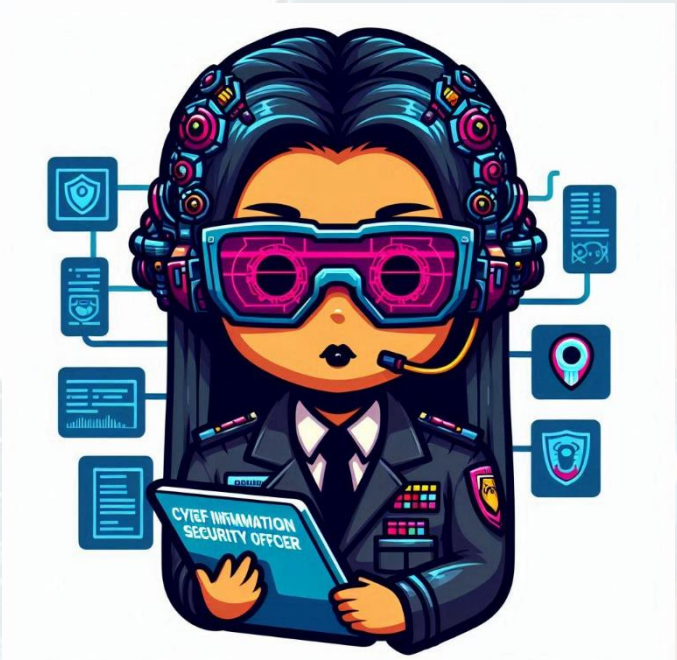

Аннотация – В документе представлен анализ отчёта Proofpoint "2024 Voice of the CISO". Анализ посвящён различным важным аспектам отчёта, в котором подробно рассматриваются проблемы и тенденции, с которыми сталкиваются руководители служб информационной безопасности (CISO) во всем мире.

Анализ представляет собой высококачественное обобщение отчёта, содержащее ценную информацию для специалистов по безопасности и других специалистов из различных отраслей. Понимая проблемы и стратегии, изложенные в отчёте, специалисты могут лучше подготовиться к меняющимся условиям кибербезопасности и повысить уровень безопасности своей организации. Этот анализ особенно полезен для тех, кто стремится привести свои усилия в области кибербезопасности в соответствие с лучшими отраслевыми практиками и новыми тенденциями.

I. Введение

Отчёт Proofpoint «2024 Voice of the CISO» рисует яркую картину неустойчивого ландшафта, в котором недавно оказались CISO. В конце концов, борьба с глобальной пандемией, хаосом удалённой работы и рекордной текучкой кадров была просто лёгкой прогулкой в парке. Теперь, когда гибридная работа становится нормой, а облачные технологии расширяют поверхность атаки до беспрецедентных уровней, CISO наконец-то могут расслабиться и начать работать, верно?

Кибер-угрозы стали более целенаправленными, сложными и частыми, чем когда-либо. Сотрудники стали более мобильными, часто заимствуя конфиденциальные данные при переходе с одной работы на другую. А ещё генеративный ИИ упростили киберпреступникам запуск разрушительных атак всего за несколько долларов.

Конечно, CISO наслаждаются более тесными связями с ключевыми заинтересованными сторонами, членами совета директоров и регулирующими органами. Но эта новообретённая близость только повышает ставки, увеличивает давление и повышает ожидания. А при фиксированных или сокращённых бюджетах от CISO ожидают гораздо большего с гораздо меньшими затратами. *Ирония, ведь обычно CISO от нижестоящих всегда ждут именно этого под соусом лояльности.*

Чтобы лучше понять, как руководители служб информационной безопасности справляются с очередным напряженным годом, Proofpoint опросил 1600 руководителей по всему миру. Они спросили их об их ролях, перспективах на следующие два года и о том, как они видят развитие своих обязанностей. В отчёте исследуется тонкий баланс между тревожностью и самоуверенностью, поскольку различные факторы коварно объединяются, чтобы усилить давление на бедных руководителей служб информационной безопасности. Рассматриваются постоянные риски, связанные с человеческой ошибкой, проблемы выгорания и личной ответственности, а также отношения между руководителями служб информационной безопасности и советом директоров.

