Кибербезопасность в когнитивную эпоху

Построение цифровой иммунной системы

IBM Institute for Business Value

Преимущества решений IBM

Киберпреступность — это скрытая угроза, принимающая поистине катастрофический масштаб. Совокупный экономический ущерб от киберпреступлений, причиненный мировой экономике, с трудом поддается оценке. По мнению некоторых экспертов, он варьируется от 375 до 575 миллиардов долларов США ежегодно. Целью злоумышленников может стать любое предприятие в любой точке мира, принадлежащее любой отрасли. IBM предлагает обширный портфель тесно интегрированных средств, включающих в себя ПО системы безопасности и услуги, которые решают задачи борьбы с киберпреступлениями: предупреждение, выявление, реагирование и устранение последствий. Эти решения помогают организациям предвидеть риски, связанные с кибербезопасностью, и заранее принимать необходимые меры. С помощью IBM Security заказчики могут создать иммунную систему безопасности, основу которой составляет аналитика, защита в реальном времени и проверенный временем опыт экспертов. Чтобы узнать подробнее о сотрудничестве IBM с различными организациями при решении задач защиты цифровой инфраструктуры, посетите сайт **ibm.com**/security/ru/ru/index.html.

Новые возможности для непростой эпохи

Ведущие организации в отрасли безопасности напряженно работают над тем, чтобы устранить три недостатка технических и организационных аспектов своих систем безопасности, связанных с анализом данных, оперативностью работы и точностью реагирования. Чтобы устранить имеющиеся недостатки и наладить упреждающий анализ рисков и угроз, некоторые организации обращаются к возможностям когнитивных решений безопасности. С этой технологией связаны невероятно высокие ожидания. 57% опрошенных нами представителей ведущих организаций в отрасли безопасности сообщили, что данная технология эффективно связывает руки киберпреступникам. 22% респондентов, которых мы выделили в категорию «Активные», уже вступили в когнитивную эпоху кибербезопасности. Они убеждены, что хорошо знают эту предметную область, готовы создавать соответствующие решения и располагают всеми необходимыми ресурсами. Прежде чем приступать к внедрению подобного решения, необходимо изучить слабые стороны вашей системы безопасности, определить роль и место когнитивных решений среди ваших решений безопасности, а также продумать образовательную программу и инвестиционный план для всех участвующих лиц.

Резюме для руководителей

В отрасли кибербезопасности наметился перелом. Экспоненциальный рост количества рисков и событий, связанных с безопасностью, значительно осложняют работу специалистов данного профиля. Стремительное изменение ландшафта угроз, усложнение самих угроз и увеличение их разнообразие делают невозможным адекватное реагирование в рамках традиционных подходов. Последствия инцидентов безопасности и утечек данных становятся все серьезнее. Финансовые издержки и риски стремительно растут. Наконец, многие организации испытывают трудности при подборе специалистов по безопасности, обладающих необходимыми навыками. Эти и другие трудности весьма осложняют для организаций поддержание здоровой иммунной системы, необходимой для защиты своей деятельности.

При составлении данного отчета мы опросили 700 ИТ-директоров по безопасности (CISO) и других руководителей служб безопасности из 35 стран и 18 отраслей экономики. Перед нами стояла цель — определить основные задачи, стоящие перед этими руководителями, выявить трудности, с которыми они сталкиваются, и выяснить используемые подходы к их преодолению. Мы также хотели выяснить, каковы их взгляды на когнитивные решения безопасности. Узнать, осознают ли руководители полезность этих решений, понять степень готовности к их внедрению и возможные факторы, препятствующие использованию когнитивных решений.

В результате мы выяснили, что основную трудность для руководителей представляет сложность угроз и необходимость оперативного реагирования. Они обеспокоены негативным влиянием инцидентов безопасности на коммерческую деятельность предприятия, а также волнуются о репутационных рисках, которые несут с собой подобные инциденты. Руководители отделов ИТ-безопасности сравнительно низко оценивают эффективность своей работы по защите вычислительных сетей и данных, а также по созданию системы оперативного и интеллектуального реагирования на угрозы. Тем не менее, они рассчитывают устранить выявленные недостатки в течение нескольких лет. Привлечение необходимых специалистов к решению этих задач может представлять собой сложную проблему. Сталкиваясь с ростом издержек и нехваткой опытных специалистов в сфере безопасности, отвечающих за это направление, руководители отделов ИТ-безопасности ищут способы более эффективного использования денежных средств, выделенных руководителями бизнеса.

Основная задача, **которую постоянно приходится решать** специалистам по кибербезопасности — **уменьшение среднего времени реагирования на инциденты и устранение последствий**.

57% Директора по ИТ-безопасности убеждены, **что когнитивные решения безопасности** значительно **связывают руки киберпреступникам**.

Согласно прогнозам, **количество специалистов** в сфере безопасности, **занятых внедрением когнитивных решений безопасности,** вырастет втрое в течение следующих 2–3 лет.

Растущий объем данных, собираемых при решении вопросов безопасности, и необходимость их глубокого анализа требуют больших трудозатрат. Эти задачи невозможно решить вручную. Как следствие, некоторые компании обращаются к когнитивным решениям безопасности, чтобы повысить эффективность, оперативность и точность интеллектуального анализа данных. Когнитивные технологии безопасности делают свои первые шаги, однако их потенциал внушает большую надежду и оптимизм. По словам участников нашего опроса, они ожидают от когнитивных решений безопасности следующих основных преимуществ: рост эффективности и точности при выявлении инцидентов и принятии решений, связанных с их устранением, значительное уменьшение времени реагирования на инциденты и улучшенное распознавание рядовых событий и инцидентов безопасности. Несмотря на многообещающие перспективы, широкомасштабное внедрение когнитивных решений требует большой подготовительной работы и обучения специалистов.

Тем не менее, нам удалось выделить группу организаций, полностью готовых к работе в когнитивную эпоху решений безопасности. Изучая вопросы эффективности систем безопасности, готовности к внедрению когнитивных решений и общего понимания предмета исследования, мы выделили группу энтузиастов среди руководителей отделов ИТ-безопасности. Они готовы вступить в когнитивную эпоху решений безопасности уже сегодня. В целом, эти руководители лучше знакомы с когнитивными решениями, больше уверены в своих навыках по обеспечению безопасности и не считают привлечение необходимых специалистов трудной задачей.

