Ларри Клинтон

КИБЕРБЕЗОПАСНОСТЬ ДЛЯ БИЗНЕСА

КАК СДЕЛАТЬ ЗАЩИТУ ОТ КИБЕРУГРОЗ
ЗАДАЧЕЙ ВСЕЙ КОМПАНИИ

КИБЕРБЕЗОПАСНОСТЬ — ЭЛЕМЕНТ СТРАТЕГИИ БИЗНЕСА

Компании часто ошибочно рассматривают кибербезопасность как исключительно техническую задачу, что приводит к недостаточному финансированию и неэффективным стратегиям. Киберпреступность наносит огромный ущерб мировой экономике, и за пугающими цифрами стоят конкретные истории взломов, утечек и потерь, которые причиняют реальный урон компаниям по всей планете.

По оценкам Всемирного экономического форума, ущерб от киберпреступности в 2020 году составил $2 трлн и продолжает расти опережающими темпами.

Цифровая трансформация — требование для каждого современного бизнеса, который хочет достойно конкурировать в своей отрасли. Но технический прогресс, открывающий новые коммерческие возможности, также увеличивает уязвимость к кибератакам.

Среди сравнительно новых факторов риска автор называет:

- распространение мобильных и облачных технологий, которое серьезно повышает риски утечки корпоративных и личных данных и требует внедрения новых мер кибербезопасности;
- развитие инструментов искусственного интеллекта (ИИ), которые злоумышленники используют для создания все более изощренных атак. Атаки с использованием ИИ особенно опасны из-за высокой способности алгоритмов анализировать и обходить установленные защиты;
- переход большого числа сотрудников на удаленку: пандемия COVID-19 резко ускорила этот процесс и вызвала взрывной рост числа кибератак. Риски утечки данных еще выше там, где для работы используются личные устройства;
- перенос операций, хранения данных и средств обеспечения безопасности в облачную инфраструктуру.

Если компания хочет устойчиво расти, ее кибербезопасность должна развиваться вместе с процессами основного бизнеса.

НАПЕРЕГОНКИ С ХАКЕРАМИ

Начиная с 1990-х годов и по настоящее время Американский национальный институт стандартов NIST (National Institute of Standards and Technology) публикует стандарты компьютерной безопасности с детальными разъяснениями и рекомендациями. Однако, к сожалению, предлагаемые меры недостаточны, потому что не способны опередить эволюцию угроз, возникающих в цифровой среде.

Киберугрозы эволюционируют быстро. Злоумышленники придумывают все новые способы нападения, включая персонализированные атаки и продвинутое программное обеспечение, для осуществления своих преступных целей.

Самые передовые и вредоносные на сегодня — атаки типа Advanced Persistent Threats (APT, продвинутая постоянная угроза). В таких атаках используются сложные, нестандартные методы, часто с применением нулевых уязвимостей (тех, о которых еще не догадывается жертва кибератаки) и социальной инженерии (то есть с использованием человеческих

слабостей для взлома защиты). APT-атаки дают злоумышленникам возможность проникать внутрь системы и долгое время оставаться незамеченными, а их цели — кража данных, шпионаж или даже разрушение инфраструктуры.

Этапы APT-атаки:

1) проникновение в сеть, например с помощью фишингового электронного письма или вредоносного вложения;
2) поиск уязвимостей: вредоносное программное обеспечение исследует уязвимости и обменивается данными с внешними серверами;
3) установка дополнительных точек взлома — это нужно, чтобы гарантировать продолжение атаки, если определенная точка входа или уязвимость будет раскрыта и защищена;
4) вредоносная деятельность в сети, к примеру сбор учетных записей и паролей, хищение конфиденциальных файлов или удаление важных данных.

APT-атаки обычно нацелены на крупные компании или даже правительственные организации, которые имеют дело со сверхсекретными данными, например с военными и финансовыми вопросами или патентами.

Чтобы действовать на опережение и надежно защищать свои данные и системы, бизнес уже не может рассчитывать только на соответствие нормативным требованиям. Динамика развития киберугроз требует выхода за рамки стандартных шаблонов, всестороннего анализа рисков и разработки процессов управления кибербезопасностью с точки зрения потенциального экономического ущерба.