A. *Достоинства*

- **Комплексные данные:** в отчёте опрашиваются 1600 руководителей служб информационной безопасности из организаций с 1000 и более сотрудников в 16 странах, что обеспечивает в целом широкий и разнообразный набор данных.
- **Текущие тенденции и проблемы:** в нем освещаются ключевые проблемы, такие как постоянная уязвимость ввиду человеческих ошибок, влияние генеративного ИИ и экономическое давление на бюджеты кибербезопасности.
- **Стратегические идеи:** в отчёте предлагаются «практические» идеи и рекомендации, такие как напоминание о важности технологий на основе ИИ, повышение осведомлённости сотрудников о кибербезопасности и необходимость надёжных планов реагирования на инциденты.
- **Отношения между советом директоров и директорами по информационной безопасности:** улучшение отношений между директорами по информационной безопасности и членами совета директоров, что имеет решающее значение для согласования стратегий кибербезопасности с бизнес-целями.

B. *Недостатки*

- **Излишний акцент на ИИ:** в отчёте уделяется большое внимание ИИ как угрозе и решению. Хотя роль ИИ в кибербезопасности неоспорима, акцент смещается с других важных областей.
- **Потенциальная предвзятость в предоставленных данных:** CISO, как правило, склонны преувеличивать свою готовность или эффективность своих стратегий, чтобы представить более благоприятный взгляд на собственную производительность.

- **Ориентация на крупные организации:** опрос ориентирован на организации с численностью сотрудников 1000 и более человек, что неточно отражает проблемы и реалии, с которыми сталкиваются небольшие организации, и ограничивает применимость результатов к более широкому кругу предприятий.
- **Экономические и региональные различия:** хотя отчёт охватывает несколько стран, экономическая и нормативная среда значительно различается в разных регионах. Результаты могут быть не универсальными, а региональные нюансы недостаточно представлены.
- **Человеко-центричная безопасность:** подход не в полной мере охватывает сложности эффективной реализации таких стратегий. Опора на обучение и осведомлённость пользователей может рассматриваться как возложение слишком большой ответственности на сотрудников, а не как улучшение системной защиты

C. Методология

1) Область исследования

- Опрос проводился исследовательской фирмой Censuswide в период с 20 января по 2 февраля 2024
- Опрос был проведён среди 1600 руководителей служб информационной безопасности (CISO) из организаций с численностью сотрудников 1000 и более человек в различных отраслях в 16 странах.
- Было опрошено 100 руководителей служб информационной безопасности на каждом из следующих рынков: США, Канада, Великобритания, Франция, Германия, Италия, Испания, Швеция, Нидерланды, ОАЭ, Саудовская Аравия, Австралия, Япония, Сингапур, Южная Корея и Бразилия.

2) Представление отрасли:

- ИТ, технологии и телекоммуникации (42%)
- Производство и производство (14%)
- Финансовые услуги (12%)
- Розничная торговля (8%)
- Бизнес и профессиональные услуги (6%)
- Государственный сектор (5%)
- Здравоохранение (3%)
- Образование (3%)
- СМИ, досуг и развлечения (3%)
- Транспорт (2%)
- Энергетика, нефть/газ и коммунальные услуги (2%)

3) Размер компаний:

- 1000–2500 сотрудников (48%)
- 2501–5000 сотрудников (33%)
- 5001 или более сотрудников (19%)

4) Исследования Стандарты:

Censuswide, исследовательская фирма, проводящая опрос, соблюдает Кодекс поведения MRS и принципы ESOMAR, обеспечивая соблюдение отраслевых стандартов и этических норм.