Развитие и распространение когнитивных решений безопасности откроет большему числу организаций свободный доступ к их преимуществам. Если вы считаете себя готовыми двигаться в этом направлении, первым шагом станет выявление недостатков, которые вы надеетесь устранить с помощью когнитивных решений безопасности. Затем вам нужно изучить возможные примеры использования этих решений и сопоставить их со слабыми сторонами вашей системы безопасности. Современный деловой мир требует обоснования любых инвестиций, поэтому уделите время обсуждению преимуществ когнитивных решений безопасности с руководителями вашей компании. В ходе беседы, общаясь на одном языке с деловыми людьми, постарайтесь подчеркнуть важность этих решений для повышения общего уровня безопасности вашей организации. Проделав предварительные шаги, вы сможете подготовить вашу организацию к работе в когнитивную эпоху кибербезопасности.

Актуальный контекст

Когда вы бегло ознакомитесь с текущим ландшафтом кибербезопасности, обрисованным в ходе опроса ИТ-руководителей по безопасности, у вас может сложиться впечатление, что текущая ситуация вполне управляема. В целом, опрошенные специалисты абсолютно уверены в эффективности растущего потенциала своей компании (как технологического, так и организационного). Большинство опрошенных (77%) считают свою организацию готовой к отражению угроз кибербезопасности ничуть не хуже отраслевых конкурентов. Респонденты также весьма оптимистично смотрят в будущее. По мнению 86% опрошенных, в следующие 2–3 года они будут лучше готовы к отражению угроз кибербезопасности, *чем свои* конкуренты по отрасли.

Подобные ответы вряд ли могут кого-то удивить, однако важно изучить причины, лежащие в их основе. ИТ-руководители по безопасности убеждены, будто справляются с угрозами ничуть не хуже своих коллег из других организаций. Они уверены в эффективности своей работы и намерены работать еще эффективнее. Почти три четверти опрошенных убеждены, что выстроили эффективный фундамент безопасности организации. При этом 72% заявляют, что наладили эффективную ИТ-гигиену, а еще 71% считают успешной созданную ими систему анализа рисков в масштабах компании. Однако давайте углубимся в тему и оценим реальное положение дел. Что на самом деле творится с задачами, последствиями инцидентов, финансированием и рентабельностью инвестиций в безопасность?

Жажда скорости

Первоочередная задача для современных ИТ-руководителей по безопасности — уменьшение среднего времени реагирования на инциденты и устранения последствий. По мнению 45% опрошенных, именно эти задачи кибербезопасности являются наиболее важными. По их мнению, названные задачи будут наиболее актуальными для организаций в течение следующих 2-3 лет. Что касается перспектив, 53% респондентов убеждены, что первоочередной задачей останется повышение оперативности реагирования (см. рис. 1).

«Мы словно коммивояжеры в золотой век пиратства — нас не защищает военный флот, нас не прикрывают полицейские силы. Мы предоставлены сами себе. Кроме того, многие из нас не умеют управляться со своими кораблями и не могут открывать огонь по нападающим (это незаконно). Мы пытаемся выжить во враждебном мире со связанными за спиной руками. Впрочем, в нашем распоряжении имеются весьма любопытные и довольно продуманные инструменты, способные выявить всю подноготную наших угроз».

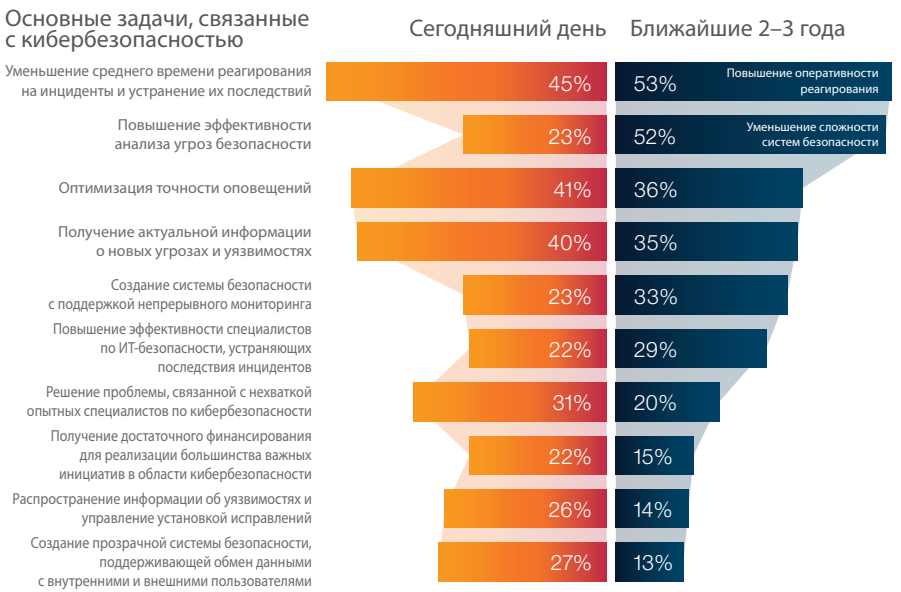
Дэвид Шипли, Директор по стратегическим инициативам, подразделение ИТ-услуг, университет Нью-Брансуика

Промедление увеличивает риски

Согласно научному исследованию, проведенному институтом Понемона в 2016 г., среднее время обнаружения утечки данных составляет 201 день, а среднее время ее устранения — целых 70 дней. Сотрудники института также выяснили, что наличие команды реагирования на инциденты - основной фактор снижения финансовых потерь, вызванных утечкой данных.[1]

Рисунок 1

Основные задачи кибербезопасности (актуальные и перспективные) глазами ИТ-руководителей по безопасности



Озабоченность этими трудностями сохраняется, даже несмотря на тот факт, что 80% организаций заметно повысили оперативность реагирования на инциденты по сравнению с показателями двухлетней давности, ускорившись в среднем на 16%. 86% опрошенных хотят нарастить оперативность реагирования в течение ближайших 2-3 лет (в среднем, еще на 24%).

