**Панкратьев Вячеслав Вячеславович**

# **М Е Т О Д И Ч Е С К О Е П О С О Б И Е**

# 

**Корпоративная**

**безопасность**

**ПОСТРОЕНИЕ СИСТЕМЫ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ**

**Москва**

**2023**

**ПОСТРОЕНИЕ СИСТЕМЫ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ**

*Корпоративная безопасность достигается:*

* созданием организационно защищенной структуры бизнеса;
* проведением мероприятий по защите бизнеса;
* обеспечением безопасности при наследовании бизнеса, изменении юридического статуса владельца (например, семейного статуса) и снижение рисков для владельцев после его закрытия

*Уровни понимания и реализации корпоративной безопасности (на примере рисков)*

* 1 уровень – понимание корпоративной безопасности с позиции регуляторных рисков (риск нарушения требований законодательства), административных рисков (риск административного ресурса) и криминальных рисков (1990-2000)
* 2 уровень – понимание корпоративной безопасности с позиции риск-ориентированного подхода (формирование карты экономических рисков как системный подход к безопасности, работа по стандартам риск-менеджмента, создание системы управления рисками) (2000-2010)
* 3 уровень – понимание корпоративной безопасности с позиции бизнес-ориентированного подхода (монетизация риска, наличие ответственности за невыполнение требований законодательства, расстановка приоритетов, игнорирование части рисков и т.д.) (2010-2020)
* 4 уровень – понимание корпоративной безопасности с позиции адаптивного подхода к рискам (неожиданное появление новых рисков, которые заранее сложно просчитать, быстрое реагирование на ситуацию, оценка не рисков, а своих уязвимостей, анализ больших данных для быстрого просчитывания ситуации, приоритет имеет скорость принятия решения, работа в условиях хаоса и неопределенности, отсутствие стратегического планирования и т.д.) (2020 – нв)

*Объекты обеспечения безопасности:*

* операционная деятельность (бизнес-процессы);
* физические лица (лица, принимающие решение, работники, с которыми у предприятия есть трудовые договора, лица, с которыми у предприятия есть гражданско-правовые договора, представители контрагентов, посетители и т.д.);
* материальные активы (имущество, товарно-материальные ценности, готовая продукция и т.д.);
* нематериальные активы (объекты интеллектуальной собственности, ноу-хау, коммерческие секреты, товарные знаки, патенты, базы данных, научные разработки, персонал, имидж, бренд и т.д.);
* финансовые средства (наличные и безналичные деньги, ценные бумаги, акции, облигации, финансовые активы, криптовалюта и т.д.);
* информация и информационные системы.

*Субъекты обеспечения безопасности:*

1 вариант – обеспечением безопасности занимается собственник или исполнительный орган предприятия;

2 вариант – обеспечением безопасности занимается работник, у которого есть другие должностные обязанности (работа по совместительству);

3 вариант – обеспечением безопасности занимается выделенный работник (отдельная должность);

4 вариант – обеспечением безопасности занимается совещательный орган (совет, комитет, комиссия и т.д.) и выделенный работник;

5 вариант – обеспечением безопасности занимается внешняя организация (аутсорсинг);

6 вариант – обеспечением безопасности занимается отдельное подразделение предприятия;

7 вариант – обеспечением безопасности занимаются все подразделения предприятия в зонах своей ответственности;

8 вариант – смешанный вариант

*Модели систем корпоративной безопасности, сложившихся к 2020-2022 году*

* в организациях с государственным участием (основные направления – выполнение задач, поставленных перед предприятием и контроль за расходованием бюджетных средств);
* в организациях без государственного участия (основные направления – оказание помощи бизнесу в получении прибыли, участие в системе управления рисками, выстраивание отношений с административным ресурсом);
* в организациях, где законодательно определены задачи безопасности (ТЭК, объекты транспортной инфраструктуры, КИИ, финансовые организации и т.д.). Основное направление – выполнение требований законодательства;
* в иностранных организациях (основное направление - комплаенс, контроль за соблюдение стандартов и нормативов, защита имиджа предприятия и т.д. Учет менталитета и национальных особенностей)

*Виды аутсорсинга безопасности*

* комплексный;
* частичный (по времени или по задачам)

*Плюсы аутсорсинга по безопасности:*

* [профессионально;](http://www.controlrisks.com)
* проще для руководства предприятия;
* понятнее, так как действия регламентируются договором;
* безопаснее, так как риск ответственности за действия лежит на другом юридическом лице;
* возможность нестандартных решений исходя из опыта работы;
* независимость от мнения руководства предприятия;
* в некоторых случаях дешевле.

*Минусы аутсорсинга по безопасности:*

* в некоторых случаях дороже;
* требуется время на погружение в специфику предприятия;
* замедленное реагирование на изменение ситуации (заключение дополнительных соглашений к основному договору);
* допуск посторонних лиц на предприятие и к информации;
* конкуренция за квалифицированный персонал внутри аутсорсинговой компании, так как наиболее профессиональные работники обслуживают ключевых клиентов (выгодно быть ключевым клиентом);
* разные интересы (увеличить прибыль для аутсорсинговой организации и снизить затраты для самого предприятия).