II. Повышенная обеспокоенность, но растущая уверенность

A. Повышенное восприятие риска:

- **Риск существенной кибератаки:** более двух третей (70%) руководителей служб информационной безопасности предчувствуют риск существенной кибератаки в течение следующих 12 месяцев, что немного больше, чем 68% в прошлом году, и значительно выше, чем 48% в 2022 году.
- **Высокая вероятность:** 31% руководителей служб информационной безопасности оценивают риск существенной атаки как «весьма вероятный» по сравнению с 25% в 2023 году.

B. Географические опасения:

- **Наиболее беспокоящие регионы:** руководители служб информационной безопасности в Южной Корее (91%), Канаде (90%) и США (87%) больше всего обеспокоены возможностью подвергнуться существенной кибератаке.
- **Оптимистичные регионы:** руководители служб информационной безопасности Бразилии настроены наиболее оптимистично, только 45% опасаются атаки.

C. Особые опасения по отраслям:

- **Отрасли с высоким уровнем риска**: образование (86%), транспорт (77%), розничная торговля, здравоохранение и государственный сектор (все 74%) лидируют по уровню опасений по поводу кибератак.

D. Осведомлённость против готовности:

- **Осведомлённость:** хотя 70% руководителей служб информационной безопасности чувствуют себя в опасности, только 43% считают, что их организация не готова справиться с целенаправленной кибератакой в 2024 году, что лучше, чем 61% в 2023 году и 50% в 2022 году.
- **Разрыв в готовности:** Разрыв между осведомлённостью и готовностью остаётся проблемой, подчёркивая разрыв между распознаванием рисков и готовностью к их устранению.

E. Основные угрозы:

- **Программы-вымогатели:** 41% руководителей служб информационной безопасности считают

программы-вымогатели главной угрозой в ближайшие 12 месяцев.

- **Другие угрозы:** вредоносное ПО (38%), мошенничество с электронной почтой (36%), взлом облачных учётных записей (34%), внутренние угрозы (30%) и DDoS-атаки (30%) также являются значительными проблемами.

F. Региональные угрозы:

- **Программы-вымогатели:** главная проблема в Японии (64%), Великобритании (51%), Швеции (49%) и Нидерландах (49%).
- **Мошенничество с электронной почтой:** главная проблема в Саудовской Аравии (50%), Австралии (46%), Германии (46%), Канаде (42%), Нидерландах (42%) и Японии (42%).

III. Человеческая ошибка: постоянная уязвимость

A. Человеческая ошибка как самая большая уязвимость:

- 74% руководителей служб информационной безопасности считают человеческую ошибку самой большой кибер-уязвимостью своей организации, по сравнению с 60% в 2023 году и 56% в 2022 году.
- Однако только 63% членов совета директоров согласны с тем, что человеческая ошибка является самой большой уязвимостью, что говорит о том, что руководителям служб информационной безопасности необходимо лучше информировать совет директоров об этом риске.

B. Халатность сотрудников как ключевая проблема:

- 80% руководителей служб информационной безопасности считают человеческий риск, включая халатность сотрудников, ключевой проблемой кибербезопасности в течение следующих двух лет, по сравнению с 63% в 2023 году.
- Это мнение сильнее всего ощущалось во Франции (91%), Канаде (90%), Испании (86%), Южной Корее (85%) и Сингапуре (84%).

C. Осведомлённость сотрудников против возможностей:

- 86% руководителей служб информационной безопасности считают, что их сотрудники понимают свою роль в защите организации, а 45% полностью согласны с этим.
- Однако руководители служб информационной безопасности по-прежнему считают, что сотрудники представляют огромный риск, подразумевая, что, хотя сотрудники понимают свои обязанности, у них нет необходимых навыков, знаний и инструментов для эффективной защиты от угроз.

D. Внедрение возможностей на основе ИИ:

- 87% руководителей служб информационной безопасности стремятся внедрить возможности на основе ИИ для защиты от человеческих ошибок и блокировки сложных кибер-угроз, ориентированных на человека.
- Отрасли, лидирующие по внедрению, включают розничную торговлю (81%), ИТ, технологии и телекоммуникации (89%), а также образование (88%).

