

Сумма выручки			
География	Последний полный год (фактический)	Текущий год (оценочно)	Следующий год (оценочно)
Великобритания / Европа			
США / Канада			
Россия			
Другие страны мира			

10. Является ли Компания некоммерческой организацией? / Is the Company a non-profit organization **Да / Yes** **Нет / No**
 Если «да», то, пожалуйста, уточните: планирует ли Компания использовать для оплаты приобретаемого покрытия денежные средства и (или) иное имущество, полученные некоммерческой организацией от иностранных государств, международных и иностранных организаций, иностранных граждан и лиц без гражданства? / If "yes" please specify does the Company plan to pay insurance premium for the purchased cover by cash and (or) other property initially received by a non-profit organization from foreign states, international and foreign organizations, foreign citizens and stateless persons
Да / Yes **Нет / No**
11. Является ли Компания стратегическим предприятием или акционерным обществом, определенным Указом Президента Российской Федерации от 4 августа 2004 года № 1009 «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ»? / Is the Company a strategic enterprise or a joint stock company defined by the Decree of the President of the Russian Federation of August 4, 2004 No. 1009 "On approval of the List of strategic enterprises and strategic joint stock companies"
Да / Yes **Нет / No**
12. Имеет ли Компания отношение к товарам двойного назначения, определенным Указом Президента Российской Федерации от 17 декабря 2011 года № 1661 «Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль»? / Does the Company have reference to dual-use goods defined by the Decree of the President of the Russian Federation of December 17, 2011 No. 1661 "On approval of the List of goods and technologies of dual use which may be used for creation of armaments and military equipment and in relation to which the export control is implemented".
Да / Yes **Нет / No**

В. ПОДВЕРЖЕННОСТЬ ДАННЫХ РИСКАМ

1. Укажите количество обрабатываемых или хранящихся записей данных по следующим категориям:

	Великобритания / Европа		США / Канада		Другие страны мира	
	Обработано	Хранится	Обработано	Хранится	Обработано	Хранится
Базовая личная информация						
Конфиденциальная личная информация						
Информация о платежной карте						
Информация о финансовом счете						
Информация, связанная со здоровьем						
Личные данные сотрудников						
Корпоративная информация третьих сторон						

2. Доводится ли информация о заказчике / клиенте третьим сторонам? **Да** **Нет**

Если «Да»:

- а. С кем осуществляется обмен данными и с какой целью?

- b. Возмещается ли ущерб в результате нарушения данных такими третьими сторонами? Да Нет
- c. Всегда ли данные анонимизируются / агрегируются до передачи? Да Нет
- d. Если данные не анонимизируются, всегда ли запрашивается разрешение у субъекта данных до их передачи?
Да Нет
3. Существует ли гарантия, что данные не передавались на какую-либо территорию, за исключением случаев, когда такая территория имеет адекватный уровень защиты прав и свобод субъектов данных в связи с обработкой личных данных?
Да Нет

С. ПОДВЕРЖЕННОСТЬ РИСКАМ ПРЕРЫВАНИЯ СЕТИ

Раздел должен быть заполнен только в том случае, если автор предложения намеревается приобрести покрытие риска прерывания сети

1. Пожалуйста, предоставьте разбивку ваших доходов / потоков доходов:
- a. Онлайн продажи %
- b. Офлайн продажи %
- c. Брокерское вознаграждение/комиссионные %
- d. Плата за единицу / использование %
- e. Контракт / подписка / лицензионные сборы %
- f. Оплата услуг специалистов / услуг %
- g. Кредитование / аренда / лизинг %
- h. Инвестиционный доход %
- i. Пожертвования %
- j. Гранты %
- k. Прочее (пожалуйста укажите) %
2. Каким образом скажется на доходах / прибыли нарушение или сбой вашей компьютерной системы, сети или приложений (пожалуйста, укажите оценку упущенного дохода, ответственности перед третьими сторонами и оттока клиентов)?
3. Просьба сообщить о любых сезонных пиках доходов, включая соответствующее процентное увеличение:
4. Пожалуйста, укажите время, по истечении которого нарушение может привести к сокращению чистой прибыли:
5. Пожалуйста, опишите действия, предпринятые для предотвращения перебоев в работе, включая использование резервных систем питания, отказоустойчивую архитектуру, избыточную пропускную способность для множественных поставщиков и т.д.:

