VARONIS

ОТЧЕТ О РИСКАХ ДАННЫХ, 2021 ГОД

ФИНАНСОВАЯ ОТРАСЛЬ

В среднем **каждый сотрудник** имеет доступ **почти к 11 миллионам файлов.**

СОДЕРЖАНИЕ

Об отчете 1

Основные выводы 2

Глобальные выводы 3

Будущее за автоматизацией 4

Путь к минимальным привилегиям 5

Слабая гигиена Active Directory 6

Состояние отрасли 7

Пример из практики: Prospect Capital 8

О компании Varonis 8

VARONIS

ОБ ОТЧЕТЕ

Это наш четвертый ежегодный 00000 0 000000, 000000000 0 0000000. В то время как прошлые отчеты содержали консолидированные выводы по более чем 30 отраслям, в этом году мы подготовили отдельные отчеты пот отраслям, наиболее подверженных риску, проанализировав отраслевые угрозы, тенденции и решения.

00000 *2021* 0. 0 000000 000000 0 00000 0000000000 00000 посвящен безопасности данных в финансовой отрасли: банках, страховании и инвестициях. Он был составлен на основе анализа 4 миллиардов файлов в 56 финансовых организациях по всему миру.

Многие выводы в отчете представлены по размеру бизнеса:

- **малый:** 0–500 сотрудников;
- **средний:** 501–1500 сотрудников;
- **крупный:** свыше 1500 сотрудников.

В дополнение к основным выводам прошлых отчетов, в этом отчете проводится существенная корреляция между текущим состоянием отрасли и растущими угрозами, с которыми сталкиваются финансовые компании. Эти выводы сделаны с использованием решений Varonis, которые анализируют хранилища данных, в сочетании с отраслевыми отчетами.

В основе отчета — анализ
4 миллиардов файлов
в **56 финансовых организациях**
по всему миру

Банки

Страхование

Инвестиции

ОСНОВНЫЕ ВЫВОДЫ

2020 год был беспрецедентным для ИТ и информационной безопасности. Организации по всему миру отреагировали на угрозу пандемии коронавируса, перейдя на дистанционную работу. Это привело к резкому увеличению числа сотрудников, которые работают удаленно, используя Microsoft Office 365 и другие облачные сервисы и приложения, а также получают доступ к корпоративным ресурсам через VPN.

Внезапный характер всего происходящего вынудил многие компании перейти в облако без должной подготовки с точки зрения кибербезопасности. Сотрудники входят в корпоративные системы через незащищенные сети и домашние компьютеры, тем самым непреднамеренно увеличивая риски реализации потенциальных атак. Когда у компаний есть очевидные пробелы в безопасности, такие как бессрочные пароли и открытые для всех папки с конфиденциальными данными, риск возрастает экспоненциально.

В среднем у сотрудника финансовой компании появляется доступ почти к **11 миллионам файлов в первый же день работы.** Для крупных организаций это число удваивается: **20 миллионов файлов открыты для всех сотрудников.** Эти проблемы остаются основными в отрасли.

Влияние на отрасль

Двумя задачами безопасности с наивысшим приоритетом для ИТ-отделов финансовых компаний стали безопасный переход на удаленную работу и блокировка открытых данных для снижения рисков, связанных с удаленным входом в систему. Переход на удаленную работу без надлежащих мер безопасности экспоненциально увеличивает риск, связанный с внутренними атаками, вредоносными программами и программами-вымогателями.

Основные выводы
о финансовой отрасли

Каждый сотрудник имеет доступ почти к **11 миллионам файлов**

Почти **две трети** компаний имеют **более 1000 конфиденциальных файлов,** открытых для **всех сотрудников.**

Около **60% компаний** имеют **более 500 паролей без срока истечения**

ГЛОБАЛЬНЫЕ ВЫВОДЫ

Будущее за автоматизацией

Данные представлены в зависимости от размера компании

Размер бизнеса	Средн. кол-во файлов	Средн. кол-во файлов, открытых всем	Средн. % файлов, открытых всем
Крупный	134 368 022	20 427 920	15%
Средний	75 085 577	10 254 062	13%
Малый	6 800 969	570 284	11%
В среднем по отрасли	**74 309 255**	**10 774 940**	**13%**

Размер бизнеса	Средн. кол-во папок	Средн. кол-во папок, открытых всем	Средн. % папок, открытых всем
Крупный	9 000 369	1 383 656	15%
Средний	5 209 135	778 045	13%
Малый	981 746	101 717	11%
В среднем по отрасли	**5 204 344**	**776 943**	**13%**

Размер бизнеса	Средн. кол-во конфиденц. файлов	Средн. кол-во конфиденц. файлов, открытых всем	Средн. % конфиденц. файлов, открытых всем
Крупный	802 315	55 396	8%
Средний	344 653	37 911	18%
Малый	163 435	12 550	19%
В среднем по отрасли	**449 855**	**36 004**	**15%**

В среднем сотрудник компании в сфере финансов имеет доступ к 13% всех файлов компании. В более широком контексте это означает, что даже сотрудники самых маленьких фирм имеют неограниченную свободу просматривать, копировать, перемещать, изменять и удалять данные, **среди которых 20% файлов содержат конфиденциальные данные сотрудников и клиентов.** Количество доступных всем файлов удваивается по мере увеличения размера компании, и у крупнейших финансовых организаций каждому сотруднику открыто в среднем более 20 миллионов файлов.