Очевидно, данный вопрос крайне важен для всех организаций. Чем дольше организация реагирует на инцидент, тем выше причиненный ущерб и тем больше затраты, связанные с устранением кризисной ситуации. Убытки прямо пропорциональны времени реагирования.

Еще одна трудность, которую все сложнее преодолевать ИТ-руководителям по безопасности, — повышение эффективности анализа угроз безопасности. 23% респондентов считают это наиболее актуальной из современных задач. Тем не менее, по мнениюцелых 52% респондентов основная задача кибербезопасности на ближайшие 2–3 года — повышение эффективности анализа угроз безопасности. Аналитикам безопасности нужна помощь при получении информации, при выявлении наиболее острых угроз безопасности, при оперативном выявлении повторяющихся действий и отклонений в деятельности пользователей. Руководители отделов ИТ-безопасности намерены использовать любые средства, способные повысить оперативность отклика и снизить остроту угроз, с которыми им приходится сталкиваться.

Рост обеспокоенности

По словам почти трех четвертей опрошенных, за последние годы вторжения злоумышленников причинили весомый ущерб текущей коммерческой деятельности. Несмотря на это, респонденты ожидают значительного улучшения ситуации в ближайшие несколько лет.

Руководство компаний все чаще опасается, что незаконное проникновение в ИТ-системы может серьезно навредить не только коммерческой деятельности, но и — репутации используемых брендов. Озабоченность репутационными издержками удваивается, если спросить респондентов о перспективах. Целых 35% считают эту угрозу наиболее серьезным вызовом последних двух лет, тогда как 68% намерены побеспокоиться о ней через несколько лет (см. рис. 2). Столь кардинальное изменение взглядов означает, что ИТ-руководители по безопасности опасаются роста серьезности последствий, которые несут с собой действия злоумышленников. При этом акцент с ущерба для коммерческой деятельности все чаще смещается на репутационные издержки. Подмоченная репутация плохо влияет на прибыль — когда доверие падает, клиенты уходят.

Рисунок 2

По словам представителей организаций, последствия проникновения злоумышленников в ИТ-системы весьма разнообразны, однако основная тяжесть последствий станет ощутима лишь через несколько лет.

Рост расходов на инфраструктуру кибербезопасности также становится все более острой проблемой. Ожидается многократное увеличение расходов. Работая в условиях постоянного риска, связанного с успешным вторжением в ИТ-системы, организации тратят все больше денег на решение этой проблемы. Руководители отделов ИТ-безопасности часто считают, будто виновника успешного проникновения в ИТ-системы всегда можно отыскать. Поэтому, чтобы защитить свои компании, они нанимают более опытных специалистов, внедряют точечные решения и улучшают инфраструктуру.

Упущения, связанные с безопасностью

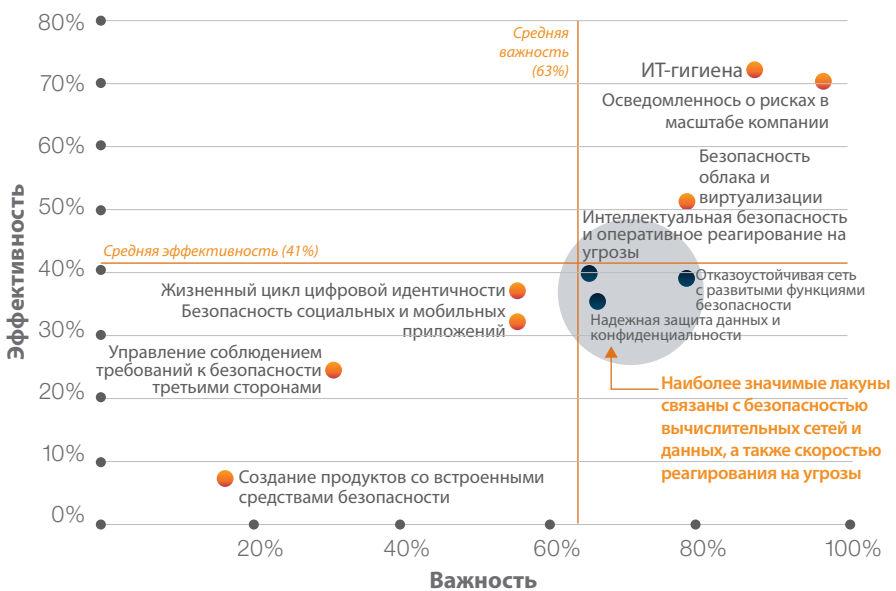
Мы попросили респондентов, занимающихся различными аспектами безопасности, назвать самые важные элементы своей системы безопасности и описать, какие категории задач они решают наиболее эффективно. Руководители отделов ИТ-безопасности считают все элементы своих систем безопасности одинаково важными, поскольку исповедуют целостный подход к защите предприятия. Однако, действуя в условиях нехватки ресурсов, невозможно всегда использовать только передовые решения на всех направлениях. Это самоочевидно, поскольку каждый день возникают новые технологии, подходы и задачи.

Большинство респондентов рассказали нам о своем подходе к ИТ-гигиене и управлением осведомленностью о рисках в масштабах компании, описав основные технологические и организационные аспекты безопасности. Мы решили исследовать направления, которые показались респондентам наиболее важными и где они сочли свою работу недостаточно эффективной (см. рис. 3). К этой категории относится защита вычислительных сетей и данных вкупе с реагированием на угрозы.

По мнению респондентов, они страдают от недостаточной эффективности в следующих аспектах деятельности: оперативность реагирования на угрозы, управления событиями с информацией о безопасности (SIEM), обнаружение действий в вычислительных сетях, фильтрация и классификация данных, а также предотвращение убытков. Безусловно, поиск подходов к управлению ростом объема и сложности рисков безопасности — одна из насущных задач любой организации. Уделив особое внимание времени реагирования и решив проблему сложности рисков с помощью развитой аналитики угроз, организации могут заметно повысить эффективность своей системы безопасности.

Рисунок 3

Сравнительный анализ важности и эффективности различных средств безопасности



«Мониторинг и анализ системы безопасности позволили найти способы заметного сокращения расходов в масштабах всего предприятия. В частности, мы сократили расходы на оплату трафика, вывели из эксплуатации недоиспользуемые ресурсы и повысили производительность труда сотрудников, уменьшив объем спама».