*На аутсорсинг рекомендуется отдать:*

* закупку «коробочных решений», то есть готовых товаров (услуг) по безопасности, которые представлены на рынке;
* работы и услуги, требующие юридической легализации результатов (ИТ безопасность, инженерно-технические решения, видеонаблюдение, СКУД и т.д.);
* деятельность, связанная с независимостью и объективностью (независимый аудит безопасности или отдельных направлений, независимое консультирование, экспертное мнение и т.д.);
* деятельность, требующая лицензирования (охрана, осуществление пропускного и внутриобъектового режимов, детективная деятельность, техническая защита конфиденциальной информации, поиск устройств, предназначенных для негласного получения информации и т.д.);
* деятельность, предполагающая большие затраты (анализ конкурентной среды, ситуационные центры и т.д.);
* деятельность, требующая специальный статус физического лица (детектив, адвокат, оценщик, внешний аудитор и т.д.)
* деятельность, требующая специального статуса юридического лица или регистрацию в реестрах (подразделение транспортной безопасности, коллекторская организация и т.д.);
* деятельность, требующая специальных навыков (расследование ИТ преступлений, форензик, детектор лжи, профайлинг, почерковедческая экспертиза и т.д.);
* деятельность, связанная с повышенным риском (неофициальная проверка физических лиц, взыскание долгов, выполнение роли доверенных лиц и т.д.);
* иная деятельность, которую проще или дешевле отдать на аутсорсинг или в которой у предприятия нет хороших специалистов.

*На подразделение безопасности рекомендуется возложить следующие задачи:*

* участие в идентификации и управлении рисками на предприятии;
* организация работ по созданию корпоративной безопасности;
* создание локальной правовой базы в области корпоративной безопасности и осуществление контроля за ее выполнением;
* координация действий работников и подразделений предприятия по вопросам безопасности;
* информационно-аналитические задачи (в первую очередь в договорной и кадровой работе);
* контрольно-ревизионные задачи;
* задачи, связанные с требованиями законодательства в области корпоративной безопасности (безопасность объектов топливно-энергетического комплекса, промышленная безопасность, пожарная безопасность , ГО и ЧС и т.д.);
* антикоррупционные задачи (комплаенс);
* антитеррористические задачи;
* задачи по созданию режимов (государственная тайна, коммерческая тайна, пропускной и внутриобъектовый режим, взаимодействие с подразделениями охраны и т.д.);
* взаимодействие с государственными контролирующими и правоохранительными органам (МВД, ФСБ, прокуратура, судебные приставы и т.д.);
* взаимодействие с аутсорсинговыми организациями, представляющими услуги по корпоративной безопасности;
* задачи по инженерно-техническому оборудованию территории;
* задачи в сфере кибербезопасности (защита критически важной информационной инфраструктуры и т.д.);
* обеспечение безопасности руководства предприятия и безопасности принятия ими решений;
* организация защиты конфиденциальной информации;
* проведение внутренних проверок и расследований по фактам совершения противоправных действий со стороны персонала предприятия;
* участие в различных комиссиях на предприятии (антикоррупционной, инвентаризационной, по расследованию несчастных случаев и т.д.)

*Первые 10 шагов на должности директор по безопасности*

* шаг 1 – выяснить - зачем бизнесу нужна безопасность. Определить объекты безопасности. Оценить бизнес функцию безопасности;
* шаг 2 - изучить законодательство в части деятельности предприятия, применительно к задачам корпоративной безопасности;
* шаг 3 - понять бизнес процессы и специфику предприятия;
* шаг 4 - изучить инциденты на предприятии. Провести аудит корпоративной безопасности;
* шаг 5 - определить субъекты безопасности. Распределить задачи в области защиты бизнеса между аутсорсинговыми организация, подразделением безопасности и иными подразделениями предприятия;
* шаг 6 - сформировать штат подразделения безопасности;
* шаг 7 - определить подчинение, коммуникативные правила взаимодействия с иными должностными лицами и критерии оценки эффективности подразделения безопасности;
* шаг 8 - создать локальную правовую базу в области корпоративной безопасности;
* шаг 9 - выстроить связи с коллегами - безопасниками из других организаций;
* шаг 10 - получить необходимые знания, навыки и компетенции, необходимые в работе на данном предприятии

*Безопасность как бизнес функция.*

*Задачи, решаемые безопасностью, с позиции бизнеса*

* управление рисками;
* выполнение обязанностей ответственных, предусмотренных законодательством (ответственный за пожарную безопасность, ответственный за антитеррор, ответственный за промышленную безопасность и т.д.);
* выполнение функции комплаенс;
* выполнение контрольных функций (контроль процессов);
* оценка, анализ и расследование инцидентов;
* безопасность продуктов (услуг) как элемент конкурентного преимущества;
* повышение эффективности бизнес процессов

*Модели работы подразделения безопасности*

* минимизация страха наступления негативных последствий. Выполнение функции страхования от рисков – обычно в государственных предприятиях;
* участие в получении прибыли в агрессивной среде – обычно на предприятиях частного сектора экономики.

*Виды деятельности функции безопасности по инцидентам:*

* проверка инцидентов;
* расследование инцидентов;
* минимизация (возмещение) ущерба от инцидентов;
* предотвращение инцидентов;
* увеличение стоимости продуктов (услуг) в связи с отсутствием инцидентов

*Функция безопасности может реализовываться:*

* работая с инцидентами (произошедшими или моделируемыми). Задача – предотвращение инцидентов;
* выполняя контрольные функции, где любое отклонение от заданных параметров будет являться инцидентами. Задача – формирование контрольной среды

*Проблематика функции безопасности*

* высокая стоимость – организация элементов безопасности в каждой единице процесса невозможна ввиду ее стоимости;
* поражение качества процесса – каждая процедура контроля влечет за собой поражение качества или увеличение стоимости самого процесса;
* отставание технологий – средства организации контроля технологически отстают от средств автоматизации процессов;
* отложенная реакция – приводит к выборочности контролей и выявлению уже случившихся инцидентов