ГЛОБАЛЬНЫЕ ВЫВОДЫ

Среднее состояние данных на терабайт

Размер компании	Файлы	Папки	Открытые папки	Конфиденциальные файлы	Папки с уникальными правами	Открытые конфиденциальные файлы	Устаревшие конфиденциальные файлы	Несоответствующие сиды (SID)	Папки с несогласованными разрешениями	Кол-во отчетов	Терабайт проанализировано на компанию
Крупный	1 280 436	108 004	19 080	19 582	12 812	1779	10 165	1227	818	20	126
Средний	1 425 052	135 883	18 175	12 134	9474	1168	9540	1590	505	18	65
Малый	1 090 355	131 775	20 516	35 506	12 484	2571	20 586	1576	1948	18	12
Средний	**1 265 822**	**124 606**	**19 251**	**22 306**	**11 634**	**1837**	**13 314**	**1456**	**1081**	**56**	**70**

Чтобы сравнение компаний разного размера было объективным, необходимо проанализировать риски на терабайт данных. В среднем терабайт содержит 1,3 миллиона файлов, и примерно 2% (20 000 из этих файлов) содержат конфиденциальную информацию, включая финансовые и персональные данные. Оценка риска на терабайт данных дает более четкое представление о типичной поверхности атаки в зависимости от размера компании и показывает, какие организации наиболее уязвимы.

Мы обнаружили, что финансовые организации в среднем имеют около 20 000 папок (доступ к которым открыт для всех[1])на терабайт, и эта цифра неизменна для компаний любого размера. Чтобы найти и вручную удалить глобальный доступ, ИТ-специалистам требуется примерно 6–8 часов для каждой папки, то есть **на исправление этих папок вручную уйдет более 15 лет** (при условии, что не добавляются новые папки, а ИТ-отдел работает круглосуточно).

Это чрезвычайно важная задача, **особенно для небольших компаний (меньше 500 сотрудников), которые считают, что они слишком малы, чтобы их заметили злоумышленники.** Но также это невероятно утомительно, и без автоматизации отнимает уйму времени.

[1]В этом отчете «для всех» означает каждого сотрудника в организации.

ГЛОБАЛЬНЫЕ ВЫВОДЫ

Путь к минимальным привилегиям

Данные по компаниям, в которых конфиденциальные файлы открыты для всех сотрудников через глобальный доступ

Конфиденциальные файлы, открытые всем	% компаний
< 1000	35,71%
1000 – 10 000	25%
> 10 000	39,29%

Устаревшие конфиденциальные данные в зависимости от размера компании

Размер бизнеса	Средн. кол-во устаревших конфиденц. файлов	Средн. % устаревших конфиденц. файлов
Крупный	526 606	63%
Средний	208 490	74%
Малый	109 152	74%
В среднем по отрасли	**290 173**	**70%**

Группы глобального доступа (например, «Все», «Пользователи домена», «Пользователи, прошедшие проверку») подвергают финансовые компании неоправданному риску. Представьте, что один пользователь нажимает на ссылку в фишинговом письме и запускает цепную реакцию. У компании, работающей в сфере финансов, уходит в среднем **233 дня на обнаружение и предотвращение утечки данных**[2]. Иными словами, среднестатистическая финансовая компания устранит взлом, приводящий к утечке данных, **через восемь месяцев** после его осуществления — достаточно времени, чтобы нанести ощутимый ущерб репутации, подорвать доверие клиентов и понести серьезные убытки.

Более 64% компаний, оказывающих финансовые услуги, имеют свыше 1000 конфиденциальных файлов, открытых каждому сотруднику. Это подвергает компании риску несоблюдения правил, требующих строгого контроля над конфиденциальной информацией, например Общий регламент ЕС по защите данных (GDPR), стандарт безопасности данных индустрии платежных карт (PCI DSS). Нарушителям грозит штраф до 20 миллионов евро или 4% от глобальных доходов компании (в случае GDPR).

Устаревшие конфиденциальные данные — критически важные данные о сотрудниках, клиентах, проектах, заказчиках и другие закрытые данные, которые не были востребованы более 90 дней, — подлежат регулированию аналогичным образом. В среднем **70% всех конфиденциальных данных считаются устаревшими.** Если эти данные хранятся сверх установленного срока, то организация подвергает себя повышенному риску.

