Ростелеком
Солар

Тренды страхования киберрисков на российском рынке

Москва 2022
rt-solar.ru

ОГЛАВЛЕНИЕ

О компании

«РТК-Солар» – национальный провайдер сервисов и технологий кибербезопасности. Под защитой – 750+ компаний и госструктур. Ключевые направления – аутсорсинг ИБ, разработка собственных продуктов, интеграционные ИБ-проекты. Компания предлагает сервисы первого и лидирующего в РФ коммерческого SOC (Security Operations Center) – Solar JSOC, а также экосистему управляемых сервисов ИБ – Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, IdM-систему Solar inRights и анализатор кода Solar appScreener. Предоставляются compliance-услуги, в том числе по защите АСУ ТП. Штат компании – 1600+ специалистов. Офисы компании расположены в Москве, Нижнем Новгороде, Самаре, Ростове-на-Дону, Хабаровске, Томске, Санкт-Петербурге, Ижевске. Деятельность компании лицензирована ФСБ России, ФСТЭК России и Министерством обороны России.

Список сервисов Solar JSOC:

- Мониторинг и анализ инцидентов ИБ
- Эксплуатация систем ИБ и реагирование на атаки
- Анализ угроз и внешней обстановки
- Комплексный контроль защищенности
- Реагирование на инциденты и техническое расследование
- Построение SOC или его частных процессов (в том числе центров ГосСОПКА)

Введение

На рынке ИБ все чаще встречается услуга киберстрахование, или страхование киберрисков. Первые общедоступные предложения появились в России в 2017 году, а уже в 2020 эксперты зафиксировали 5-кратное увеличение спроса на услугу. В 2021 году тенденция сохранилась, и спрос вырос еще на 60%. На такой всплеск во многом повлияла пандемия, вынудившая бизнес уйти в онлайн и перевести сотрудников на удалённую работу. Одновременно с этим увеличилась и активность хакеров. На этом фоне стало очевидно, что с кибератакой и её последствиями теперь может столкнуться абсолютно любая компания независимо от отрасли и масштаба. И, как следствие, спрос на киберстраховку начал расти. В данном отчете отражено отношение организаций, представляющих разные отрасли, к услуге страхования киберрисков.

Отчет составлен на основе опроса, проведённого экспертами компании «РТК-Солар» в первой половине 2022 года.

Всего было проведено около 400 онлайн-интервью. В число респондентов вошли как коммерческие организации (60%), так и предприятия государственного сектора (40%), включая федеральные и региональные органы власти. В опросе приняли участие представители различных сегментов бизнеса (B2G, B2E, B2B,SMB) и отраслей (нефтегаз, металлургия и горнодобывающая промышленность, финансы, транспорт, ретейл и ТЭК).

Ключевые тезисы

6% респондентов уже пользуются услугой страхования киберрисков, а **21%** планирует воспользоваться услугой в будущем;

2/3 из тех, кто уже страхует риски, – это представители ИТ и финансовой отрасли;

Респонденты считают, что киберстраховка сделает компанию более привлекательной для инвесторов, повысит уровень ее защищенности и поможет быстрее восстановиться после инцидента;

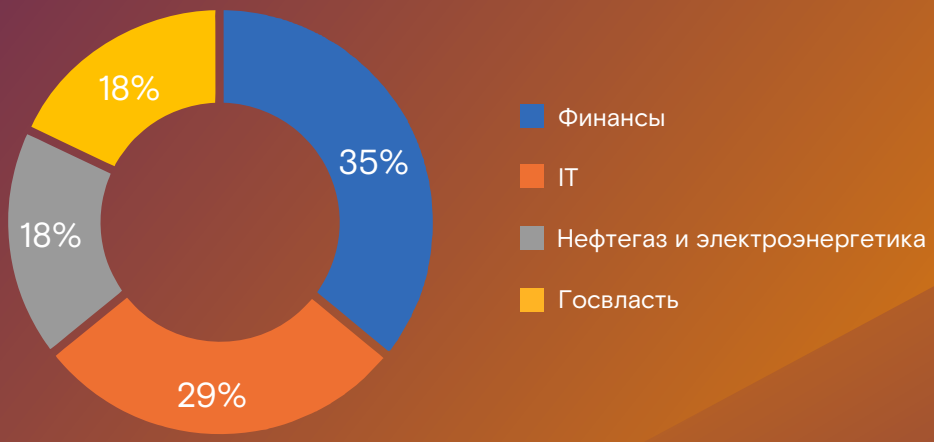
Для **33%** основной барьер для внедрения киберстраховки – отсутствие бюджета;