ЭКОНОМИКА КИБЕРБЕЗОПАСНОСТИ

Экономические стимулы в кибербезопасности на первый взгляд не кажутся убедительными. Затраты компаний на предупреждение кибератак могут быть достаточно значительными, а возможный урон представляться не таким уж большим, пока он не нанесен.

К тому же любой ответственный специалист по кибербезопасности скажет, что полная защита невозможна. Инвестируя большие средства в собственную безопасность, компании лишь снижают свои риски, но никогда не могут их полностью исключить.

Даже хорошо защищенные системы, такие как военные сети, могут быть взломаны атаками среднего уровня.

Кроме того, руководителей может сбивать с толку понимание, что затраты злоумышленников на подготовку атак ничтожны (особенно если сравнить с их преступными прибылями). И этот дисбаланс будет существовать всегда: затраты на защиту выше затрат на нападение.

И все же тем, кто умеет мыслить стратегически, не нужно доказывать необходимость киберзащиты. Конечно, нет смысла, защищая свои активы, терять конкурентоспособность основного бизнеса.

Задача при управлении киберзащитой компании состоит в поиске оптимального баланса между рентабельностью и безопасностью.

КИБЕРРИСКИ И ФИНАНСЫ

Традиционные методы оценки киберугроз часто фокусируются на технических аспектах, но не учитывают экономические и стратегические последствия. При этом потенциально каждая кибератака может привести к финансовым, операционным или репутационным потерям компании.

Чтобы принимать обоснованные решения в сфере кибербезопасности, руководителям нужно видеть конкретные цифры — потенциальный ущерб в деньгах и стоимость защитных мер, которые могут свести его к минимуму.

Финансовый подход к оценке киберугроз включает:

- идентификацию и количественную оценку киберрисков в финансовых терминах;
- варианты для принятия, снижения или передачи рисков;
- согласование киберрисков с общим управлением рисками в компании.

Инвестиции в кибербезопасность могут приносить значительную отдачу ROI (Return on Investment), особенно если они направлены на специалистов, а не только на технологии.

Для оценки рисков используются эмпирические данные и финансовые модели, которые позволяют прогнозировать потенциальные потери и определять приоритеты в обеспечении кибербезопасности.

ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ

Для того чтобы усилия по кибербезопасности приносили максимальный эффект, задачи по ее обеспечению должны быть интегрированы во все аспекты бизнеса, включая деятельность HR и юристов, управление цепочками поставок и кризисное управление.

ВНЕШНИЙ И ВНУТРЕННИЙ АУДИТ

В значительной степени кибербезопасность зависит от внешнего и внутреннего аудита, и их роль должна меняться, чтобы можно было эффективно решать проблемы, возникающие в связи с развитием технологий и нарастанием угроз. Глобальный акцент на защите данных и конфиденциальности требует от предприятий выделения значительных бюджетных средств на выполнение требований по соблюдению нормативно-правовых актов, а также отслеживания изменившихся правил и рисков их несоблюдения. Для этого аудиту нужно взаимодействовать с другими отделами предприятия, чтобы согласовывать свою деятельность с бизнес-целями организации, принимать участие в стратегических проектах и лучше понимать инновационные технологии и методы, внедряемые в компаниях.

РОЛЬ СОВЕТА ДИРЕКТОРОВ

Совет директоров, как главный орган управления компанией, должен рассматривать кибербезопасность как стратегический приоритет, а также быть в курсе основных киберугроз и их потенциального влияния на бизнес.

Совет играет ключевую роль в управлении кибербезопасностью, обеспечивает разработку стратегии кибербезопасности, рабочих планов реагирования на инциденты, а также регулярно оценивает эффективность мер защиты.

В этой деятельности совет директоров опирается на пять ключевых принципов:

1. Кибербезопасность требует системного управления рисками на уровне предприятия.
2. Киберриски имеют конкретные юридические последствия.