E. Региональные и отраслевые различия:

- Руководители служб информационной безопасности в Саудовской Аравии (84%), Канаде (83%) и Франции (82%) больше всего обеспокоены тем, что человеческие ошибки являются самой большой кибер-уязвимостью их организаций.
- Отрасли, в которых больше всего опасений по поводу человеческих ошибок, включают образование (89%), средства массовой информации, досуг и развлечения (85%), а также государственный сектор (78%).

IV. Защита данных и внутренние угрозы

A. Сокращение потерь данных:

- Менее половины (46%) руководителей служб информационной безопасности по всему миру сообщили о существенной потере конфиденциальной информации за последние 12 месяцев, что ниже показателя в 63% в прошлом году.

B. Географические различия:

- Южная Корея (77%), Канада (61%), Франция (58%) и Германия (57%) сообщили о более высоких показателях потери конфиденциальных данных по сравнению со средним мировым показателем.

C. Отраслевые потери данных:

- Секторы образования (68%), финансовых услуг (54%), а также СМИ, досуга и развлечений (54%) больше всего пострадали от потери конфиденциальных данных.

D. Причины потери данных:

- В 42% случаев потери данных виноваты нерадивые сотрудники или небрежные сотрудники.
- Другие существенные причины включают внешние атаки (40%) и злонамеренных или преступных сотрудников (36%).
- Дополнительные факторы включали неправильную настройку системы (27%) и утерянные или украденные устройства (28%).

E. Текучка кадров и потеря данных:

- 73% руководителей служб информационной безопасности заявили, что уход сотрудников

из их организаций сыграл свою роль в событиях потери данных.

- Хотя обеспокоенность по поводу потери данных из-за смены работы снизилась с 82% в прошлом году, она остаётся значительной проблемой.

F. Влияние потери данных:

- Последствия потери данных включали финансовые потери (43%), расходы на восстановление после атаки (41%) и потерю критически важных данных (40%).

G. Стратегии смягчения (последствий):

- Для борьбы с потерей данных руководители служб информационной безопасности фокусируются на обучении сотрудников передовым методам обеспечения безопасности (53%) и использовании облачных решений безопасности (52%).

- Другие меры включают развёртывание технологии предотвращения потери данных (DLP) (51%), безопасности конечных точек (49%), безопасности электронной почты (48%) и технологии изоляции (42%).

H. Будущие приоритеты:

- 87% руководителей служб информационной безопасности согласны с тем, что защита информации и управление данными являются главными приоритетами, что значительно больше, чем в предыдущие годы.

- Внедрение технологии DLP резко возросло: её теперь используют 51% руководителей служб информационной безопасности, по сравнению с 35% в прошлом году.

- 81% руководителей служб информационной безопасности считают, что их данные надёжно защищены, по сравнению с 60% в 2023 году.

V. Киберреалии для руководителей служб информационной безопасности в 2024 году

A. Генеративный ИИ:

- **Риски безопасности:** 54% руководителей служб информационной безопасности считают, что генеративный ИИ представляет угрозу безопасности для их организации.

- **Двойное применение:** хотя ИИ может помочь киберпреступникам, упрощая масштабирование и выполнение атак, он также предоставляет защитникам информацию об угрозах в режиме реального времени, с которой традиционные методы не могут сравниться.

- **Основные опасения:** ChatGPT и другие генеративные модели ИИ рассматриваются как существенные риски, за ними следуют инструменты совместной работы, такие как Slack и Teams (39%) и Microsoft 365 (38%).

B. Экономическое влияние:

- **Экономические условия:** 59% руководителей служб информационной безопасности согласны с тем, что текущие экономические условия негативно повлияли на способность их организаций выделять бюджеты на кибербезопасность.

- **Региональное влияние:** руководители служб информационной безопасности в Южной Корее (79%), Канаде (72%), Франции (68%) и Германии (68%) ощущают экономические последствия наиболее остро.