Ведущая компания Канады в отрасли страхования финансовых рисков, управления частным капиталом и активами

Следим за бюджетом

Руководители отделов ИТ-безопасности решают широкий круг вопросов, причем каждый требует внимания. Они хорошо представляют грядущий рост расходов на обеспечение эффективной безопасности и убеждены, что этот рост сохранится и впредь. 78% руководителей отмечают рост расходов на кибербезопасность за последние два года, а 84% прогнозируют дальнейший рост расходов на протяжении еще 2–3 лет. В действительности, более 70% опрошенных тратят на кибербезопасность более 10% общего ИТ-бюджета (большинство тратит 10-15%). В основном, эти расходы направлены на предупреждение и выявление угроз. Наибольшие затраты на кибербезопасность несут финансовые учреждения, которые тратят на эти цели до 500 млн долларов США ежегодно.[2] Высокие расходы не гарантируют высокой эффективности защиты, поэтому долгосрочный рост затрат себя не оправдает. — Руководителям отделов ИТ-безопасности придется искать способы обоснования этих инвестиций.

92% респондентов заявили, что их заявки на финансирование инициатив в сфере кибербезопасности требуют предварительного расчета рентабельности (ROI) или иного финансового анализа. В противном случае, эти расходы окажутся необоснованными и не будут одобрены. Среди доводов в пользу внедрения новых решений можно выделить два основных фактора: четкое артикулирование текущего уровня рисков для организации (61% опрошенных) и поддержка этой инициативы со стороны ключевых руководителей, возглавляющих отделы финансов, риск-менеджмента, коммерческой деятельности и др. (51% опрошенных). Руководители отделов ИТ-безопасности должны уметь формулировать свои потребности на языке бизнеса и обращаться за поддержкой к другим руководителям высшего звена своей компании.[3] Кроме того, они обязаны искать новые подходы к обоснованию расходов на кибербезопасность и должны демонстрировать эффективность этих вложений. Необходимо окончательно избавиться от представления, будто расходы на безопасность аналогичны расходам на страхование бизнеса или текущую деятельность.

Устраняем недоработки

Впрочем, есть и хорошие новости. Опрошенные нами руководители отделов ИТ-безопасности знают о недостатках своего подхода к построению системы безопасности и планируют устранить их в ближайшем будущем. Организации реализуют различные инициативы, повышающие готовность к наступлению рисков (см. рис. 4). В настоящее время они прилагают основные усилия к повышению эффективности сотрудников, налаживая образование и обучение (67% опрошенных представителей организаций). Кроме того, 47% респондентов внедряют ПО для мониторинга персональных данных. В целом, именно эти подходы к устранению недостатков являются основными.

Рисунок 4

Реализуемые руководителями по ИТ-безопасности инициативы в целях повышения готовности к наступлению рисков кибербезопасности

Положение сегодня		Положение через 2–3 года	Инициативы
1	▼-30%	5	Повышение эффективности сотрудников путем обучения
2	▼-25%	7	Внедрение ПО для мониторинга действий пользователей
3	▲+8%	4	Создание отчетности об операционных и стратегических мерах безопасности с помощью новых аналитических средств
4	▲+28%	1	**Повышение эффективности мониторинга сети, приложений и безопасности на уровне данных**
5	▲+17%	3	**Совершенствование методологии реагирования на инциденты, рабочих процессов и оперативности реагирования**
6	▼-9%	8	Расширение штата аналитиков безопасности и их обучение
7	▼-16%	10	Тестирование безопасности приложений (включая мобильные приложения и API)
8	▲+36%	2	**Создание или модернизация средств SOC**
9	▲+14%	6	Внедрение решений безопасности на базе когнитивных технологий
10	▲+1%	9	Использование средств сетевой криминалистики при обеспечении ИТ-безопасности

«Руководители устали выбрасывать деньги на безопасность, не получая никакой положительной отдачи. У них не складывается ощущение, что расходы прошлых лет помогли обезопасить организацию. Отвечающие за безопасность руководители должны изыскивать новые обоснования для инвестиций. Недостаточно просто оценить положение дел, выявить недостатки и попросить денег на их устранение».

Чед Холмс (Chad Holmes), Технический директор и руководитель нескольких направлений (киберстратегия, технология и развитие) в консалтинговом агентстве Ernst & Young LLP

В ближайшие 2-3 года ожидается кардинальное изменение подхода к реализации подобных инициатив. По мнению респондентов, тройка ведущих инициатив будет выглядеть совершенно иначе. На первое место выйдет усиление безопасности на уровне сети, приложений и данных (57% опрошенных). Второй по важности инициативой станет создание или модернизация средств SOC. И наконец, третье место займет повышение оперативности реагирования на инциденты. Каждый из этих аспектов соответствует выделенным ранее направлениям, работу по которым руководители признают неэффективной.

Приятно видеть, как Руководители отделов ИТ-безопасности устраняют недостатки своей деятельности, однако изменение приоритетов может привести к возникновению новых недостатков или усугублению имеющихся. Руководители отделов ИТ-безопасности должны любой ценой решить важнейшие вопросы, напрямую связанные с деятельностью своих предприятий. Весь вопрос в том, окажутся ли достаточными планируемые усилия.

Недостатки как они есть

Все вышеупомянутые трудности, слабые места, усилия и проблемы можно свести к трем недостаткам, связанным с недостаточно интеллектуальным, оперативным и точным анализом угроз. Отвечающие за безопасность руководители обязаны устранить выявленные недостатки, при этом не забывая об управлении издержками и сохранении рентабельности.

Нехватка интеллектуального анализа

- По мнению 65% респондентов, именно исследование угроз связано с наибольшими трудностями, возникающими ввиду нехватки специалистов.
- 40% респондентов заявили, что одна из основных трудностей при обеспечении кибербезопасности — получение сведений об актуальных угрозах и уязвимостях.

Недостаточная оперативность

- Наиболее сложная задача кибербезопасности, актуальность которой не меняется со временем, — уменьшение среднего времени реагирования на инциденты и устранения последствий. И это несмотря на то, что 80% респондентов уверяют, что среднее время реагирования на инциденты заметно сократилось, если сравнивать с показателями двухлетней давности.
- Респонденты прогнозируют увеличение трудозатрат на деятельность в этой области в ближайшие годы. Только 27% сообщили, что в настоящее время реализуют инициативы, связанные с сокращением времени реагирования на инциденты. Впрочем, количество таких организаций вырастет до 43% в течение ближайших 2-3 лет.

