Varonis назвала тренды кибербезопасности в 2021 году

Тематика: **IT и телекоммуникации**
Статьи и исследования

г. Москва

Дата публикации: 12.01.2021

Дата мероприятия / события: 12.01.2021

Эксперты Varonis в России спрогнозировали пять основных трендов в области кибербезопасности, которые будут определять развитие российского ИБ-рынка в наступившем 2021 году. По мнению специалистов компании, ключевые перемены в отрасли будут обусловлены переходом на гибридные графики, сочетающие удаленную и офисную работу, ограниченностью бюджетов бизнеса, а также ростом активности злоумышленников в условиях изменения ИТ-ландшафтов компаний.

1. Переосмысление подходов к ИБ при гибридном формате работы
Информационные периметры компаний станут еще более размытыми: теперь в них необходимо включать все устройства, на которых работают сотрудники. Повсеместный переход на удаленную работу приведет к тому, что периметры организаций изменятся. Усиливается фактор географической распределенности рабочих мест: в том числе из-за того, что компании в условиях удаленной работы стали чаще нанимать сотрудников из других регионов. Децентрализация инфраструктуры, перевод ресурсов в облака и использование средств коллаборации сотрудников также приводит к необходимости существенно менять парадигму системы информационной безопасности.

Для директора по информационной безопасности это означает необходимость защищать не только инфраструктуру, развернутую на площадках компании и в облаках, но и информационные системы, находящиеся в распоряжении сотрудников у них дома. Для этого важно четко понимать, какие именно данные хранятся на личных устройствах, и какие риски возникают из-за этого.

«Удаленная работа очень сильно отличается как с точки зрения построения бизнес-процессов, так и с точки зрения защиты данных. Когда сотрудник не находится в офисе, никто достоверно не знает, в каких условиях он сейчас работает, кто еще видит информацию на его экране. Нельзя даже наверняка сказать, кто на самом деле работает с данными компании: сам сотрудник или злоумышленник, перехвативший данные учетной записи. Это создает дополнительные риски и необходимость внедрения новых инструментов защиты», — рассказывает **глава Varonis в России Даниэль Гутман.**

2. Увеличение доли ИБ в ИТ-бюджетах российского бизнеса
Сложная экономическая ситуация приводит к двум последствиям. С одной стороны, она подстегивает рост активности киберпреступников. С другой, ограничивает возможности роста ИТ-бюджетов бизнеса. Инвестиции в информационную безопасность традиционно оцениваются

как процент от ИТ-бюджетов компаний. В ситуации, когда бюджеты компаний на технологии в среднем не растут (а у многих компаний сокращаются), вероятно временное перераспределение бюджетов в пользу инструментов безопасности — в первую очередь, за счет сокращения расходов на развитие ИТ-инфраструктур.

Кроме того, во многих компаниях произойдет и перераспределение бюджетов ИБ. Возникновение свежих угроз приводит к необходимости строить новые модели безопасности, оценивать риски, расследовать инциденты, поэтому часть бюджетов будет перераспределяться в пользу консалтинговых услуг.

3. Использование поведенческого анализа для защиты данных
Среди специалистов по информационной безопасности уже сложилось понимание того, что не может быть единого решения, которое защищало бы компанию от всех угроз. Надежная система безопасности имеет модульную структуру и состоит из набора интегрированных друг с другом решений. Средства периметральной и межсетевой защиты, безопасность веб-приложений (WAF) и инструменты предотвращения утечек данных (DLP) становятся обязательными для любых крупных компаний.

Помимо этого, аналитики прогнозируют рост продаж систем в категориях Managed security services (MSS), SOC и SIEM. По мнению экспертов Varonis, во всех этих решениях будет расти роль инструментов поведенческого анализа. Эта тенденция связана с необходимостью распознавать нетипичное поведение и аномальную активность учетных записей в условиях удаленной работы.

4. Развитие инструментов автоматизации
Повышенная активность злоумышленников и ограниченность ресурсов приводят к тому, что растет потребность в технологиях, позволяющих автоматизировать работу ИБ-департаментов. Например, к таким инструментам относятся средства для автоматизированной классификации данных по уровню их конфиденциальности.
Серьезное развитие в 2021 году получат и средства корреляции, позволяющие правильно находить взаимосвязь между событиями и обращать внимание ИБ-департамента только на действительно опасные события. Такие системы помогут, с одной стороны, избавить сотрудников от необходимости проверять огромное количество уведомлений, а с другой — не пропустить действительно важные оповещения, свидетельствующие о потенциальных атаках.

5. ИБ-специалисты будут развивать аналитические навыки
Требования к специалистам по кибербезопасности существенно меняются. ИБ-директорам и их подчиненным становится недостаточно технических данных, и требуется все больше навыков аналитика. Для построения и развития жизнеспособной системы кибербезопасности нужно постоянно анализировать бизнес-процессы и понимать их «узкие места».

Успешный CISO должен не только знать теоретическую базу, но и понимать состав данных в организации, места их хранения, уровень конфиденциальности и конкретные риски для каждой категории данных. Сотрудникам департаментов ИБ требуется новый комбинированный набор из технических и аналитических навыков, что в свою очередь изменит образовательные программы подготовки специалистов по кибербезопасности.

О компании Varonis
Varonis Systems – разработчик программных решений для защиты от комплексных кибератак, основанных на поведенческом анализе пользователей и защите данных компании. Компания была основана в 2005 году, став пионером в области управления и контроля неструктурированных данных. По разным источникам, Varonis занимает более 70% мирового рынка в этой области.

Среди разработок Varonis решение по аудиту периметра сети и поведенческому анализу, которое помогает заказчикам вовремя выявлять продвинутые кибератаки и защищаться от них. Сегодня у компании более 6000 заказчиков во всем мире.