*Оценка работы подразделения безопасности*

* метод «учебной тревоги». Данный метод хорошо зарекомендовал себя при проверке эффективности охранных мероприятий, разновидности этого метода – попытки несанкционированного проникновения на территорию, прохода по поддельным пропускам, имитация кражи или выноса материальных ценностей;
* метод соблюдения регламентов. Данный метод основан на контроле за выполнением регламентов по отдельным направлениям деятельности (регламент проверки контрагента, регламент проверки кандидата на работу и т.д.);
* выполнение требований законодательства в области корпоративной безопасности;
* оценка на основе абсолютных и относительных показателей, которые можно подсчитать (процент краж, сумма предотвращенных хищений, выявленные нарушения в бизнес-процессах, взысканные долги и т.д.);
* метод оценки по количеству раскрытых нарушений. Данный метод опасен тем, что работники подразделения безопасности могут начать искусственно создавать нарушения, чтобы показать свою значимость и эффективность;
* метод оценки выполнения поставленных задач и планов;
* метод оценки по успехам - неудачам в деятельности предприятия. Эффективность данного метода тем выше, чем больше показатели в деятельности предприятия зависят от работы подразделения безопасности;
* метод KPI (коэффициент эффективности участия);
* экспертные оценки;
* метод оценки по совокупным показателям. Основу этого способа составляет разработанная на предприятии система показателей, которая может включать в себя объективные требования, знание теории и практики, общие экономические показатели на предприятии, неплановые проверки и т.д.

*При оценке учитывается*

* кто оценивает деятельность СБ: руководитель предприятия или руководитель СБ (учитывая различия подходов);
* какова специфика СБ (структура, цели, задачи СБ в компаниях различной направленности могут сильно отличаться);
* принцип - «за что платят (СБ), то и делаем»;
* успешность и финансовые результаты деятельности предприятия;
* наличие законодательных требований в деятельности предприятия.

*Подчинение подразделения безопасности:*

* владельцу бизнеса (учредителю);
* совету директоров;
* исполнительному органу (генеральному директору);
* акционерам;
* разделение подразделение безопасности на два подразделения (например, СБ и собственная безопасность) и подчинение каждой структуры разным лицам.

*Структура подразделения безопасности (по функционалу):*

* руководитель - статус заместитель директора предприятия (директор по безопасности);
* экономист - зона ответственности – экономическая безопасность;
* оперативник - зона ответственности – кадровая безопасность;
* аналитик - зона ответственности информационно-аналитическая работа;
* технарь - зона ответственности инженерно-техническая безопасность;
* кибербезопасник - зона ответственности информационная безопасность и ИТ безопасность;
* режимщик - зона ответственности взаимодействие с охраной, пропускной и внутриобъектовый режим;
* контролер (аудитор) – зона ответственности участие в контрольно-ревизионная деятельности;
* технолог – зона ответственности – консультирование подразделения безопасности по технологических процессам на предприятии

*Взаимодействие подразделения безопасности:*

* служба персонала;
* ИТ подразделение;
* юридическое подразделение;
* контрольно-ревизионное подразделение;
* комплаенс подразделение;
* подразделение по управлению рисками;
* маркетинговое подразделение;
* подразделение по продажам;
* подразделение по закупкам;
* финансовое подразделение;
* основные бизнес подразделения.

*Название подразделения безопасности:*

* служба безопасности;
* служба защиты активов;
* служба собственной безопасности;
* служба экономической безопасности;
* служба безопасности и режима.

*При создании и функционировании подразделения безопасности учитывается:*

* в законодательстве отсутствует понятие Служба безопасности. Поэтому подразделение безопасности может носить разное название. Также отсутствует профессия безопасник и профессиональные стандарты по работе безопасника (за исключением информационной безопасности, риск-менеджменту, промышленной безопасности и т.д.). Есть только отдельные отрасли, где в законодательстве применяется понятие СБ (например, в постановлениях Правительства РФ по обеспечению безопасности объектов топливно-энергетического комплекса);
* на подразделение безопасности возлагают задачи, которые ранее безопасники не выполняли (например, оценка эффективности бизнес-процессов, участие в стратегических сессиях и т.д.);
* понятие «безопасность» все чаще ассоциируется с риск-менеджментом;
* основные задачи корпоративной безопасности связаны с контрольными, информационно-аналитическими и инженерно-техническими мероприятиями;
* существуют различия по задачам СБ в организациях без государственного участия, в коммерческих организациях с государственным участием (госкорпорации, госкомпании и т.д.) и в иностранных компаниях;
* в последнее время снижается значимость связей безопасника с правоохранительными органами и другими силовыми структурами;
* подразделение безопасности будет конфликтовать как с основными подразделениями, так и с иными контролирующими подразделениями (служба внутреннего контроля, служба аудита, служба информационной безопасности и т.д.);
* подразделение безопасности комплектуются не только бывшими работниками правоохранительных органов, но и иными специалистами (экономистами, технологами, специалистами по информационной безопасности и т.д.);
* в иностранном законодательстве (в первую очередь европейском и американском) также нет понятия служба безопасности. У них безопасность не выделена в отдельный процесс, а привязана к основным бизнес процессам. Кроме того вся безопасность в обязательном порядке привязана к рискам, обязательно наличие должности риск-менеджер (или подразделения);
* нет четких должностных обязанностей у безопасника, на разных предприятиях работники безопасности могут выполнять разные должностные обязанности;
* нет стандартов по корпоративной безопасности, поэтому система корпоративной безопасности строится индивидуально под конкретную организацию. Как правило, учитываются три фактора – риски для предприятия, требования законодательства и пожелания владельца (заказчика);
* желательно, чтобы СБ помогала бизнесу зарабатывать деньги, а не являлась только затратным пассивом (например, предоставляло информационно-аналитичекие материалы для получения конкурентных преимуществ и т.д.);
* могут быть имиджевые потери для предприятия от деятельности СБ. К этому надо быть готовым и стараться их минимизировать. Мероприятия с повышенным имиждевым риском для предприятия желательно отдавать на аутсорсинг;
* безопасник часто становится доверенным лицом, обеспечивающим безопасность руководителя, поэтому на первый план выходит лояльность безопасника, а не его профессионализм;
* идет тенденция к сокращению штата подразделений безопасности. Многие задачи, решаемые безопасниками ранее, переданы на аутсорсинг или распределены между подразделениями. Безопасников используют там, где недостаточно текущего профессионализма работника или профессиональные навыки нельзя быстро получить (например, умение вести визуальное наблюдение, расследовать инциденты и т.д.), а также там, где требуется осуществлять более жесткие контрольные или информационно-аналитические функции;
* в связи с сокращением штатов подразделений безопасности безопасники трансформируются в риск-менеджеров, контролеров или комплаенс-менеджеров;
* в работе СБ все чаще ставятся задачи по защите нематериальных активов. Актуальны задачи по защите бренда, интеллектуальной собственности, деловой репутации, товарного знака и т.д.;
* безопасник должен хорошо знать цифровые технологии и уметь работать в условиях «цифрового мира»