Недостаточная точность

- По мнению респондентов, второй по важности вопрос - оптимизация оповещений безопасности, поскольку современные системы выдают слишком много ложных срабатываний.
- Еще одним направлением, ставшим сложным из-за нехватки специалистов, 61% респондентов называет выявление и оценку угроз, а также выбор инцидентов, которые нужно передавать более опытным специалистам.

Наиболее известные преимущества когнитивного решения безопасности

1. Интеллектуальность

Развитые средства обнаружения инцидентов и принятия решений при реагировании

2. Оперативность

Значительное сокращение времени реагирования на инциденты

3. Точность

Повышенная точность выявления настоящих инцидентов; меньше ложных срабатываний

Трехкратный рост

количества когнитивных решений безопасности, планируемых к внедрению в ближайшие 2–3 года

Перспективы применения когнитивной безопасности

Когнитивные системы будут использоваться для анализа тенденций в сфере безопасности, а также для анализа огромных объемов структурированных и неструктурированных данных с целью извлечения практически полезных знаний. Руководители отделов ИТ-безопасности и подчиненные им аналитики не могут освоить все созданные людьми знания, связанные с вопросами безопасности, включая результаты научных исследований, отраслевые публикации, аналитические отчеты и блоги. Когнитивные системы используют эту информацию совместно с более традиционными данными о безопасности. Когнитивные решения безопасности используются совместно с автоматизированными технологиями безопасности, приемами и процессами, которые учитывают поступающие данные. В результате достигается высочайшая эффективность учета контекста и невероятная точность анализа.

Когнитивные решения безопасности могут дополнять собой возможности SOC-анализа. Вследствие этого они увеличивают скорость реагирования, помогают лучше выявлять угрозы и эффективнее защищать приложения, а также снижают общий уровень риска на предприятии. Цель — избавить аналитиков от рутинных задач, связанных с обеспечением безопасности, и поручить им более интеллектуальный труд.

Когнитивные решения безопасности как ответ на эти вопросы

Чтобы устранить выявленные недостатки, необходимо использовать различные технологии и подходы. Организациям не удастся решить эту задачу путем привлечения более опытных специалистов или увеличением расходов, если мы говорим о долгосрочной стратегии. Многолетнее развитие технологий безопасности позволило перейти от простых средств управления периметром (например, поддерживающих только статичную защиту) к более развитым средствам интеллектуального анализа безопасности (например, анализ данных в реальном времени и поиск отклонений от паттернов использования).

Мы вступаем в когнитивную эпоху безопасности, для которой характерны решения, умеющие понимать контекст и поведение, умеющие анализировать как структурированные, и неструктурированные данные о безопасности. Когнитивная безопасность предусматривает новые аспекты взаимодействия между аналитиками безопасности и технологическими средствами, которые они используют. Эти решения способны интерпретировать и упорядочивать информацию, раскрывать ее смысл путем анализа и рационально обосновывать полученные выводы. Кроме того, они постоянно обучаются на основе накапливаемых данных и результатов анализа, получаемых в ходе взаимодействия со специалистом.

Преимущества когнитивных решений безопасности

Представьте, что в вашем распоряжении оказался набор решений на базе когнитивных технологий. Вот что они смогут:

- Расширение возможностей младших аналитиков SOC путем предоставления доступа к передовым методам работы и результатам анализа, использование которых раньше требовало многолетнего опыта.
- Повышение оперативности реагирования с помощью внешней аналитики, поступающей из блогов и других источников, чтобы вы могли принимать меры еще до получения вирусных сигнатур.
- Оперативное выявление угроз и рискованного поведения пользователей, утечек данных и заражения вредоносным ПО с помощью развитых аналитических методов.
- Расширение обозримого контекста инцидентов безопасности благодаря автоматизации анализа и сбора данных (локальных и внешних).

Трудности и перспективы

Многие из опрошенных убеждены, что преимущества когнитивных решений безопасности помогут закрыть слабые места в собственной системе безопасности. Когнитивные технологии делают только первые шаги, однако 57% респондентов убеждены — когнитивные решения безопасности заметно связывают руки преступникам. Именно в этом они видят потенциальные преимущества новых решений.

Опросив руководителей отделов ИТ-безопасности, мы попросили назвать преимущества когнитивных решений безопасности. 40% сообщили о повышении эффективности выявления инцидентов и реагирования на них, включая принятие более точных решений, 37% указали на заметное сокращение времени реагирования на инциденты, а еще 36% заявили о более точном распознавании настоящих инцидентов. Респонденты хотят, чтобы когнитивные решения безопасности закрывали наиболее слабые места собственной системы безопасности. Им требуются решения, служащие основой интеллектуального, оперативного и точного анализа угроз.

В настоящее время только 7% опрошенных работают над внедрением когнитивных решений безопасности, чтобы повысить степень готовности предприятия к рискам кибербезопасности. Эта цифра не вызывает удивления, поскольку соответствующие решения появились совсем недавно. Однако в ближайшем будущем число желающих внедрить подобные решения вырастет втрое, достигнув 21%. В ближайшие несколько лет мы станем свидетелями ускоренного внедрения решений этого класса, поскольку отвечающие за безопасность руководители станут использовать возможности когнитивных систем в составе цифровых иммунных систем.

Респонденты также отметили сложности, связанные с внедрением когнитивных решений безопасности. Нельзя сказать, что руководители отделов ИТ-безопасности не понимают концептуальные принципы новой технологии или не уверены в ее преимуществах по сравнению с другими решениями. Основные трудности на пути внедрения связаны с нехваткой специалистов, несовершенством процессов и скудностью методик. 45% респондентов сообщили, что наибольшие трудности, связанные с внедрением, проистекают из некомпетентности и нехватки специалистов с требуемыми навыками (см. рис. 5). Чтобы развеять эти опасения, требуются предварительная подготовка и дополнительное обучение сотрудников.