3. Совет имеет доступ к экспертам по кибербезопасности и регулярно обсуждает с ними текущие и стратегические вопросы.
4. В компании необходимо иметь систему управления киберрисками с достаточным бюджетом и выделенным ответственным персоналом.
5. Обсуждение киберрисков должно включать экономические прогнозы возможных потерь и планы по их минимизации.

Часть стратегии кибербезопасности — план реагирования на киберинциденты, который должен предусматривать меры по восстановлению нормальной операционной деятельности, уведомление третьих сторон, а также взаимодействие с правоохранительными органами и внешними экспертами.

РОЛЬ И ОТВЕТСТВЕННОСТЬ HR-ОТДЕЛА

HR-отдел — ключевой элемент в реализации политики кибербезопасности, потому что половина всего ущерба из-за кибератак связана с ошибками сотрудников. HR должен способствовать созданию культуры безопасности, обучая сотрудников безопасным практикам офисной и удаленной работы, заботясь о своевременном информировании о новых киберугрозах, разрабатывая и внедряя процессы контроля подготовленности персонала в сфере кибербезопасности.

Среди мер, которые HR может принять ради повышения культуры кибербезопасности в компании, автор называет также разработку системы поощрений для сотрудников, информирующих о потенциальных уязвимостях и демонстрирующих ответственный подход к кибербезопасности. Кроме того, работа HR заключается в том, чтобы в случае увольнения сотрудника контролировать своевременную (в течение 24 часов) блокировку доступа к корпоративным данным и системам, чтобы минимизировать риски потери данных и ущерба репутации компании.

Отдельный интересный аспект работы HR — это поиск, наем и удержание специалистов по кибербезопасности, спрос на которых значительно превышает предложение. Для этого необходимо партнерство с университетами и разработка программ стажировок и привлечения новых талантов, предложение конкурентоспособной заработной платы и возможности карьерного роста.

РОЛЬ ЮРИДИЧЕСКОГО ОТДЕЛА

Юридический отдел отвечает за мониторинг законодательных изменений в сфере борьбы с киберугрозами, а также за соответствие компании нормативным требованиям, в том числе в сфере сбора, хранения персональных данных и управления ими.

Законодательные требования к обеспечению кибербезопасности могут меняться в зависимости от того, в каких юрисдикциях находятся партнеры, клиенты или поставщики компании. Юристы следят за тем, чтобы все процедуры компании соответствовали отраслевым и государственным стандартам (например, требованиям GDPR (General Data Protection Regulation) в США, общим правилам обработки персональных данных в странах Евросоюза и т. п.).

Также юридический отдел участвует в управлении киберинцидентами и в анализе выявленных атак и угроз, помогая руководству подразделений извлечь уроки и не допустить подобного в будущем.

СЛУЖБА КИБЕРБЕЗОПАСНОСТИ В СТРУКТУРЕ КОМПАНИИ

В наши дни уже очевидно, что задачи киберзащиты не может выполнять только ИТ-отдел, традиционные изолированные структуры управления кибербезопасностью устарели и требуют реформирования. Но вопрос о том, как именно должна быть организована функция кибербезопасности, каждый бизнес решает по-своему.

В крупных компаниях часто создают собственные центры киберзащиты (Security Operation Center, SOC), компании меньшего размера пользуются услугами подрядчиков для обеспечения кибербезопасности. Все чаще в компаниях появляется директор по информационной безопасности (CISO, Chief Information Security Officer), который отвечает за защиту критически важных данных и активов организации от кибератак и пользуется прямым доступом к высшему руководству и совету директоров с целью эффективного управления рисками.

По данным опроса, проведенного в 2020 году, можно сделать вывод, что большинство компаний понимает необходимость этого. Только 2 из 10 руководителей, отвечающих за кибербезопасность, состоят в ИТ-отделе, остальные 8 подчиняются непосредственно генеральному директору.
В 2019 году консалтинговая компания Deloitte провела исследование «О будущем кибербезопасности» и установила, что компании, внедрившие в бизнес-подразделения специалистов по кибербезопасности, успешнее тех, кто поручил киберзащиту ИТ-отделу.