- **Бюджетные ограничения:** почти половине (48%) руководителей служб информационной безопасности было предложено сократить штат, отложить заполнение или сократить расходы.

C. Приоритеты и стратегии:

- **Основные приоритеты:** улучшение защиты информации и поддержка бизнес-инноваций остаются главными приоритетами для 58% руководителей служб информационной безопасности.

- **Осведомлённость сотрудников о кибербезопасности:** повышение осведомлённости сотрудников о кибербезопасности стало вторым по значимости приоритетом, что свидетельствует о переходе к стратегиям безопасности, ориентированным на человека.

D. Отношения с советом директоров:

- **Согласованность с советом директоров:** 84% директоров по информационной безопасности теперь сходятся во взглядах с членами совета директоров по вопросам кибербезопасности, что выше, чем 62% в 2023 году.

- **Экспертиза на уровне совета директоров:** 84% директоров по информационной безопасности считают, что экспертиза в области кибербезопасности должна быть обязательной на уровне совета директоров, что отражает значительный рост по сравнению с предыдущими годами.

E. Проблемы и давление:

- **Нереалистичные ожидания:** 66% директоров по информационной безопасности считают, что к их роли предъявляются чрезмерные требования, что продолжает расти по сравнению с предыдущими годами.

- **Выгорание**: более половины (53%) директоров по информационной безопасности испытали или стали свидетелями выгорания за последние 12 месяцев, хотя наблюдается небольшое улучшение: 31% сообщили об отсутствии выгорания, что выше, чем 15% в прошлом году.

- **Личная ответственность:** 66% руководителей служб информационной безопасности обеспокоены личной, финансовой и юридической ответственностью, а 72% не желают присоединяться к организации без страхования директоров и должностных лиц или аналогичного страхования.

VI. Укрепление отношений между советом директоров и директором по информационной безопасности

A. Улучшение согласованности:

- **Более высокий уровень согласия:** 84% директоров по информационной безопасности теперь сообщают о том, что они сходятся во взглядах с членами совета директоров по вопросам кибербезопасности, что значительно больше, чем 62% в 2023 году и 51% в 2022 году.
- **Отраслевые различия:** самые высокие уровни согласия наблюдаются в здравоохранении (91%), транспорте (88%), а также в энергетике, нефтегазовой отрасли и коммунальных услугах (81%).

B. Экспертиза на уровне совета директоров:

- **Экспертиза в области кибербезопасности:** 84% директоров по информационной безопасности считают, что экспертиза в области кибербезопасности должна быть обязательной на уровне совета директоров, по сравнению с 62% в 2023 году.
- **Региональные различия:** директора по информационной безопасности в Саудовской Аравии (95%), Бразилии (92%), Германии (90%) и ОАЭ (90%) сообщают о самых высоких уровнях согласия со своими советами директоров.

C. Проблемы совета директоров:

- **Основные проблемы:** директора по информационной безопасности считают, что их советы директоров больше всего обеспокоены нарушением работы (44%), потерей дохода (44%) и ущербом репутации (43%) в случае существенной кибератаки.
- **Проблемы, связанные с конкретной страной**: проблемы различаются в зависимости от страны, некоторые регионы отдают приоритет различным аспектам воздействия кибератак.

D. Факторы, лежащие в основе улучшения отношений:

- **Влияние после пандемии**: многие директора по информационной безопасности сохранили своё место за столом после пандемии, влияя на более широкую бизнес-стратегию.
- **Коммуникация:** директора по информационной безопасности предприняли шаги, чтобы говорить на языке совета директоров, переводя проблемы безопасности в потенциальные бизнес-влияния.

E. Устойчивая интеграция:

- Долгосрочные изменения: Интеграция директоров по информационной безопасности в совет директоров рассматривается как устойчивое улучшение бизнес-стратегии, необходимое для успеха в современную цифровую эпоху.