Рисунок 5

Основные трудности внедрения когнитивных решений безопасности, названные руководителями отделов ИТ-безопасности

«Мы намерены перейти к следующему этапу внедрения когнитивных и интеллектуальных решений, которые смогут эффективно хранить и упорядочить огромный объем сведений и знаний по вопросам безопасности, включая актуальный контекст, управление которыми сейчас отнимает наше время и ресурсы».

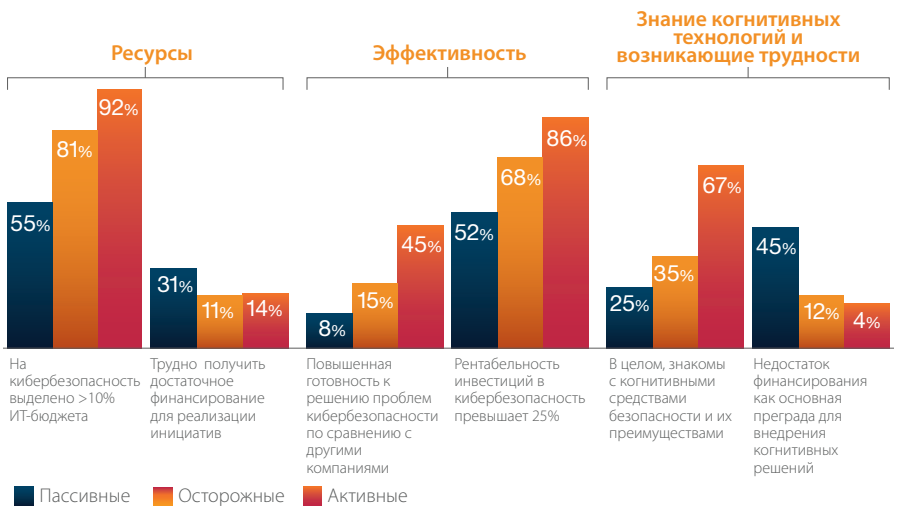
Ведущая компания Канады в отрасли страхования финансовых рисков, управления частным капиталом и активами

Активная кибербезопасность в когнитивную эпоху

Чтобы понять, какие организации готовы ворваться в эпоху когнитивной безопасности, мы составили профиль наших респондентов, опираясь на их собственную оценку эффективности своей системы безопасности, осведомленность о когнитивных решениях и готовность к их внедрению. Проанализировав ответы, мы поделили респондентов на три группы (см. рис. 6).

Рисунок 6

По степени готовности организации делятся на «Пассивных», «Осторожных» и «Активных».



Респонденты *из категории «Пассивных»*,составляющие 52% выборки, испытывает трудности с финансированием и подбором персонала. В среднем, эти организации меньше осведомлены о возможностях и преимуществах когнитивных средств безопасности. Как правило, эти организации выделяют на кибербезопасность меньшую долю ИТ-бюджета и чаще говорят о трудностях, связанных с получением необходимого финансирования и подбором кадров. Одними из препятствий на пути внедрения когнитивных решений они также назвали нехватку финансирования. (Чтобы узнать подробнее о том, как мы выделили эти кластеры и распределяли компании, см. раздел «Демография и методология» на стр. 20).

Респонденты *организации*, составляющие 27% выборки, не испытывают затруднений с нехваткой специалистов, которые характерны для «Пассивных» однако они на сегодняшний день не вполне готовы к внедрению когнитивных решений безопасности нового поколения.

Респонденты «*Активные*», на которую приходится 22% выборки, вошли наиболее осведомленные о когнитивных решениях безопасности организации, которые с большим энтузиазмом воспринимают внедрение этих систем. «Активные» организации лучше знакомы с когнитивной безопасностью и больше уверены в своих навыках, бюджете и перспективной рентабельности, нежели остальные. Руководители этих организаций убеждены, что исповедуют более зрелый подход к безопасности. Заметная их часть утверждает, что штатная группа специалистов безопасности способна отслеживать актуальные изменения ландшафта угроз. Они эффективно информируют руководство компании и совет директоров об актуальных рисках безопасности, а также учитывают кибернетические угрозы при моделировании рисков предприятия (см. рис. 7).

Рисунок 7

«Пассивные», «Осторожные» и «Активные» организации описывают свой подход к обеспечению безопасности

«Нас окружает невероятный объем информационного шума. Человеческий мозг не может ежедневно бороться с ним. Нам нужен помощник — например, искусственный интеллект или когнитивные технологии».

Чед Холмс (Chad Holmes), Технический директор и руководитель нескольких направлений (киберстратегия, технология и развитие) в консалтинговом агентстве Ernst & Young LLP

«Безопасностью нужно заниматься круглосуточно, поэтому у многих организаций нет денег на соответствующих специалистов. Здесь на помощь приходит когнитивная система безопасности, не знающая ни сна, ни усталости».

Майкл Пинч, Директор по ИТ-безопасности, Рочестерский университет

Какие требования предъявляют отвечающие за безопасность руководители к когнитивным решениям безопасности, приступая к их внедрению? Общаясь с представителями компаний из категории «Активные», мы выделили следующие особенности когнитивных решений безопасности, которые показались им наиболее важными:

- Круглосуточный режим работы, непрерывная поддержка
- Меньшее количество ложных срабатываний, поиск аномалий в поведении пользователей и систем
- Тщательный анализ ландшафта угроз и описание инцидентов в контексте текущий событий
- Управление поддержкой, риск-менеджментом и соответствием с учетом уникальных требований, предъявляемых отраслью, географическим положением и законодательством
- Изменение характера деятельности по обеспечению безопасности — оптимизация труда аналитиков и повышение его эффективности.

Следует ожидать, что отвечающие за безопасность руководители, уверенные в собственной компетентности и располагающие достаточными ресурсами, первыми приступят к внедрению совершенно новой технологии (такой, как когнитивная безопасность). Однако важно понимать, что любой специалист, прошедший обучение и обладающий необходимым опытом, может использовать когнитивные технологии для устранения недостатков своей системы безопасности и помощи аналитикам в повышении эффективности мер безопасности.

Рекомендации

Мы изучили актуальный ландшафт безопасности, чтобы понять, с какими трудностями и задачами сталкиваются наши респонденты и какие у них приоритеты. По результатам наших наблюдений мы составили список рекомендаций, которые помогут вам и вашей организации подготовиться к вступлению в эпоху когнитивной кибербезопасности.