1/3 респондентов готовы к подорожанию услуг ИБ за счет страховки на **10%**.

Кто уже страхует киберриски?

Доля компаний, которые уже пользуются услугой страхования киберрисков, пока не велика: всего 6%. При этом почти 2/3 из них - это представители финансовой отрасли и ИТ, что неудивительно: ведь это две наиболее цифровизированные отрасли. Кроме того, такие компании, как правило, имеют достаточные бюджеты, чтобы направить их не только на развитие непосредственно самой системы ИБ, но и на обеспечение ее финансовой защиты в формате страхования киберрисков. При этом в традиционно консервативных отраслях экономики есть потребители этой услуги. Так 16% респондентов, страхующих киберриски, приходится на нефтегазовую и электроэнергетическую промышленность, а также на органы госвласти.

Кто уже использует услугу



Страхуют киберриски, как правило, крупные корпорации и организации, обладающие значительными бюджетами и распределённой ИТ-инфраструктурой. Для них вывод из строя даже отдельных сегментов сети может привести к остановке бизнес-процессов, на восстановление которых требуется много времени. Страховая выплата в этом случае поможет закрыть часть убытков и компенсировать простой.

- **38%** работающих с услугой компаний отметили, что страхование позволило им быстрее восстановиться после киберинцидента;

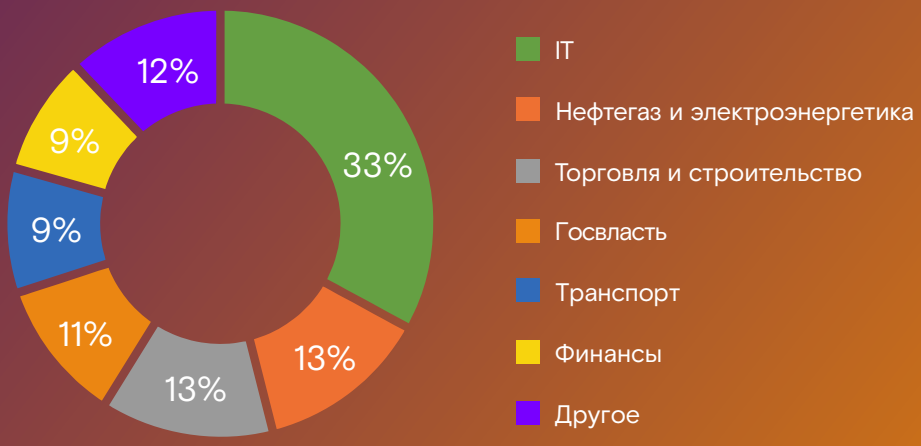
- Более **60%** респондентов внедрили этот инструмент для повышения уровня защищенности компании;

- **2/3** считают, что их компания стала гораздо привлекательнее (для клиентов, партнёров, сотрудников) после внедрения киберстрахования.

Кто планирует внедрить услугу?

Доля тех, кто планирует внедрить услугу в ближайшей перспективе, не так уж и мала – 21%. Но здесь распределение несколько иное и лидирующую позицию занимают ИТ-компании (33% респондентов), а представители финансовой отрасли, напротив, несколько отстают (лишь 9% из них собираются работать со страхованием киберрисков в будущем).