В США созданием обновленных организационных моделей занимается ANSI (American National Standards Institute) — Американский национальный институт стандартов.

В 2008 году институт выпустил документ, в котором определены:

- технические требования к установлению и поддержанию безопасного соединения между двумя или более системами/компаниями;
- требования к обмену конфиденциальной информацией;
- обязанности каждой из сторон по обеспечению безопасности и целостности обмениваемой информации.

Этот стандарт предполагает назначение ответственного специалиста для управления кибербезопасностью и выделение бюджета на кибербезопасность.

Также в документе описаны семь ключевых шагов по управлению киберрисками:

1) определение ответственности руководителей подразделений за управление киберрисками. Руководящую роль обычно возлагают на финансового или исполнительного директора компании;
2) создание межфункциональной команды по управлению киберрисками, включающей представителей различных отделов;
3) проведение перспективной оценки рисков на уровне всей организации;
4) учет различий в регулировании кибербезопасности в разных юрисдикциях;
5) совместная подготовка отчетов для совета директоров, включая метрики, которые количественно оценивают влияние киберугроз на бизнес;
6) разработка общего корпоративного плана управления киберрисками и стратегии внутренних коммуникаций в случае киберинцидента;
7) выделение комплексного бюджета на киберриски, предусматривающего затраты на поиск, наем и стимулирование лояльности квалифицированных специалистов, обучение

сотрудников, обеспечение соответствия нормам законодательства и управление поставщиками.

Другая современная организационная модель сосредоточена на анализе внутренних процессов компании и получила название «Три линии защиты»:

1) первая линия — управление: отвечает за управление рисками, внедрение контрольных процедур и мониторинг уязвимостей;
2) вторая линия — риск-менеджмент: определяет политику безопасности, проверяет первую линию и оценивает уровень риска;
3) третья линия — внутренний аудит: обеспечивает независимую оценку эффективности управления рисками и контроля.

В ходе цифровой трансформации бизнеса все более распространенной становится модель Enterprise Architecture (EA), которая позволяет согласовать ИТ-инфраструктуру с бизнес-целями компании. В ее рамках описываются структура корпоративных информационных систем и четкие механизмы интеграции мер безопасности на всех уровнях — от проектирования приложений до управления доступом. Такой подход снижает вероятность уязвимостей, возникающих из-за несогласованности между подразделениями, и делает защиту данных проактивной, а не реактивной.

EA позволяет на этапе разработки бизнес-процессов учитывать требования к шифрованию данных, сегментации сетей или политике резервного копирования, обеспечивая непрерывность бизнеса даже в случае инцидентов.

Компании финансового сектора все чаще используют совместные модели работы, тесно увязывая кибербезопасность с другими направлениями управления рисками, например с выявлением мошенничества и противодействием отмыванию денег. Такой подход помогает выстроить более цельную и скоординированную систему защиты от финансовых угроз.

ВЗАИМОДЕЙСТВИЕ ИБ С ОСНОВНЫМ БИЗНЕСОМ

Рабочее взаимодействие специалистов по кибербезопасности с бизнес-подразделениями — один из важнейших аспектов в строительстве и поддержании работоспособности киберщиты компании. Специалисты по ИБ должны своевременно и доходчиво доносить до каждого сотрудника мысль о том, как важно соблюдение стандартов цифровой гигиены в их повседневной деятельности: при исполнении текущих операций, при найме и увольнении, заключении контрактов, поиске контрагентов и т. д.

При этом важно, чтобы специалисты по ИБ были заинтересованы в успехе бизнеса в целом, стремились максимально эффективно и удобно встроить необходимые меры киберзащиты в деятельность своих коллег. Интеллект, эмпатия и искреннее стремление к командной работе необходимы специалисту по кибербезопасности не меньше, чем сотрудникам клиентского сервиса.