6. Пожалуйста, опишите действия, которые были бы предприняты для сокращения продолжительности такого перебоя, если бы он произошел, включая подробные сведения о любых операционных и системных мерах по переключению на резервный ресурс:
7. Просьба описать действия, которые были бы предприняты, в том числе возможные затраты, связанные с такими действиями, для смягчения последствий существенного перерыва в работе.
 Примерами таких расходов могут быть дополнительные кадровые / сверхурочные расходы, открытие дополнительных контактных центров или перемещение ИТ-оборудования / серверов / центров обработки данных или выплата компенсационных выплат клиентам:
8. Имеются ли официальные планы обеспечения непрерывности бизнеса и восстановления после аварийных ситуаций?
 Да Нет
- Если "Да":
- a. Каковы целевые сроки восстановления системы?
- b. Как часто такие планы тестируются?
9. Имеется ли формальная политика управления изменениями, включающая оценку рисков, тестирование, авторизацию, процедуры контроля изменений и процедуры отката для основных систем?
 Да Нет
10. Имеется ли процесс управления жизненным циклом для оценки и замены системы / сетевого оборудования?
 Да Нет

D. ПОДВЕРЖЕННОСТЬ РИСКАМ, СВЯЗАННЫМ С ИСПОЛЬЗОВАНИЕМ ВНЕШНИХ ПОСТАВЩИКОВ

Раздел должен быть заполнен только в том случае, если автор предложения предоставляет услуги ИТ/передачи данных третьим сторонам

1. Укажите пожалуйста все услуги ИТ и услуги, связанные с данными, которые передаются на внешний подряд третьим сторонам, включая поставщиков облачных технологий (при необходимости используйте отдельный лист):

Услуга	Наименование поставщика:	Услуга по требованию (включая модели инфраструктуры и модели платформы или программного обеспечения как услуги)
		Да Нет
		Да Нет
		Да Нет

Услуга	Наименование поставщика:	Услуга по требованию (включая модели инфраструктуры и модели платформы или программного обеспечения как услуги)
		Да Нет
		Да Нет
		Да Нет
		Да Нет
		Да Нет

2. Какие меры должной осмотрительности принимаются до взаимодействия с новым внешним поставщиком услуг (OSP)?

3. Имеется ли процесс регулярного аудита безопасности OSP? Да Нет

4. Где сторонние поставщики обрабатывают или хранят данные, как оцениваются риски, связанные с общей инфраструктурой, например облаками или общими серверами, и как организация управляет ими?

5. Хранятся ли данные о всех услугах по требованию в частном облаке?
 Да Нет
 Если «Нет», то в какой степени используются общедоступные облака и как контролируется доступ к данным?

6. Если происходит нарушение данных, какая сторона несет расходы по уведомлению и какова обязанность OSP в этой ситуации?

7. Если система OSP или облачная услуга недоступна, каково их вероятное влияние на ваш бизнес?

8. Какие договорные возмещения действуют в случае нарушения данных или недоступности сети, причиненных OSP или поставщиком облачных услуг/пострадавшего от них?

9. Каким образом планы обеспечения непрерывности бизнеса и/или аварийного восстановления направлены на предотвращение нарушений OSP или облака?

Е. БЕЗОПАСНОСТЬ ДАННЫХ

1. Имеется ли директор по вопросам конфиденциальности и безопасности данных?

Да Нет

Если «Нет», пожалуйста, объясните, как эта функция отслеживается и контролируется в вашей организации и кто несет ответственность:

2. Имеется ли политика конфиденциальности и безопасности данных в масштабах всей группы?

Да Нет

Если «Да», то соблюдается ли она?

Да Нет

3. Имеется ли политика установления степени конфиденциальности данных с адекватным уровнем безопасности ?

Да Нет

4. Настроена ли сеть таким образом, чтобы доступ к конфиденциальным данным был ограничен надлежащим образом авторизованными запросами, а привилегии регулярно проверялись?