Кто планирует внедрить киберстраховку



Среди них 63% считают, что страхование киберрисков поможет повысить уровень защищенности компании. А более трети респондентов рассматривают услугу как способ быстрее оправиться после инцидента. Вместе с тем 42% респондентов полагают, что услуга будет способствовать возврату инвестиций в ИБ.

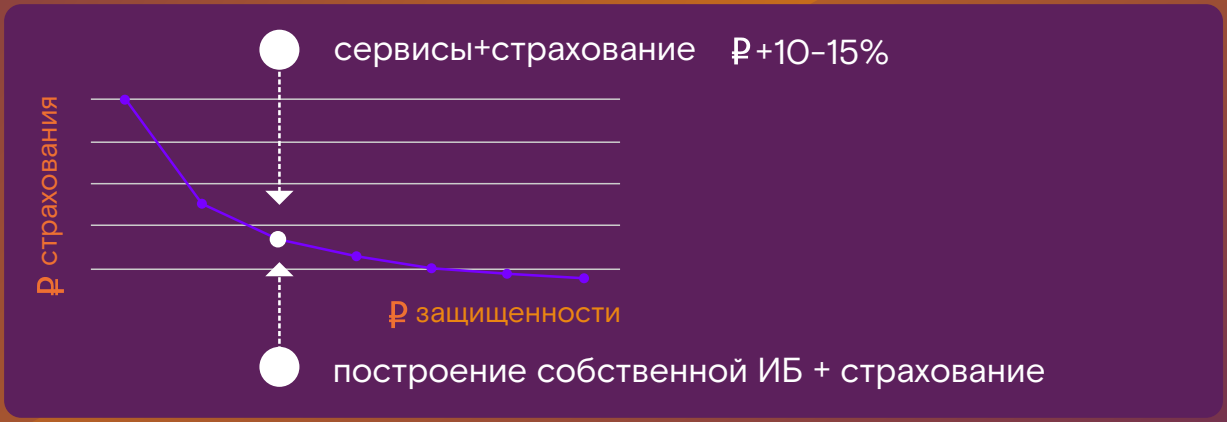
Цена и другие преграды

Полученные результаты говорят о том, что и коммерческие, и государственные организации понимают, что в современных условиях потери от кибератак фактически становятся постоянной статьей расходов. Но, к большому сожалению, по причине своей дороговизны данная услуга пока доступна лишь ограниченному кругу компаний: 33% организаций указали этот фактор в качестве основного барьера для приобретения услуги.

Здесь хотелось бы обратить внимание на важность соотношения вложений непосредственно в саму защиту и в страховку - соблюдение так называемого Security Insurance Balance. Очевидно, что делать бесконечные инвестиции в ИБ, доводя это чуть ли не до абсурда, контрпродуктивно. В то же время нельзя полагаться исключительно на страховые выплаты в надежде, что они помогут компенсировать все последствия атаки.

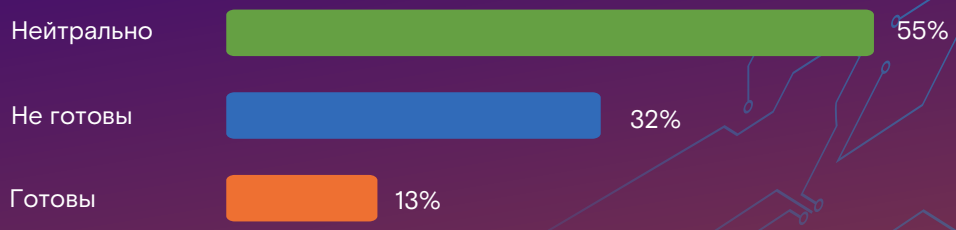
Именно поэтому, на наш взгляд, оптимальным решением здесь может стать формрование комплексного предложения «ИБ+страхование» в режиме одного окна. Если речь идет о сервисной модели ИБ, то такое комплексное предложение может стоить на 10-15% дороже изначальной стоимости ИБ-услуг, - так считают большинство опрошенных. Компания также может строить ИБ по модели in-house, и тогда она сама обращается в страховую организацию - и здесь сложно рассчитать примерную стоимость услуги, так как каждое предложение индивидуально.