ИБ ВО ВЗАИМОДЕЙСТВИИ С КОНТРАГЕНТАМИ И ПАРТНЕРАМИ

Поскольку киберугрозы постоянно меняются, их источником могут стать не только новые поставщики и партнеры, но и те, с которыми бизнес работает в течение многих лет. Чтобы минимизировать риски, в партнерские соглашения нужно включать требования по кибербезопасности и описание условий и правил информационного обмена.

СЛИЯНИЯ И ПОГЛОЩЕНИЯ

С ростом финансовых потерь от кибератак меняется подход к due diligence, который сегодня обязательно включает проверку состояния кибербезопасности.

За последние несколько лет в процессе или после крупных сделок по слиянию и поглощению (M&A) произошло множество громких инцидентов, связанных с кибербезопасностью. Эти инциденты вызвали обеспокоенность руководителей компаний, инвесторов и регулирующих органов.

В 2017 году в ходе сделки по поглощению крупная интернет-компания обнаружила три последовательных утечки данных в приобретаемой компании. Это привело к снижению цены покупки на 7%, что составило $350 млн. Кроме того, продавец гарантировал компенсировать 50% ущерба в случае повторов киберинцидентов.

Высокая динамика сделок по слиянию и поглощению может затруднить выявление рисков. Инвестиционные банки часто проводят аукционы, чтобы стимулировать конкуренцию между заинтересованными участниками торгов. В условиях жестких временных ограничений бизнесмены, принимающие решения, как правило, оценивают стратегические, финансовые, юридические или операционные вопросы, но оставляют без внимания киберриски.

Своевременное выявление киберугроз позволяет не только получить более точную финансовую оценку (включая как разовые, так и регулярные расходы на устранение пробелов), но и демонстрирует заинтересованным сторонам, что компания действует проактивно. Это особенно важно при отчетности перед советом директоров, акционерами или регуляторами: качественно проведенная оценка киберрисков сегодня рассматривается как элемент ответственного управления активами.

Даже если обнаруженные уязвимости не приводят к отмене сделки, инвестор или покупатель, как правило, настаивает на четком понимании масштабов унаследованных проблем. Он может потребовать пересмотра условий сделки, например учесть необходимые затраты на устранение уязвимостей, оформление страхового покрытия или использование механизмов возврата средств в случае инцидента.

Автор советует компаниям-покупателям уже на стадии подготовки к интеграции разработать четкий план устранения несоответствий нормативным требованиям, снижения потенциальных угроз и при необходимости — объединения процессов обеспечения информационной безопасности.

Автор настаивает, что при подготовке сделок M&A вопросами кибербезопасности должны заниматься обе стороны процесса. Речь идет не только о проверке киберугроз, связанных с интеграцией информационных систем компаний, но и о том, что во время сделки, освещаемой прессой и деловым сообществом, риск кибератаки всегда возрастает.

10 ЛУЧШИХ МЫСЛЕЙ

1.
Кибербезопасность — стратегическая и повседневная задача для всей компании, которая требует комплексного подхода и участия всех сотрудников — от рядовых до руководителей.

2.
Киберриски усиливаются в периоды цифровой перестройки бизнеса, внедрения новых технологий и перевода сотрудников на удаленный режим.

3.
Недооценка значимости киберзащиты приводит к недостатку финансирования и небрежному отношению к стратегии и тактике ИБ в компании.

4.
Киберриски и меры защиты от них нужно оценивать в деньгах, чтобы принимать взвешенные управленческие решения.

5.
Киберзащитой должны заниматься специалисты. Компании, которые поручают эти задачи ИТ-отделу, менее успешны на рынке.

6.
Процедуры и стандарты кибербезопасности требуют регулярной настройки, чтобы быть эффективными против актуальных угроз.

7.
Руководители балансируют между необходимостью защитить бизнес от киберугроз и сохранить рентабельность.

8.
Половина кибератак случается из-за ошибок сотрудников. Поэтому важно регулярно обучать персонал, а также тщательно продумывать процедуры найма и увольнения.

9.

Требования к кибербезопасности нужно включать в контракты с поставщиками и партнерами.

10.

Компании необходимо иметь стратегию киберзащиты, а также план действий на случай кибератаки, выделенных ответственных и бюджет на ИБ.