VII. История продолжается… Непрекращающееся давление на руководителей служб информационной безопасности

A. Повышенные ожидания:

- **Нереалистичные требования:** 66% руководителей служб информационной безопасности считают, что к их роли предъявляются чрезмерные требования, что является постоянным ростом с 61% в 2023 году и 49% в 2022 году.
- **Глобальные различия:** самые высокие уровни воспринимаемых чрезмерных ожиданий наблюдаются в Саудовской Аравии (88%), ОАЭ (87%) и Южной Корее (75%).

B. Выгорание:

- **Высокая заболеваемость**: более половины (53%) руководителей служб информационной безопасности испытали или стали свидетелями выгорания за последние 12 месяцев.
- **Улучшение:** наблюдается определённый прогресс: 31% руководителей служб информационной безопасности сообщили об отсутствии выгорания, что выше, чем 15% в прошлом году.
- **Региональные различия:** CISO в Южной Корее (72%), Швеции (63%) и Австралии (62%) чаще всего испытывают или становятся свидетелями выгорания.

C. Опасения по поводу личной ответственности:

- **Юридические и финансовые риски:** 66% CISO обеспокоены личной, финансовой и юридической ответственностью, по сравнению с 62% в 2023 году.
- **Страховое покрытие:** 72% CISO не присоединились бы к организации без страхования директоров и должностных лиц (D& O) или аналогичного покрытия финансовой ответственности в случае успешной кибератаки.
- **Опасения по поводу отрасли:** CISO в сфере производства и производства (75%), финансовых услуг (74%) и розничной торговли (68%) больше всего уверены в необходимости такого страхования.

D. Влияние громких дел:

- **Влияние судебных дел:** громкие судебные дела, такие как обвинения SEC против директора по информационной безопасности SolarWinds,

усилили обеспокоенность по поводу личной ответственности.

E. Текущие проблемы:

- **Ограничения ресурсов:** директора по информационной безопасности продолжают сталкиваться с проблемами из-за фиксированных или сокращённых бюджетов, что затрудняет удовлетворение растущих требований и ожиданий, возлагаемых на них.

VIII. Выводы

A. Возросшая обеспокоенность, но улучшенная готовность:

- Все больше руководителей информационной безопасности обеспокоены возможностью существенной кибератаки в ближайшем будущем.
- Меньше руководителей информационной безопасности чувствуют себя неподготовленными, что свидетельствует о большей уверенности в своих мерах защиты.

B. Более тесные отношения с заинтересованными сторонами:

- Директора информационной безопасности сообщают о более тесных отношениях с ключевыми заинтересованными сторонами и советом директоров.
- Это изменение подчёркивает растущее признание роли директора по информационной безопасности на самых высоких уровнях организации и важность кибербезопасности.

C. Текущие проблемы:

- **Текучка кадров:** продолжает оставаться серьёзной проблемой, поскольку увольняющиеся сотрудники представляют собой постоянный риск потери данных во всех секторах.
- **Внедрение технологии DLP:** многие директора по информационной безопасности внедрили технологию предотвращения потери данных (DLP) и инвестировали в обучение сотрудников, чтобы снизить этот риск.

D. Изменяющийся ландшафт угроз:

- **Знакомые угрозы:** атаки с использованием программ-вымогателей и компрометации деловой электронной почты (BEC) остаются серьёзными проблемами.
- **Новые технологии:** ИИ создаёт новые проблемы, но также предлагает потенциальные решения.

E. Безопасность, ориентированная на человека:

- Люди и их поведение продолжают представлять наибольший постоянный риск для организаций.
- Многие директора по информационной безопасности больше инвестируют в подходы к безопасности, ориентированные на человека, используя ИИ для снижения человеческих ошибок.

F. Проблемы роли CISO:

- **Личная ответственность:** Растущая обеспокоенность по поводу личной ответственности.
- **Чрезмерные ожидания:** Все большее число CISO сообщают о чрезмерных ожиданиях, выгорании и сложных бюджетах.
- Решение этих проблем имеет решающее значение для того, чтобы CISO были готовы к своим ролям сейчас и в будущем.