Оптимизация расходов отражена на графике:



Вместе с тем на текущий момент не так много организаций (всего 13%) готовы сменить своего ИБ-провайдера на нового, предлагающего, помимо прочего, услугу киберстрахования.

Готовность сменить ИБ-провайдера на нового с услугой киберстраховки



Что влияет на выбор нового сервис-провайдера

Примечательно, что здесь наибольшую готовность демонстрируют компании среднего и малого бизнеса (SMB), а также некрупные представители B2B. В целом SMB на общем фоне проявляет наибольший интерес к услуге киберстрахования:

- **23%** компаний сегмента планируют внедрить данный продукт;
- **16%** готовы сменить ИБ-провайдера при наличии комплексного предложения «ИБ+страхование»;
- Более **55%** рассматривают киберстрахование как финансовый инструмент ИБ.

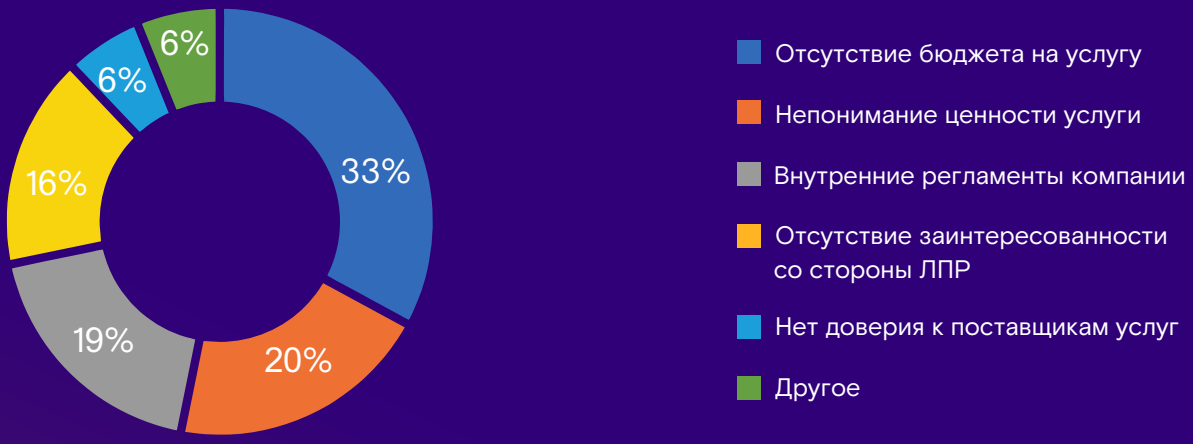
Такие результаты вполне объяснимы. Для представителей среднего и малого бизнеса даже простая атака со стороны низкоквалифицированных злоумышленников может привести к серьезным последствиям вплоть до банкротства. При этом содержание в штате опытного ИБ-специалиста может быть сопоставимо или даже превышать размер ежегодной страховой премии. Также у небольших компаний менее разветвленная ИТ-инфраструктура, и смена сервис-провайдера для них менее сложный и ресурсозатратный процесс, чем, например для крупных корпораций.

Также от приобретения киберстраховки большинство компаний останавливает тот факт, что задача не находится у них в приоритете. Это вполне объяснимо. Для начала им надо выстроить комплексную систему ИБ, что связано с выбором провайдера и набора необходимых услуг и сервисов, их дальнейшей настройкой и наращиванием при необходимости системы защиты. И тогда страхование киберрисков, в частности остаточных, станет своего рода финальным штрихом, направленным на повышение общей защищенности компании и ее ИТ-инфраструктуры. А «дырявую» инфраструктуру вряд ли кто-то согласится застраховать, или же стоимость полиса будет неоправданно высокой.