*Начальник подразделения безопасности должен отвечать следующим требованиям:*

* быть лояльным к руководителю предприятия и заинтересованным в развитии бизнеса;
* понимать цели бизнеса и бизнес процессы;
* понимать финансы и способы получения прибыли;
* знать бизнес лексику (форкаст, корреляция, предикт и т.д.);
* уметь видеть и строить корпоративную безопасность как систему;
* быть специалистом в основной задаче, которая стоит перед безопасностью;
* понимать, что нужно бизнесу от безопасности;
* понимать, что безопасность в организациях частного сектора экономики строится по другим правилам, чем в государственных органах;
* знать общее понимание технологий процессов, в первую очередь информационных технологий в бизнесе и безопасности;
* предлагать руководителю решения в области корпоративной безопасности, которые нужны бизнесу, а не те решения, которые он умеет делать исходя из прошлого опыта службы.

*Законодательство в области корпоративной безопасности*

* международное законодательство, включая конвенции ООН и т.д.
* международные универсальные стандарты по безопасности (например, ИСО);
* международные стандарты по безопасности, применимо к специфике деятельности (например, стандарт безопасности TAPO для складов и производственно-сортировочных центров);
* российское законодательство
* Конституция РФ;
* федеральные законы в форме кодексов (УК, КОАП, ГК, ТК, НК);
* федеральные законы (о частной детективной и охранной деятельности, об ОРД, о коммерческой тайне, о персональных данных, об информации, информатизации и защите информации, о государственной тайне, о безопасности объектов ТЭК, о транспортной безопасности, о промышленной безопасности, о противодействию терроризму, о противодействию коррупции, о безопасности критической информационной инфраструктуры, о пожарной безопасности и т.д.);
* Указы Президента РФ и постановления Правительства РФ.
* ведомственные акты и стандарты (банковские стандарты, приказы Минфина, Минтруда, Росимущества, ФНС и т.д.);
* корпоративные акты и стандарты (например, приказы госкорпораций или иностранных компаний);
* локальные акты предприятия в части обеспечения безопасности

*Особенности построения корпоративной безопасности в иностранных компаниях:*

* слабое понимание иностранными владельцами как защищать бизнес в России;
* восприятие правоохранительных органов как угрозу бизнесу;
* отсутствие веры в независимость и эффективность судебной защиты;
* непонимание значимости «административного ресурса» для деятельности предприятия;
* уверенность в коррумпированности всех государственных органов;
* стремление соблюдать все требования законодательства как при ведения бизнеса, так и в мероприятиях по обеспечению его безопасности;
* использование требований международного законодательства на территории РФ;
* отсутствие понятия «безопасник». Есть риск-менеджеры, комплаенс-менеджеры, работники внутренний контроля, аудиторы;
* большая значимость рисков имиджевых потерь для предприятия, чем рисков материального ущерба;
* построение корпоративной безопасности на основе стандартов и правил, применяемых в своих странах

*Структура корпоративной безопасности в иностранных компаниях*

* нормативно-правовое соответствие (security compliance). Это направление безопасности включает в себя построение определенных процессов, написание политик и процедур, отслеживание их соответствия в различных подразделениях компании;
* операционная безопасность (operational security), это та часть безопасности, которая отвечает за операционные процессы и интеграцию в них различных элементов – сотрудников охранного предприятия, технических средств (видеонаблюдение и его интеграция с системами складского учета, контроль и разграничение доступа, досмотровое оборудование, охранная сигнализация и т.д.;
* операционная эффективность и взаимодействие с бизнес-функциями (operational efficiency and crossfunctional cooperation);
* культура безопасности и обучение (security culture and awareness);
* управления рисками на предприятии (enterprise risk management program).

*Принципы построения корпоративной безопасности:*

* комплексность;
* своевременность (превентивный характер);
* непрерывность;
* активность;
* законность;
* системность и плановость;
* целесообразность (цена безопасности – цена потерь от ее отсутствия);
* дублирование (процессов, информации и т.д.);
* специализация;
* взаимодействие и координация;
* совершенствование;
* «не навредить бизнесу»;
* централизация управления;
* золотое сечение безопасности. Существуют три понятия: качество, скорость и цена. Строя систему безопасности, определитесь с приоритетностью. Приоритет можно отдать только двум из трех;
* построение безопасности по трем факторам – люди, процессы и технологии;
* работа при отсутствии «контура безопасности»;
* персональная ответственность;
* минимальное использование человеческого фактора;
* ограничение и разграничение полномочий;
* многорубежность систем безопасности;
* сегментированность (процессов, информационных систем и т.д.);
* равнопрочность;
* сочетание гласности с конспирацией;
* психологическое воздействие на правонарушителя.

*Средства обеспечения безопасности*

* технические средства;
* организационные средства;
* информационные средства;
* финансовые средства;
* правовые средства;
* кадровые средства.