Да Нет

5. Отслеживается ли в сети доступ к конфиденциальной информации? Да Нет

6. Хранится ли вся деликатная и конфиденциальная информация в ваших базах данных / серверах и файлах данных в зашифрованном виде?

Да Нет

Если «Нет», то пожалуйста, опишите меры безопасности (т.е. средства контроля доступа), применяемые для защиты этой информации:

7. Шифруется ли деликатная / конфиденциальная информация при передаче? Да Нет

8. Производится ли резервное копирование всех критически важных данных по крайней мере раз в неделю? Да Нет

9. Хранятся ли в организации собственные резервные плёнки / кассеты / диски и т.д.? Да Нет

Если «Да», то хранятся ли они в физически защищенном месте? Да Нет

10. Пожалуйста, укажите, соблюдаются ли следующие требования:

	Соблюдаются?				Если «Нет», просьба представить подробную информацию:
	Да	Нет	Нет данных		
Стандарты безопасности данных индустрии платежных карт					
Выберите версию		2.0	3.0		
Выберите уровень		1	2	3 4	
Закон о справедливых и точных кредитных сделках (FACTA)	Да	Нет	Нет данных		
Закон об ответственности и переносе данных о страховании здоровья граждан (HIPAA)	Да	Нет	Нет данных		

	Соблюдаются?			Если «Нет», просьба представить подробную информацию:
	Да	Нет	Нет данных	
Закон об информационной технологии здравоохранения для экономического и клинического здоровья (HITECH)	Да	Нет	Нет данных	
Закон Грамм-Лич Блайли (1999 год)	Да	Нет	Нет данных	
Другое (пожалуйста, укажите)	Да	Нет	Нет данных	

11. Пожалуйста, опишите вашу политику хранения и уничтожения данных:

12. Имеются ли процедуры отзыва учетных записей пользователей после увольнения сотрудников? Да Нет

F. СЕТЕВАЯ БЕЗОПАСНОСТЬ

1. Используется ли следующее (пожалуйста, выберите все, что применимо)?

Брандмауэры в периметре сети

Брандмауэры, защищающие конфиденциальные ресурсы, хранящиеся внутри сети

Брандмауэры веб-приложений (WAF)

Антивирус или программное обеспечение по защите от вредоносных программ, которое обновляется или исправляется в соответствии с рекомендациями поставщика

Системы обнаружения или предотвращения вторжений

Упреждающее сканирование уязвимостей

Если выбран этот параметр, включены ли в сканирование уязвимости все веб-страницы? Да Нет

Физические элементы управления, препятствующие доступу к сети

Управление удаленным доступом к сети (например, VPN с двухфакторной аутентификацией)

2. Применяется ли “жесткая политика в отношении паролей”, требующая достаточной сложности и длины, а также требующая избегать повторного использования для всех учетных записей?

Да Нет

Если «Нет», пожалуйста, опишите меры, принимаемые для обеспечения безопасности паролей:

3. Практикуется ли увеличение степени безопасности конфигурации серверов и приложений? Да Нет

4. Имеется ли в организации рекомендательный список, предотвращающий запуск вредоносных и других неавторизованных программ?

Да Нет

Если «Нет», применяется ли принцип наименьших привилегий к правам пользователя? Да Нет

5. Пожалуйста, опишите процесс управления и установки исправлений в системах и приложениях (включая любой этап тестирования / проверки до развертывания):

6. Используете ли вы какие-либо неподдерживаемые операционные системы или программное обеспечение? Да Не



Если «Да», то как вы планируете решить эту проблему?

