Киберпреемственность

Компаниям все чаще приходится иметь дело с угрозами кибербезопасности и проблемами регулирования защиты данных, включая вопросы управления ИИ и большими языковыми моделями (такими, как ChatGPT), а также возможности взломов и кибершпионажа. Но ответственные лица (как правило, директора по информационной безопасности), которые назначаются во многих компаниях для решения подобных задач, зачастую не оставляют после себя преемников

Оригинальный текст на сайте CNBC.com

Текст
АНАТОЛИЙ ВЕЧКАНОВ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**



Примерно 41% компаний не имеют плана преемственности для директора по информационной безопасности, согласно данным рекрутинговой компании Heidrick & Struggles. По ее информации, примерно три четверти директоров по информационной безопасности сообщили, что готовы перейти в другую компанию в ближайшие три года, и это подчеркивает важность плана преемственности и retention-стратегий.

«Отсутствие плана преемственности для директора по информационной безопасности мы считаем существенным риском, который компании, впрочем, могут легко снизить, — сообщил **Мэтт Аиелло**, партнер и руководитель подразделения глобальной кибербезопасности компании Heidrick & Struggles. — Результаты исследований вызывают беспокойство, если учесть, насколько важно киберлидерство в современной бизнес-среде».

Риски в связи с отсутствием плана преемственности

Исследование также показало, что, если у организации имеется план преемственности, то, как правило, он включает в себя лишь одного сотрудника, который к тому же недостаточно квалифицирован, добавил Мэтт Аиелло. Это происходит потому, что директора по информационной безопасности обычно нанимают «игроков одной позиции», таких как специалисты по ИБ, безопасности приложений и комплаенсу, но не будущих руководителей.

Организации, у которых нет плана преемственности, подвергают бизнес чрезмерным рискам, поскольку ландшафт угроз и регуляторная среда стремительно меняются. В случае если позиция директора по информационной безопасности по какой-то причине станет вакантной, последствия для бизнеса могут быть серьезными.

Кроме того, директора по информационной безопасности сложно заместить. Существуют ограничения при подготовке внутренних кандидатов в необходимых областях в связи с их повседневной работой. Следовательно, организациям проще найти нового директора по информационной безопасности среди внешних кандидатов. Однако и этот процесс отнимает время, деньги и силы, ведь кадровый потенциал ограничен.

Без четкого плана преемственности для руководителей по кибербезопасности организации становятся уязвимыми для серьезных кибератак и неподготовленными к работе в условиях их возможных последствий. Темп развития маркетплейсов и технологий столь стремителен, что руководству компаний следует относиться к преемственности директора по информационной безопасности так же серьезно, как и к преемственности генерального директора.



«В случае ухода директора по информационной безопасности в организации возникает недостаток ценных институциональных знаний, что может препятствовать адаптации к быстро меняющимся киберугрозам», — сообщил **Дэниэл Соо,** главный консультант по рискам и финансам в отделе кибер- и стратегических рисков консалтинговой компании Deloitte.

Отсутствие преемника может прервать деятельность операций по кибербезопасности, привести к задержкам и пропускам мероприятий по управлению киберрисками, а также затруднить реагирование на киберинциденты и принятие решений по ним.

Кроме того, план преемственности директора по информационной безопасности — это способ обеспечить наличие в организации нужного человека в нужное время, чтобы достигать киберцели компании. Отсутствие корректного планирования преемственности может привести к сбою в работе всей организации. К примеру, это может ухудшить ресурсный потенциал компании, снизить уверенность персонала, способствовать деградации организационной культуры и увеличению временны́х затрат на достижение стратегических целей.

Как подготовить список потенциальных преемников

«Организациям необходимо начать планирование преемственности, как только назначен новый директор по информационной безопасности. В планировании должны принимать участие руководители и совет директоров организации. Это позволит провести тщательный анализ приоритетов и рисков и поможет заложить основы для подготовки преемника в различных сферах, включая кадровую», — отметил Дэниэл Соо.

При планировании также нужно предусмотреть будущие требования по безопасности с учетом тенденций изменений в бизнесе и технологическом ландшафте. Директору по информационной безопасности следует анализировать аспекты безопасности в нововведениях и разрабатывать политики, технологии и методики, чтобы удовлетворить будущие потребности. Внедрение программы подготовки поможет обучить сотрудников навыкам решения предстоящих задач повышения информационной безопасности.

Как показало исследование компании Heidrick & Struggles, большинство директоров по информационной безопасности считают, что через пять лет киберриски будут серьезно отличаться от сегодняшних. Это означает, что идеальный преемник должен быть выбран с учетом того, с чем руководителю по информационной безопасности придется иметь дело в будущем, а не сейчас, уточнил Мэтт Аиелло. Комитет по отбору также должен проводить due diligence и анализировать кадровый потенциал как внутри, так и вне организации.

Важная часть любого плана преемственности — подготовка списка потенциальных преемников с целью уберечь компанию от рисков в ближайшей и долгосрочной перспективе. Иначе говоря, подготовка нужна для многих преемников заранее. Для этого требуется ответственный подход к налаживанию процессов преемственности на регулярной основе, включая постоянное развитие киберштата внутри организации.

Помимо этого компаниям следует вести документацию с ключевыми обязанностями и заданиями по каждой функции директора по информационной безопасности. Это поможет продумать текущие и будущие обязанности сотрудника на этой позиции. Б.О