*Организационно защищенная структура бизнеса:*

* регистрация предприятия в оффшоре;
* разделение бизнеса. Например, на два блока - владеющие (активы) и операционные юридические лица (договорная работа). Или на четыре блока – владеющие, управляющие, торговые и производственные;
* создание холдинга (экосистемы);
* отсутствие собственности и активов, интересных для рейдеров (аренда помещений, лизинг оборудования и т.д.);
* обременение активов (например, использование залоговых схем);
* наличие филиалов и представительств;
* диверсификация бизнеса;
* включение интересов государства в бизнес (часть акций принадлежит государству, вхождение в госкорпорации, участие в гособоронзаказе, в госпроектах, в нацпроектах и т.д.);
* защищенная организационно-правовая форма (например, хозяйственное партнерство или непубличное акционерное общество);
* защита лиц, принимающих решения;
* работа в иностранном правовом поле.

*Защита собственников (исполнительных органов) предприятия осуществляется:*

* установлением защищенности принятия решения (распределение акций, выстраивание отношений с инвесторами, и т.д.);
* наличием нескольких генеральных директоров;
* наличием Совета директоров, куда включаются независимые директора;
* выдачей доверенностей и делегированием полномочий;
* назначением ответственных за отдельные направления деятельности (ГО и ЧС и т.д.);
* принятием решений на основе комиссионных мнений;
* отсутствием в период проведения конфликтных мероприятий (проверки и т.д.);
* установлением для генерального директора максимальной суммы сделки, которую он может заключать;
* подчинением безопасности, аудита, комплаенс собственникам бизнеса (Совету директоров);
* заключением срочного трудового договора с генеральным директором;
* финансовой заинтересованностью генерального директора от успехов предприятия;
* страхованием управленческих рисков;
* защитой от претензий со стороны наследников или бывших супругов;
* согласованием принятия стратегических решений (например, взятие кредитов);
* наличием двойного гражданства.

*Система безопасности включает в себя подсистемы:*

* информационная безопасность;
* кадровая безопасность;
* экономическая безопасность;
* физическая безопасность;
* личная безопасность;
* инженерно-техническая безопасность;
* техническая безопасность;
* кибербезопасность;
* правовая безопасность;
* экологическая безопасность;
* техногенная безопасность;
* промышленная безопасность.

*Информационная безопасность достигается:*

* режимными мероприятиями;
* инженерно-техническими мероприятиями;
* организационными мероприятиями;
* правовыми мероприятиями;
* IT мероприятиями;
* кадровыми мероприятиями

*Кадровая безопасность достигается:*

* мероприятиями при подборе кадров;
* мероприятиями по защите от противоправных (некомпетентных) и иных действий со стороны работников, включая как превентивные мероприятия, так и проведением внутренних проверок и расследований;
* мероприятиями при увольнении работников.

*Экономическая безопасность достигается:*

* управлением экономическими рисками;
* организацией безопасной договорной работы;
* проверкой контрагентов и оценкой безопасности коммерческих предложений;
* управлением дебиторской задолженностью;
* мероприятиями по защите активов;
* контрольно-ревизионными мероприятиями;
* аудитом финансовой деятельности;
* взаимодействием с государственными контролирующими и правоохранительными органами.

*Физическая безопасность достигается:*

* контрольными мероприятиями силами работников предприятия;
* проведением охранных мероприятий внешними организациями.

*Личная безопасность достигается:*

* мероприятиями по физической защите лиц, принимающих решения;
* мероприятиями по юридической защите лиц, принимающих решение;
* мероприятиями по психологической защите лиц, принимающих решения (защита от манипулирования, от принятия решения в состоянии аффекта и т.д.);
* мероприятиями по технической защите помещений (автотранспорта) в которых находятся лица, принимающие решения.

*Инженерно-техническая безопасность достигается:*

* противопожарными мероприятиями;
* мероприятиями по контролю и управлению доступом на территорию предприятия;
* осуществлением видеонаблюдения на территории предприятия;
* контролем периметров;
* установкой систем сигнализации.

*Техническая безопасность достигается:*

* мероприятиями по защите акустического канала утечки информации;
* мероприятиями по защите визуального канала утечки информации;
* мероприятиями по защите от побочных электромагнитных излучений и наводок.

*Кибербезопасность достигается:*

* мероприятиями по защите информации;
* мероприятиями по защите информационных систем, в которых находится и обрабатывается информация

*Правовая безопасность достигается:*

* соблюдением требований законодательства (работа в правовом поле);
* отслеживанием изменения законодательства в области деятельности предприятия;
* профессиональными действиями корпоративных юристов;
* созданием защищенной структуры бизнеса;
* организацией безопасной договорной работы;
* привлечением адвокатов и организаций, специализирующихся на правовой защите

*Экологическая безопасность достигается:*

* выполнением требований законодательства в сфере экологии;
* проведением исследований помещений, занимаемых предприятием (радиационный фон, химические вещества и т.д.)

*Техногенная безопасность достигается:*

* выполнением требований законодательства в области ГО и ЧС;
* выполнением требований антитеррористической защиты объектов (территорий);
* выполнением требований законодательства в области промышленной безопасности;
* выполнением требований законодательства в области пожарной безопасности.

*Промышленная безопасность достигается:*

* выполнением требований законодательства в области промышленной безопасности (безопасность опасных производственных объектов)

*Способы функционирования системы безопасности*

* «одевание брони»;
* изменение местоположения;
* устранение угрозы;
* нахождение защитника;
* маскировка истинного положения дел.