7. Есть ли у вас официальная политика контроля изменений, которая включает оценку рисков, тестирование, авторизацию, процедуры контроля изменений и процедуры отката для основных систем?
Да Нет
8. Производится ли резервное копирование критически важных систем чаще, чем некритических систем? Да Нет
9. Позволяется ли использование сотрудниками на работе собственных устройств? Да Нет
Если да, то как вы управляете этим риском? Пожалуйста, укажите также информацию о контроле доступа и удаленной очистке памяти устройств:
10. Отключен ли сотрудникам доступ к записи на USB-накопители? Да Нет
11. Пожалуйста, опишите, как отслеживаются и активно блокируются продвинутые вредоносные программы (которые не могут быть обнаружены традиционными антивирусными программами):
12. Представлена ли организация в социальных сетях? Да Нет
Если «Да», то все ли учётные записи имеют специальный пользовательский интерфейс, а не интерфейс общего администрирования, и как отслеживается активность в социальных сетях?
Да Нет

G. ПОЛИТИКА В ОБЛАСТИ БЕЗОПАСНОСТИ И ПРОЦЕДУРЫ ТЕСТИРОВАНИЯ

1. Поддерживаются ли какие-либо сертифицированные стандарты информационной безопасности? Да Нет
Если «Да», просьба указать (например, ISO27001):
2. Имеется ли общекорпоративная политика безопасности, которая доводится до сведения всех сотрудников? Да Нет
3. Имеется ли функция сбора информации о кибер-угрозах? Да Нет
4. Проводится ли регулярное тестирование на проникновение третьей стороны? Да Нет
Если «Да»:
а. Когда проводился последний тест?
б. Были ли высказаны какие-либо серьезные опасения в связи с каким-либо аспектом сети? Да Нет
с. Были ли определены и успешно устранены проблемы? Да Нет
5. Проводятся ли третьими сторонами регулярные аудиты безопасности? Да Нет
Если «Да»:
а. Когда проводился последний аудит?
б. Были ли высказаны какие-либо серьезные опасения в связи с каким-либо аспектом сети? Да Нет
с. Были ли определены и успешно устранены проблемы? Да Нет
6. Имеется ли программа непрерывного обучения сотрудников по вопросам конфиденциальности/безопасности данных, включая вопросы юридической ответственности и социального инжиниринга?
Да Нет



Если «Да», то включает ли это какое-либо активное тестирование сотрудников на социальный инжиниринг (например, фишинг)?

Да Нет

7. Производится ли проверка анкетных данных всех кандидатов на работу, подрядчиков и сторонних пользователей?

Да Нет

Н. КОММЕРЧЕСКИЕ СУБЪЕКТЫ, ТОЧКИ ПРОДАЖ И ИНДУСТРИЯ ПЛАТЁЖНЫХ КАРТ

Раздел заполняется только в том случае, если автор предложения принимает оплату картой

1. Принимается ли оплата посредством операций типа «С присутствием карты (Card-Present)»? Да Нет
Если «Да»:

a. Имеется ли полное соответствие стандартам обработки карт EMV Да Нет

b. Есть ли у ваших POS-систем функции защиты от взлома? Да Нет

c. Опишите процесс шифрования и/или токенизации данных, проходящих через сеть POS, укажите, используется ли межконцевое шифрование:

d. Вызывают ли изменения отдельных файлов в системе POS оповещения в режиме реального времени? Да Нет

e. Требуют ли изменения в системах POS официального согласования до внедрения? Да Нет

f. Регулярно ли POS-устройства проверяются на наличие вредоносных программ или устройств скимминга? Да Нет

g. Как часто сеть POS аудировается третьей стороной?

h. Выявил ли последний аудит сети POS критические уязвимости или уязвимости высокого уровня? Да Нет

Если да, то были ли они исправлены? Да Нет

i. Ваша система POS разработана и поддерживается поставщиком, отвечающим требованиям PA-DSS? Да Нет

j. Были ли изменены все пароли по умолчанию, предоставленные поставщиком? Да Нет

k. Пожалуйста, опишите, как разделяется сеть POS и корпоративная сеть?

l. Отслеживается ли вся активность пользователей в сети? Да Нет

m. Ведётся ли журнал учёта данных платежных операций и контролируется ли он на регулярной основе? Да Нет

2. Принимается ли оплата посредством транзакций типа «При отсутствии карты (Card-not-Present)»? Да Нет
Если «Да»:

a. Используются ли сторонние платежные шлюзы для обработки платежей? Да Нет

b. Пожалуйста опишите, как данные платежных карт фиксируются и передаются процессору кредитных карт, включая процесс шифрования и/или токенизации?

I. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ И ИСТОРИЯ ПРЕТЕНЗИЙ

1. Ведется ли журнал инцидентов, регистрирующий все нарушения системы безопасности и сбои в работе сети?

Да Нет

Если «Да», пожалуйста, опишите процесс эскалации и разбора таких инцидентов:

2. Имеется ли план реагирования на инциденты, включающий команду с определенными ролями и обязанностями?

Да Нет



Если «Да», то проверялся ли он в течение последних 12 месяцев? Да Нет

3. Был ли причинён ущерб за последние 5 лет по следующим причинам?

Несанкционированное разглашение или передача любой конфиденциальной информации, за которую организация несет ответственность

Да Нет

Любое вторжение, несанкционированный доступ или несанкционированное использование компьютерной системы

Да Нет

Любое случайное, небрежное или непреднамеренное действие или бездействие со стороны сотрудника организации или сотрудника любого стороннего поставщика услуг во время эксплуатации, обслуживания или модернизации вашей компьютерной системы

Да Нет

Приостановка или деградация компьютерной системы Да Нет

Невозможность получить доступ к данным из-за удаления, повреждения, порчи, изменения или потери таких данных

Да Нет

Вымогание выкупа или угроза безопасности Да Нет

Получение претензии в отношении любого из вышеперечисленных Да Нет

Любые формальные или официальные действия, расследование, запрос или аудит регулирующего органа, возникшие в связи с использованием, контролем, сбором, хранением, обработкой или подозрением на неправомерное использование личной информации

Да Нет

Если дан ответ “Да” на любой из вышеперечисленных вопросов, пожалуйста, укажите полную информацию:

J. ЗАПРАШИВАЕМЫЕ ПОКРЫТИЯ

Выберите, пожалуйста, запрашиваемые покрытия из нижеперечисленных:

Название покрытия	Лимит	Франшиза	Да / Нет
Первичное реагирование	48 часов	Отсутствует	
Защита данных и киберответственность			
Расходы в связи с киберинцидентом			
Сбои в работе сети			
Сбои в работе сети: Сбои у внешнего поставщика			
Сбои в работе сети: системный сбой			
Кибервымогательство			
Компьютерное преступление			



ДЕКЛАРАЦИЯ

Настоящим Заявитель подтверждает и заявляет, что все сведения, указанные в настоящем заявлении, являются полными и достоверными, а также что Страховщику настоящим заявлением сообщены все известные ему обстоятельства, имеющие существенное значение для определения вероятности наступления страхового случая и размера возможных убытков от его наступления (страхового риска).

Если после заключения договора страхования (страхового полиса) будет установлено, что страховщику были сообщены заведомо ложные сведения, Страховщик вправе потребовать признания договора страхования (страхового полиса) недействительным.

В период действия договора страхования (страхового полиса) Заявитель и Застрахованное лицо обязаны незамедлительно письменно сообщать Страховщику о ставших им известными значительных изменениях в обстоятельствах, сообщенных Страховщику при заключении и исполнении договора страхования (страхового полиса), если эти вышеназванные изменения могут существенно повлиять на увеличение страхового риска. Значительными признаются любые изменения в сведениях, указанных (содержащихся) в договоре страхования (страховом полисе), настоящем заявлении, а также иных документах, предоставленных (переданных) Страховщику при заключении и исполнении договора страхования (страхового полиса). Настоящее заявление, а также указанные выше документы являются неотъемлемой частью договора страхования (страхового полиса).

Подпись

Должность

Организация

Дата

АО «ГАРДИЯ» (лицензии на страхование ЦБ РФ СИ № 3947, СЛ №3947, ОС №3947-04, на перестрахование ПС №3947, последняя редакция от 11 января 2023 года, предлагает широкий спектр страховых услуг по имущественному и личному страхованию (страхованию иному, чем страхование жизни). Компания представлена на российском страховом рынке почти 30 лет. Уникальным преимуществом компании является сочетание глубокого знания российского рынка с международной практикой и стандартами предоставления услуг. За годы работы в России компания выплатила свыше 10,6 млрд рублей клиентам по страховым случаям. АО «ГАРДИЯ» является действующим членом ВСС, НССО.