Поэтому в первую очередь мы говорим именно о страховании остаточных рисков, то есть тех, закрытие которых становится экономически нецелесообразным. Это и есть тот самый Security Insurance Balance. В таком варианте киберстрахование станет доступным не только для крупных компаний, но и для представителей SMB и банков с базовой лицензией (ББЛ). Последние, будучи представителями финансовой отрасли и вынужденные следовать требованиям регулятора, весьма заинтересованы в подобной услуге.

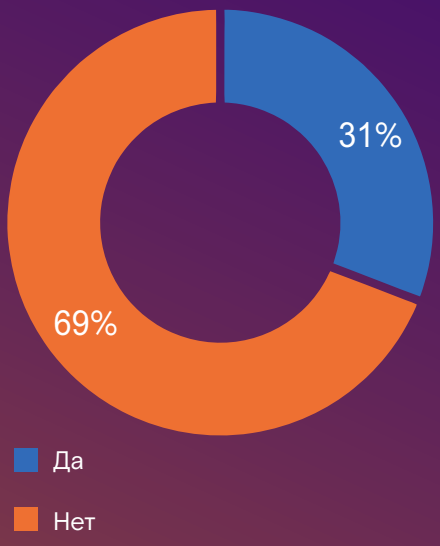
Очевидно, что на это накладывается также и сложность регламентирования страховых рисков. Особенно это касается длительных инцидентов, когда сложно зафиксировать время и дату начала атаки и доказать ее связь с возникшим ущербом.

Барьеры для внедрения киберстрахования

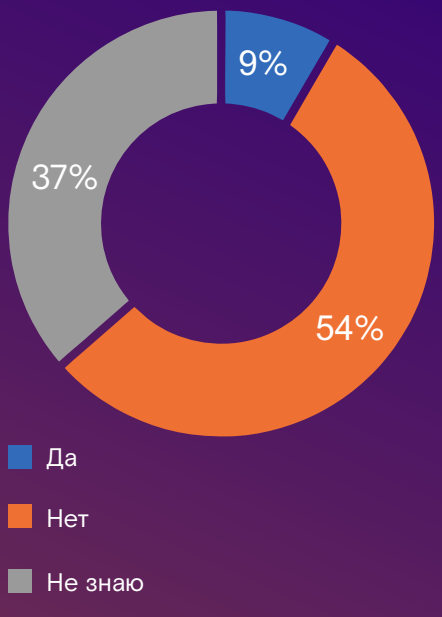


В связи с тем, что продукт относительно новый, в настоящее время на рынке не так много готовых и «обкатанных» решений. Отсюда и определённый скептис со стороны потенциальных потребителей. По этой же причине не все понимают пользу, которую киберстрахование может принести, и рассматривают его лишь как пустую трату денег и неокупаемые вложения.

Готовность заложить в бюджет на ИБ услуги киберстрахования



Были ли негативные последствия из-за отсутствия киберстраховки



И здесь стоит отметить, что 9% компаний, опрошенных нами, столкнулись с той ситуацией, когда пожалели, что на момент наступления киберинцидента у них не был оформлен киберполис, благодаря которому они могли бы восстановиться гораздо быстрее.

Выводы

Как видно, интерес к услугам страхования киберрисков со стороны бизнеса есть. Как мы уже отметили, в компаниях различных уровня и сферы деятельности формируется понимание необходимости не только существенного увеличения бюджетирования ИБ, но и проработки дополнительных мер защиты, одной из которых является страхование киберрисков.

Очевидно, для того чтобы занять прочную нишу на российском рынке ИБ, услуге требуется какое-то время, в результате чего постепенно появятся новые и более доступные предложения, включая комплексные услуги. Особенно это актуально в эпоху современности, когда все уже практически привыкли к формату одного окна, позволяющему получить все требуемые услуги и продукты в одном месте.

При этом компаниям стоит осознавать, что один только полис не защитит от кибератаки. И прежде чем идти в страховую организацию, нужно «довести до ума» свою ИБ-защиту. Только в таком варианте это будет разумный и эффективный шаг, а страховая выплата сможет действительно компенсировать часть потерь и быстрое восстановление после инцидента.

Ростелеком
Солар

rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70