*При определении уровня финансирования системы безопасности нужно учитывать:*

* система безопасности является непроизводственной сферой, она не зарабатывает деньги, она способствует их сохранению;
* полноценная отдача от системы безопасности в целом может быть получена примерно через полгода после начала ее создания, хотя отдельные подсистемы могут начать активно функционировать и выполнять поставленные задачи с первых дней;
* обеспечение высокого уровня безопасности требует больших финансовых вложений

Особенность построения корпоративной безопасности в условиях экономического кризиса

*Период экономического кризиса характеризуется:*

* снижением финансирования мероприятий, направленных на обеспечение безопасности;
* снижением количества оборотных денег;
* снижением количества «коммерческих» денег при увеличении доли «бюджетного финансирования»;
* снижением покупательского спроса у населения;
* изменением направлений деятельности и оптимизацией организационной структуры предприятия;
* снижением заработной платы работников и общего уровня жизни;
* отсутствием полной загрузки работников с предоставлением вынужденных неоплачиваемых отпусков;
* массовыми увольнениями работников;
* обострением отношений между акционерами (совладельцами) предприятия;
* увеличением случаев невыполнения договорных обязанностей контрагентами и увеличением задолженностей по платежам.

*Особенность экономической и политической ситуации 2022*

* включение в рыночные отношения элементов административно-командного регулирования (локдаун, запрет на банкротство, мобилизация и т.д.);
* неэффективность работы классической (стандартизированной) системы риск-менеджмента, ориентированной на рыночные отношения. Основной риск – нарушение непрерывности бизнес процессов и не выполнение поставленных задач;
* специальная военная операция, содействие предприятий проведению СВО;
* мобилизация (добровольная и принудительная) как населения, так и экономики. Релокация трудовых ресурсов;
* монополизация экономики, включение интересов государства в коммерческую деятельность, увеличение доли государственных интересов в бизнесе (госкорпорации, госкомпании, акционерные общества с государственным участием, организации, созданные для выполнения задач, поставленных перед государственными органами и т.д.). Построение госкапитализма;
* увеличение доли бюджетных денег при снижении доли коммерческих денег. Финансы и ресурсы в основном находятся в руках государства;
* поддержка государством отдельных отраслей (ИТ отрасли, оборонно-промышленный комплекс и т.д.). Ожидание и оказание помощи предприятиям от государства (госзаказы, участие государства в бизнесе, снижение налогов и т.д.);
* информационные войны, появление большого количества недостоверной и манипулятивной информации;
* неэффективность юридических гарантий по договорам, особенно международным. Приостановка авторских прав и объектов интеллектуальной собственности для предприятий из недружественных стран. Актуальность понятия «форсмажор». Личные связи и неофициальные договоренности с должностными лицами более надежны, чем юридические нормы договора;
* снижение административного давления на бизнес (мораторий на проверки и т.д.);
* санкционное воздействие со стороны иностранных государств. Разделение стран на дружественные и недружественные и влияние этого фактора на экономические связи с ними. Риски попасть под первичные и вторичные санкции;
* выход инвесторов недружественных стран из российских проектов;
* импортозамещение и ориентация на внутренний рынок;
* появление параллельного импорта, а также создание организаций (технических компаний), созданных для обхода санкций и реализации параллельного импорта. Релокация предприятий;
* уменьшение количества достоверной и объективной информации (закрытие информации по компаниям, попавшими под санкции, уведичение доли закрытых торгов, уход с российского рынка международных рейтинговых агентств, закрытие информации по акционерам и т.д.);
* непредсказуемость (непросчитываемость на долгосрочный период) ситуации, а также быстрое изменение ситуации. Снижение горизонта планирования. Отсутствие стратегического планирования. Применение теории хаоса на практике;
* быстро меняющееся законодательство и административные решения государственных органов;
* закрытие границ и разрушение логистических цепочек;
* нарушение международного банковского обслуживания применительно к российским предприятиям и физическим лицам. Усложнение валютных операций;
* массовый перевод работников на дистанционную работу;
* увеличение социальной защиты работников со стороны государственных органов и судов;
* смена поколений. В руководство предприятий приходит другое поколение. Проблема связи поколений;
* появление цифровых финансовых активов (криптовалюта, цифровые обязательства, токены и т.д.);
* снижение доли посреднических задач в одних бизнес процессах и увеличение посредников в других бихнес процессах (например, при обходе санкций);
* различная правовая ситуация по регионам (особенно применимо к понятию форсмажор);
* уменьшение количества рабочих мест (в связи с цифровизацией), изменение потребностей в профессиях, увольнение персонала;
* изменение бизнес процессов в связи с массовым внедрением информационных технологий и элементов искусственного интеллекта (цифровизация экономики и бизнес процессов). Приоритет информационных технологий над безопасностью;
* уменьшение количества трудовых отношений и увеличение количества гражданско-правовых отношений.

*Особенности построение системы безопасности в период экономического кризиса:*

* изменение направлений деятельности подразделения безопасности исходя из изменения рисков;
* реорганизация (сокращение) подразделения безопасности в связи с передачей части функций в другие подразделения или на аутсорсинг;
* изменение концепции безопасности предприятия;
* привлечение подразделения безопасности к проведению антикризисных мероприятий;
* проведение мероприятий с увольняемыми работниками с целью недопущения нанесения ими ущерба интересам предприятия после увольнения;
* увеличение количества внутренних расследований и проверок;
* увеличение количества мероприятий по пресечению противоправных действий со стороны персонала;
* увеличение количества мероприятий, направленных на оценку надежности контрагентов;
* увеличение количества мероприятий, направленных на взыскание дебиторской задолженности.