Узнайте свои слабости
Руководители отделов ИТ-безопасности стремятся повысить оперативность работы систем безопасности и снизить их сложность. Они больше всего обеспокоены возможными репутационными издержками инцидентов безопасности. Определите основные слабости и уязвимости внутри вашей организации. Как они взаимосвязаны? Какие из них наиболее приоритетны?

- Страдаете ли вы от недостатка интеллектуального анализа и исследования угроз?
- Достаточно ли оперативно вы реагируете на инциденты и устраняете их последствия в ходе текущей деятельности?
- Легко ли вы отличаете ложные инциденты от настоящих? Испытываете ли вы сложности при получении контекста инцидента?

Изучите возможности когнитивных средств безопасности
Используйте целостный, формализованный подход к изучению решений в области когнитивной безопасности Среди сотрудников вашей организации могут бытовать ошибочные представления о возможностях этих средств, издержках их использования и трудностях внедрения.

- Знайте возможные сценарии использования когнитивных решений безопасности и закрываемые ими слабые стороны вашей системы безопасности. Хотите видеть расширенный контекст инцидентов безопасности, наладить сбор доказательств, чтобы повысить качество принимаемых решений или найти новые способы заблаговременной оценки риска?
- Спланируйте, как вы будете объяснять преимущества когнитивных решений безопасности руководителям, отвечающим за решение технических и коммерческих вопросов — составьте план обучения ваших подчиненных и руководителей.

«Когнитивная безопасность отличается совершенно невероятным потенциалом — она поможет вам уменьшить профиль рисков и повысить эффективность реагирования. Кроме того, она помогает понять контекст происходящего. Люди привыкли воспринимать контекст в виде четкой последовательности событий, из которой становится ясно - что случилось и кто виноват. Кроме того, когнитивные технологии предъявляют меньшие требования к навыкам специалистов, желающих работать в кибербезопасности. Когнитивные технологии помогут вам привлечь к решению задач разноплановых специалистов без опыта работы в ИТ».

Дэвид Шипли, Директор по стратегическим инициативам, подразделение ИТ-услуг, университет Нью-Брансуика

- Определите, специалистов какого профиля вам не хватает для внедрения новой технологии в своей организации, и наймите сотрудников с нужными навыками.

Разработайте инвестиционный план.

Безусловно, составление инвестиционной программы для новой технологии, еще не доказавшей своих преимуществ на рынке, связано с множеством трудностей. — Сложно найти примеры, на которые можно сослаться. Сложно создать атмосферу доверия. Поскольку подавляющее большинство респондентов утверждает, что заявки на финансирование требуют обоснования рентабельности или иного финансового анализа, руководители отделов ИТ-безопасности обязаны использовать иной подход при внедрении когнитивных решений безопасности.

- Рассматривайте когнитивные решения безопасности как совершенно отдельную категорию продуктов. Отойдите от традиционных обоснований внедрения систем безопасности (например, уменьшение затрат на устранение последствий инцидентов) — придумайте нечто новое. Уделите основное внимание следующему факту: когнитивный подход к безопасности повышает общую эффективность любой деятельности, связанной с обеспечением безопасности.
- Используйте разработанный вами план обучения, чтобы добиться понимания со стороны других руководителей бизнеса. Сделайте так, чтобы они помогли вам составить инвестиционный план.
- Мыслите творчески и подходите нестандартно к ответу на вопрос, каким образом ваши инвестиции в когнитивные технологии смогут помочь бизнесу, кроме увеличения рентабельности.

Анализируйте перспективу расширения возможностей вашей системы безопасности с помощью новой технологии, даже если используемые решения вполне эффективны

Организации из категории «Активные» обычно располагают большим объемом ресурсов, они более уверены в навыках своих специалистов и лучше готовы к внедрению когнитивных решений безопасности. Однако это не означает, что когнитивная безопасность предназначена для отдельной группы организаций. Когнитивные решения безопасности — это новое направление развития высоких технологий, возможности которых полезны любым организациям, начиная от небольших и заканчивая самыми крупными.

- *Если ваша организация относится к категории «Пассивные»:* Определите роль и место когнитивных решений безопасности в преодолении трудностей бизнеса и замещении специалистов, затем составьте инвестиционный план.
- *Если ваша организация относится к категории «Осторожные»:* Целенаправленно занимайтесь сбором информации, чтобы меньше волноваться о нехватке специалистов с необходимыми навыками.
- *Если ваша организация относится к категории «Активные»:* Беритесь за дело с энтузиазмом! Возьмите конкретный сценарий использования для пилотного внедрения когнитивной системы и постарайтесь задействовать ее в решении текущих задач, связанных с безопасностью.

Дополнительная информация

Чтобы узнать подробнее об этом научном исследовании, проведенном научно-исследовательским институтом IBM Institute for Business Value, отправьте электронное письмо по адресу iibv@us.ibm.com. Читайте нас в Твиттере по реплаям @IBMIBV. Чтобы получить полный каталог наших научных исследований или подписаться на наш месячный бюллетень, посетите сайт **ibm.com**/iibv.

Читайте отчеты для руководителей, составленные специалистами IBM Institute for Business Value, прямо на телефоне или планшете, загрузив бесплатное приложение IBM IBV для iOS или Android из магазина приложений.

Надежный партнер в изменчивом мире

Работая в тесном контакте с заказчиками, IBM внедряет решения на основе систем бизнес-аналитики, современные технологии и научные исследования, чтобы обеспечить заказчикам значительное конкурентное преимущество в современной стремительно меняющейся деловой среде.

IBM Institute for Business Value

Научно-исследовательский институт IBM Institute for Business Value, входящий в состав подразделения IBM Global Business Services, составляет аналитические отчеты стратегического характера для высшего руководства компаний, посвященные критически важным проблемам государственного и частного сектора и опирающиеся на проверенные факты.

Авторы
Лиза ван Дет, менеджер по маркетингу, направление «Проведение кампаний и стратегия формирования мнений», IBM Security; Кристоф Велтсос, адъюнкт-профессор, кафедра информатики Миннесотского университета, Манкейто.

