alpha-numeric-symbol14-space-rus = [А-Я0-9!@#$%^&*()-_+=]

alpha-numeric-symbol32-space-rus = [А-Я0-9!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

loweralpha-rus = [а-я]

loweralpha-space-rus = [а-я]

loweralpha-numeric-rus = [а-я0-9]

loweralpha-numeric-space-rus = [а-я0-9]

loweralpha-numeric-symbol14-rus = [a-я0-9!@#$%^&*()-_+="]

loweralpha-numeric-symbol14-space-rus = [a-я0-9!@#$%^&*()-_+="]

loweralpha-numeric-symbol32-space-rus = [a-я0-9!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

mixalpha-rus = [a-яA-Я]

mixalpha-space-rus = [a-яA-Я]

mixalpha-numeric-rus = [a-яA-Я0-9]

mixalpha-numeric-space-rus = [a-яA-Я0-9]

mixalpha-numeric-symbol14-rus = [a-яA-Я0-9!@#$%^&*()-_+=]

mixalpha-numeric-all-space-rus = [a-яA-Я0-9!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

any-other-set = набор не удовлетворяющий требованиям всех перечисленных выше наборов символов

10. ПРИЛОЖЕНИЕ 2: СУММАРНАЯ СТАТИСТИКА ПО ИСПОЛЬЗУЕМЫМ НАБОРАМ СИМВОЛОВ В ПАРОЛЯХ

Набор символов	Доля, %
Только цифры (numeric)	52,73%
Символы английского алфавита в нижнем регистре (loweralpha)	17,96%
Символы английского алфавита в нижнем регистре и цифры (loweralpha-numeric)	17,51%
Символы английского алфавита в разных регистрах и цифры (mixalpha-numeric)	3,4%
Символы английского алфавита в разных регистрах (mixalpha)	1,63%
Символы английского алфавита в верхнем регистре и цифры (alpha-numeric)	1,35%
Символы русского алфавита в нижнем регистре (loweralpha-rus)	1,12%
Символы английского алфавита в нижнем регистре, цифры и спец. символы (loweralpha-numeric-symbol14)	0,8%
Пустая строка (NULL)	0,7%
Символы английского алфавита в верхнем регистре (alpha)	0,52%
Символы английского алфавита в нижнем регистре, цифры, спец. Символы и пробел (loweralpha-numeric-symbol32-space)	0,52%
Символы русского алфавита в нижнем регистре и цифры (loweralpha-numeric-rus)	0,47%
Символы английского алфавита в разных регистрах, цифры и спец. символы (mixalpha-numeric-symbol14)	0,35%
Символы английского алфавита в верхнем регистре, цифры и спец. символы (alpha-numeric-symbol14)	0,26%
Другие наборы символов (any-other-set)	0,15%
Символы русского алфавита в разных регистрах (mixalpha-rus)	0,14%
Символы английского алфавита в верхнем регистре, цифры, спец. символы и пробел (alpha-numeric-symbol32-space)	0,07%
Символы английского алфавита в разных регистрах, цифры, спец. символы и пробел (mixalpha-numeric-all-space)	0,06%
Символы русского алфавита в верхнем регистре (alpha-rus)	0,05%
Символы русского алфавита в разных регистрах и цифры (mixalpha-numeric-rus)	0,03%

Символы русского алфавита в верхнем регистре и цифры (alpha-numeric-rus)	0,03%
Символы русского алфавита в нижнем регистре, цифры, спец. символы и пробел (loweralpha-numeric-symbol32-space-rus)	0,02%
Символы русского алфавита в нижнем регистре, цифры и спец. символы (loweralpha-numeric-symbol14-rus)	0,01%
Символы русского алфавита в разных регистрах, цифры и спец. символы (mixalpha-numeric-symbol14-rus)	0,008%
Символы английского алфавита в нижнем регистре и пробел (loweralpha-space)	0,008%
Символы русского алфавита в нижнем регистре и пробел (loweralpha-space-rus)	0,007%
Символы английского алфавита в разных регистрах, цифры и пробел (mixalpha-numeric-space)	0,007%
Символы английского алфавита в разных регистрах, цифры, спец. символы и пробел (mixalpha-numeric-all-space-rus)	0,005%
Символы английского алфавита в нижнем регистре, цифры и пробел (loweralpha-numeric-space)	0,004%
Символы английского алфавита в верхнем регистре, цифры и пробел (alpha-numeric-space)	0,004%
Символы английского алфавита в верхнем регистре, цифры и спец. символы (alpha-numeric-symbol14-rus)	0,002%
Символы русского алфавита в верхнем регистре, цифры, спец. символы и пробел (alpha-numeric-symbol32-space-rus)	0,002%
Символы русского алфавита в нижнем регистре, цифры и пробел (loweralpha-numeric-space-rus)	0,002%
Символы английского алфавита в верхнем регистре и пробел (alpha-space)	0,002%
Символы английского алфавита в разных регистрах и пробел (mixalpha-space)	0,001%
Символы английского алфавита в нижнем регистре, цифры, спец. символы и пробел (loweralpha-numeric-symbol14-space)	0,001%
Символы английского алфавита в верхнем регистре, цифры, спец. символы и пробел (alpha-numeric-symbol14-space)	0,0005%
Символы русского алфавита в разных регистрах и пробел (mixalpha-space-rus)	0,0005%

11. ПРИЛОЖЕНИЕ 3: TOP 20 НАИБОЛЕЕ ЧАСТО ИСПОЛЬЗУЕМЫХ ПАРОЛЕЙ РОССИЙСКИМИ ПОЛЬЗОВАТЕЛЯМИ

Пароль	Позиция	Доля, %
1234567	1	3,36%
12345678	2	1,65%
123456	3	1,02%
Пустая строка	4	0,72%
12345	5	0,47%
7654321	6	0,31%
qweasd	7	0,27%
123	8	0,25%
qwerty	9	0,25%
123456789	10	0,23%
1234	11	0,22%
7777777	12	0,18%
111111	13	0,18%
87654321	14	0,15%
1111111	15	0,15%
1	16	0,13%
987654321	17	0,11%
11111111	18	0,1%
111	19	0,09%
88888888	20	0,08%