*Особенности построения безопасности при санкционном давлении*

Санкции в разбивке по группам регуляторного давления:

* особая группа;
* уголовная ответственность;
* критическая гражданско-правовая ответственность;
* блокирование имущества или имущественных прав;
* ограничение или запрет на сделки;
* отзыв или приостановление лицензий (разрешений);
* санкции в отношении капитала (финансирования);
* запрет на заход транспортных средств в географическую зону, запрет перевозок;
* запрет на право пользования телекоммуникационными сетями (радиочастотным ресурсом);
* экспортные ограничения;
* визовые ограничения;
* запрет государственных закупок у объекта санкций;
* запрет на участие в приватизации (аренду государственного имущества);
* дополнительные инспекции

В зависимости от степени ущерба, потенциал которого заложен в каждую соответствующую санкцию, они распределены на 4 уровня существенности, в частности:

* уровень 1 - наименьший негативный эффект;
* уровень 2 - средний негативный эффект;
* уровень 3 - повышенный негативный эффект;
* уровень 4 - критический негативный эффект

Системы, существенные для российских хозяйствующих субъектов, наиболее подверженные санкциям:

* контрагенты и хозяйственные связи с ними;
* зарубежные страны, включая существенные для операций предприятия;
* базовая страна – Российская Федерация;
* нормативные режимы экспорта и импорта;
* пограничные режимы;
* хозяйствующие субъекты, защита которых возложена на нас, в частности:
* корпоративная структура;
* система финансирования;
* системы сбыта;
* система снабжения

Для прогнозирования санкционных уязвимостей на предприятии используется применяемая США в ряде санкционных систем мера «блокирование имущества и имущественных прав объекта» и т.н. «Правило 50». Данное правило на сегодня действует во исполнение Приказа Министерства финансов США от 13.08.2014 г. Применение «Правила 50» означает, что считается заблокированным лицом организация, в капитале которой доля равная 50 и более процентов прямо или косвенно, принадлежит одному или более заблокированным лицам, единолично или совместно, в сумме.

Имущество и имущественные интересы такой организации считаются заблокированными вне зависимости от того вносится ли организация в приложение к соответствующему Исполнительному указу и упоминается ли она в списке заблокированных лиц («US SDN формат»), который администрирует OFAC. Правило 50 также применяется к секторальным санкциям («US SSI формат»), которые в основном направлены на то, чтобы ограничить доступ объекта санкций и лиц под его контролем к зарубежному финансированию. Прогнозирование уязвимостей проводится путем оценки применения «Правила 50» к головной компании группы и головным компаниям субхолдингов внутри группы.

*Типы санкций*

* блокирующие;
* отраслевые;
* транспортные;
* территориальные;
* торговые;
* персональные

*Особенность построения безопасности в условиях хаоса и неопределенности:*

*Теория хаоса. Основа:*

* тео́рия ха́оса — математический аппарат, описывающий поведение некоторых [нелинейных динамических систем](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BB%D0%B8%D0%BD%D0%B5%D0%B9%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), подверженных при определённых условиях явлению, известному как [хаос](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%BD%D0%B0%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%85%D0%B0%D0%BE%D1%81) (динамический хаос);
* в бытовом контексте слово «[хаос](https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BE%D1%81)» означает «быть в состоянии беспорядка».
* примерами подобных систем являются [атмосфера](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%BC%D0%BE%D1%81%D1%84%D0%B5%D1%80%D0%B0_%D0%97%D0%B5%D0%BC%D0%BB%D0%B8), [турбулентные потоки](https://ru.wikipedia.org/wiki/%D0%A2%D1%83%D1%80%D0%B1%D1%83%D0%BB%D0%B5%D0%BD%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C),  [биологические популяции](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BF%D1%83%D0%BB%D1%8F%D1%86%D0%B8%D1%8F), [общество](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%BE) как система коммуникаций и его подсистемы: экономические, политические, психологические культурно-исторические и другие социальные системы;
* теория хаоса гласит, что сложные системы чрезвычайно зависимы от первоначальных условий, и небольшие изменения в окружающей среде могут привести к непредсказуемым последствиям.

*Особенности построения корпоративной безопасности в условиях хаоса и неопределенности*