Благодарности
Калеб Барлоу, вице-президент, направление всемирного маркетинга портфеля продуктов, подразделение IBM Security; Мария Баттаглиа, директор по маркетингу, направление отказоустойчивых решений, IBM Security; Вангуй Маккилви, директор по маркетингу портфеля продуктов (услуги безопасности и защита от интернет-мошенничества), подразделение IBM Security; Кевин Скапинец, директор по стратегии, подразделение IBM Security; аналитическое бюро Oxford Economics, за помощь при администрировании сбора данных в ходе опроса.

Примечания и источники

1 «Научное исследование: ущерб от утечек данных за 2016 г.: глобальный анализ (2016 Cost of Data Breach Study: Global Analysis) Институт Понемона. Июнь 2016 г. http://www-03.ibm.com/security/data-breach/

2 Гэйб Фридман (Friedman, Gabe) Уполномоченный JPMorgan: банк потратит 500 млн долларов США на кибербезопасность (JPMorgan Chase Atty: Bank Will Spend $500M on Cyber Security) 29 января 2016 г. https://bol.bna.com/jpmorgan-chase-atty-bank-will-spend-500m-on-cyber-security/. Дата последнего доступа: 21 сентября 2016 г.

3 Келли, Диана и Карл Нордман (Kelley, Diana, Carl Nordman). Защита большого босса: перспективы кибербезопасности с точки зрения высшего руководства и совета директоров (Securing the C-suite: Cybersecurity perspectives from the boardroom and C-suite). IBM Institute for Business Value 2016. ibm.biz/csuitesecurity

Демография и методология
Чтобы лучше понимать связанные с обеспечением безопасности задачи, стоящие перед организациями, их подходы к решению этих задач и их представление о характере и потенциале когнитивных решений безопасности, институт IBM Institute for Business Value (IBV) и Oxford Economics опросили 700 ответственных за безопасность ИТ-директоров и прочих специалистов в сфере безопасности из 35 стран и 18 отраслей экономики в период с мая по июль 2016 г. Эта совокупность специалистов отличается равномерным распределением свойств.

Чтобы выделить кластеры организаций («Пассивные», «Осторожные» и «Активные»), мы использовали алгоритм кластеризации k-средних, позволивший выявить три различных паттерна поведения. Чтобы определить эти поведенческие паттерны, мы задавали различные вопросы, связанные с эффективностью безопасности, пониманием особенностей когнитивных технологий и готовностью к их внедрению.

Об авторах
Диана Келли — исполнительный советник по безопасности (ESA) подразделения IBM Security и руководитель IBM Security Newsroom. В роли ESA она использует свой более чем 25-летний опыт работы в ИТ-безопасности, предоставляя советы и рекомендации ИТ-директорам и специалистам по безопасности. Она является одним из соавторов отчета IBM X-Force и часто делится оригинальными идеями и передовыми методиками в своих статьях, публикуемых в блоге Security Intelligence. Она также является действующим научным сотрудником IANS Research, членом консультативного совета InfoSec World, а также участником комитета по разработке повестки дня конференции женщин-руководителей Executive Women's Forum. Диана часто выступает на конференциях, посвященных вопросам безопасности. Ее часто привлекают как эксперта по безопасности такие издания, как *The New York Times, TIME*, MSNBC.com, *журнал Information Security* и *The Wall Street Journal*. Она является соавтором книги *«Криптографические библиотеки для разработчиков» (Cryptographic Libraries for Developers)*. Электронная почта Дианы: ibm.com.

Виджай Дип — руководитель программ в подразделении IBM Security Division. Он занимается созданием коммерческих продуктов на основе новейших технологий. В настоящее время он руководит разработкой целого портфеля предложений, связанных с интеллектуальным анализом угроз безопасности, в состав которого входят улучшенные аналитические средства, когнитивные технологии и SaaS. Ранее он руководил подразделениями, занятыми кибернетической криминалистикой и мобильной безопасностью. Виджай — блестящий специалист по высоким технологиям и невероятно увлеченный своим делом человек. Ему принадлежит титул IBM Master Inventor. В его патентный портфель входят инновации, связанные с мобильными технологиями, совместной работой и безопасностью. Он получил международную степень MBA в Школе бизнеса Фукуа школа при Университете Дьюка и степень магистра компьютерной техники в канадском университете Ватерлоо. Электронная почта Виджая: vdheap@us.ibm.com.

Дэвид Джарвис — руководитель отделов ИТ-безопасности и информационных технологий в научно-исследовательском институте IBM Institute for Business Value. Он отвечает за разработку и реализацию программ, связанных с изучением актуальных деловых и технологических трендов в этих областях. Дэвид с энтузиазмом занимается разработкой и управлением проектами, связанными с анализом рынка, распространением оригинальных идей и стратегическим анализом. Работая в IBM, он занимал множество постов, связанных с реализацией подобных проектов. Он является автором большого числа отчетов о кибербезопасности, содержащих ряд оригинальных концепций, включая составленный IBM отчет CISO Assessments за 2012-2014 гг. Кроме научно-исследовательской деятельности, Дэвид преподает деловое планирование и обучает творческому подходу к принятию решений. Электронная почта Дэвида: djarvis@us.ibm.com.

Карл Нордман — международный директор научно-исследовательской программы изучения руководителей высшего звена C-suite Study Program. Он также возглавляет исследование потребностей финансовых директоров предприятий в научно-исследовательском институте IBM Institute for Business Value. Он отвечает за проведение важнейших исследований в обеих предметных областях. Под его руководством сотрудники ведут исследования, помогающие вскрыть текущие тренды и очертить перспективы, связанные с актуальными вопросами стратегического значения. За плечами Карла более 25 лет работы специалистом по финансовым рискам и борьбе с мошенничеством. Ранее он занимал различные должности в подразделении консалтинговых услуг IBM. Эти должности предусматривали взаимодействие с финансовыми директорами компаний из списка Fortune 1000, а также оказание различным клиентам аутсорсинговых услуг, связанных с финансами и учетом, в качестве ведущего специалиста по работе с клиентами. Электронная почта Карла: carl.nordman@us.ibm.com.

IBM Восточная Европа/Азия
123317, Москва
Пресненская наб., 10
Тел.: +7 (495) 775-8800
Факс: + 7 (495) 258-6468, 258-6404
ibm.com/ru

SEL03111-RURU-00