[2] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

ГЛОБАЛЬНЫЕ ВЫВОДЫ

Слабая гигиена Active Directory

Компании с бессрочными паролями

Бессрочные пароли	% компаний
< 500	41,07%
500 – 1500	37,50%
> 1500	21,43%

Компании с фантомными пользователями

Размер групп пользователей с устаревшими данными	% компаний
< 1000	35,71%
1000 – 10 000	25,00%
> 10 000	39,29%

Зачастую самый простой и быстрый способ попасть на сервер и незаметно перемещаться по устройствам — это получить доступ к учетным записям пользователей и служб, которые неактивны, но включены («фантомные пользователи»). Наличие фантомных учетных записей наряду с устаревшими группами пользователей и привилегированными пользователями с бессрочными паролями дает хакерам лазейку для незаметной кражи данных или нарушения работы компании.

Для ручного поиска этих уязвимостей требуется время и организованное сотрудничество между отделами и группами. К сожалению, этому редко отдается приоритет. В результате **59% компаний, предоставляющих финансовые услуги, имеют более 500 бессрочных паролей,** а **почти 40% имеют свыше 10 000 фантомных учетных записей**.

СОСТОЯНИЕ ОТРАСЛИ

Финансовые компании оказались в странной ситуации: будучи лидерами с точки зрения зрелости безопасности, они всё еще подвергаются сравнительно высокому риску. Финансовая отрасль остается наиболее подверженной хакерским атакам, во многом из-за конфиденциальных данных, которые собирают компании о своих клиентах[3]. Средняя стоимость утечки данных[4] является одной из самых высоких среди отраслей и составляет 5,85 млн долларов США.

В 2020 году финансовые организации могут похвастаться самой быстрой реакцией на инцидент — среднее время выявления и устранение утечки данных короче, чем в других вертикалях. Однако удаленная работа может значительно увеличить время реакции. Чем позже следует реакция на инцидент, тем выше цена утечки данных. Невозможно переоценить важность обеспечения прозрачности и наглядности сетевых сред и автоматизации безопасности.

По мере того как финансовые организации переходят к удаленной работе через Office 365, всё большее значение приобретает наличие инструментов, обеспечивающих контроль и управление рисками. В такой ситуации обеспечение соответствия нормативным требованиям может быть непростой задачей, поэтому наличие четких журналов регистрации событий и механизмов отчетности жизненно необходимо.

3 https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/financial-services-data-breaches/

4 https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Средняя стоимость утечки данных в финансовых компаниях является одной из самых высоких среди других отраслей **и составляет 5,85 миллиона долларов США.**

ПРИМЕР ИЗ ПРАКТИКИ

PROSPECT CAPITAL

Как Varonis помогает компании Prospect Capital создавать отчеты о соответствии за минуты, а не часы

Prospect Capital переносит свои данные в облако Microsoft. Чтобы сделать этот шаг и упростить соблюдение требований регуляторов, компании требовались инструменты обеспечения наглядности инфраструктуры данных и механизмов отчетности.

Узнайте, как Varonis помог в этой ситуации.

СКАЧАТЬ ИСТОРИЮ УСПЕХА PROSPECT CAPITAL

О КОМПАНИИ VARONIS

Varonis — передовая компания в области кибербезопасности и аналитики данных, специализирующаяся на программном обеспечении для защиты данных, обнаружения угроз и реагирования на них, а также соблюдения нормативных требований. Varonis защищает данные компаний, анализируя информацию о телеметрии периметра сети, а также поведение пользователей и действия с данными. Решения компании предотвращают потери, блокируя доступ к конфиденциальной информации, и эффективно поддерживают защищенное состояние с помощью автоматизации.

Varonis — 000 000000 00, 000 000000000 000 0000000 000000000 00000000000 00000000 0 0000 00000 000000000000000 0 000000000000 0 0000000000 0000000000 00000000000. 000000, 00 00000000000 0000000 000000 0000000 000, 000000000 *Varonis* 00000000000 0000000000000 00000 000 00 *10* 00000.

АЛ ФАЭЛЬЯ
Технический директор Prospect Capital

Хотите проверить, как обстоят дела в **вашей организации**?

Мы проведем бесплатную оценку рисков кибербезопасности и подготовим подробный отчет об уровне защищенности и скрытых рисках, которым подвергаются конфиденциальные данные вашей компании.

СВЯЗАТЬСЯ С НАМИ

Нам доверяют

ING Nasdaq John Hancock UnionBank AXA Amundi ASSET MANAGEMENT BAILLIE GIFFORD BDO

VARONIS

www.varonis.com/ru