* законы рыночной экономики и идеальной конкуренции работают только в идеальных условиях, которых нет в реальной жизни. Модель существует, чтобы объяснять мир в каком-то приближении. Везде, кроме экономики, модель подгоняется под мир. **Только в экономике мир подгоняется под модель;**
* в условиях неопределенности отсутствует система стратегического планирования – предприятие работает в отсутствии долгосрочных планов. На первый план выходит способность быстро ориентироваться в ситуациях и принимать (менять) решения в зависимости от обстановки. Происходит переход от планирования к постановке задач;
* из планов на первое место выходят антикризисные планы (планы действий в чрезвычайных ситуациях, действий при наступлении определенных событий, мобилизационные планы и т.д.);
* в договорах использовать статью 157 ГК РФ (отлагательные и отменительные условия) – Сделки, совершенные под условием.
* «Сделка считается совершенной под отлагательным условием, если стороны поставили возникновение прав и обязанностей в зависимость от обстоятельства, относительно которого неизвестно, наступит оно или не наступит»
* «Сделка считается совершенной под отменительным условием, если стороны поставили прекращение прав и обязанностей в зависимость от обстоятельства, относительно которого неизвестно, наступит оно или не наступит»
* в договорах использовать статью 327.1 ГК РФ (потестативное условие) – Обусловленное исполнение обязательства.
* «Исполнение обязанностей, а равно и осуществление, изменение и прекращение определенных прав по договорному обязательству, может быть обусловлено совершением или несовершением одной из сторон обязательства определенных действий либо наступлением иных обстоятельств, предусмотренных договором, в том числе полностью зависящих от воли одной из сторон»
* в условиях неопределенности классические системы контроля являются неэффективными (такие как контроль регламентов, контроль процессов и т.д.). Целесообразно предоставить некоторую свободу действий. На первый план выходит контроль выполненных задач, а не процессов. Пример - контроль за дистанционными работниками;
* в условиях неопределенности применяется такая «военная тактика» как «разведка боем», то есть попытка понять как будет разворачиваться ситуация на практике при реализации какого-либо события (вброс нужной информации или дезинформации, заключение договора на небольшую сумму и т.д.);
* в условиях неопределенности меняется система менеджмента – единая система разбивается на множество подсистем, работающих автономно без жесткой системы централизованного управления. Жесткая «вертикаль власти» и наличие единого и единственного центра принятия решений является неэффективной. Происходит делегирование полномочий в принятии управленческих решений на всех уровнях;
* в условиях неопределенности особое значение приобретает доступ к обективной и достоверной информации. Предприятие будет успешным, когда научится оперативно получать и быстро анализировать информацию. Например, создание ситуационных центров, работающих в круглосуточном режиме**;**
* в условиях неопределенности приобретает значение аналитика, особенно в области управления рисками. При анализе ситуации сначала разрабатываются негативные сценарии, затем нейтральные, потом позитивные. Аналитики предлагают несколько вариантов развития событий (сценариев);
* в условиях неопределенности в аналитике происходит переход от просчитываемости ситуации и рисков к просчитываемости своих возможностей и уязвимостей**;**
* в условиях неопределенности локальные нормативные документы, подготовленные ранее, не работают. Приходится или постоянно работать в «ручном режиме» или переделывать нормативные документы и включать в них большие «допуски» при принятии управленческих решений. Но это увеличивает вероятность наличия коррупциогенных факторов в локальных документах предприятия;
* в условиях неопределенности юридические нормы работают плохо, все, что прописано в договорах с контрагентами может быть не выполнено по объективным причинам, не зависимым от контрагента. Поэтому на первое место выходит не юридическая сторона взаимоотношений, а межличностная. Безопасникам желательно лично знать лиц, принимающих решения у контрагентов. Но это повышает риск аффилированности, личной заинтересованности и конфликта интересов;
* в условиях неопределенности безопасникам желательно создавать универсальные алгоритмы действий, которые будут работать во всех ситуациях**;**
* в условиях неопределенности нужно учитывать биологические и психологические особенности человека, принимающего решения. При неясности ситуации решения человеком принимаются на основе инстинктов;
* **при принятии управленческих решений приобретает повышенное значение такое качество как «пластичность»;**
* незначительные события могут иметь значительные последствия (эффект бабочки). Изменения на рынке выглядят случайными, но между ними есть связь, поэтому статистически они не являются случайными;
* в условиях неопределенности особое значение приобретают потенциальные резервы (финансовые, кадровые и т.д.), но уменьшается значение материально-технических резервов. Также важна диверсификация ресурсов, направлений деятельности, договоренностей и т.д.;
* способность четко просчитывать действия (например, как в шахматах) заменяется умением быстро ориентироваться в ситуации (например, как в футболе);
* особое значение принимает быстрота принятия решения, это становится важнее безопасности и оценки рисков в принятии решения;
* осуществляется постоянная обработка большого количества информации для формирования разных моделей поведения при разных исходных данных. Информатизация и цифровая трансформация;
* происходит диверсификация ресурсов, направлений деятельности, договоренностей и т.д.;
* в людях ценится психологическая устойчивость к быстро меняющемуся миру, готовность к любым неожиданностям;
* отсутствует надежность во всем - контрагенты, люди, процессы, договоренности и т.д.;
* уделяется повышенное внимание временным срокам (оборачиваемости капитала, процессов, тайм-то-маркет и т.д.), уменьшается жизненный цикл товаров, услуг и т.д. Чем меньше срок – тем безопаснее;
* происходит оценка ситуации, рисков и иных параметров применимо к конкретному периоду времени;
* происходит понимание, что измерения и прогнозы никогда не бывают точны, предсказания имеют долю вероятности и т.д. Оценка с точностью до миллиметра не производится. Как правило, оценка идет по трехуровневой шкале – маловероятно, вероятно, очень вероятно. Или по системе светофора – красный, желтый, зеленый;
* приходит понимание, что на основе статистических параметров из прошлого нельзя строить прогнозы на будущее. Статистика несовершенна и манипулятивна. Невозможно использовать опыт других организаций;
* динамические системы (быстро меняющиеся) не поддаются оценке (например, оценка человека);
* **найденная успешня бизнес-модель и не может продолжаться долго, успехи или неудачи других компаний формировались в условиях другой обстановки, поэтому простое копирование их действий не приводит к аналогичным результатам;**
* в условиях неопределенности в аналитике ценность приобретают те результаты, которые говорят не то, что будет, а то, что точно не будет. Это более надежно и гарантировано;
* популярность приобретают саморегулируемые модели, которые самостоятельно настраиваются в зависимости от изменяющейся обстановки (желательно без участия человека). Самоорганизующийся порядок, возникает из сочетания взаимозависимости элементов с их относительной свободой. Если в компании у каждого сотрудника свои цели, свои KPI показатели, свое виденье рынка и своей работы, все процессы бюрократизированы и формализованы, а решения принимаются только высшим руководством, то никакой самоорганизации быть не может. Такие компании имеют шанс на успех только в стабильных и предсказуемых условиях;
* принятые неправильные решения могут корректироваться дальнейшими хаотическими событиями;
* полученные предприятием достижения и успехи могут быть скорректированы и нивелированы в условиях хаоса;
* в условиях неопределенности безопаснику иногда лучше доверять интуиции, чем аналитическим прогнозам;
* становится неэффективным перфекционизм (доведение до совершенства);
* в условиях неопределенности самым слабым звеном оказывается человек, поэтому происходит массовое внедрение «искусственного интеллекта» в технологию принятия решений;
* хаотические (непредсказуемые) системы безопасности являются более эффективными;
* системы сбалансированных показателей (Balanced Scorecard), KPI, BCG матрицы, SMART-цели и другие методы, основанные на математике и игнорирующие переменчивость внешней среды, становятся неэффективными, так как не учитывают явления хаоса

*При построении системы корпоративной безопасности желательно знать:*

* наиболее эффективная система корпоративной безопасности возникает тогда, когда система создается в виде баррикады, где с одной стороны находятся руководство, персонал, подразделение безопасности, а с другой стороны правонарушитель;
* корпоративная безопасность уходит от расследования фактов нарушений к предотвращению негативных событий (анализ, риск-менеджмент и т.д.);
* при построении системы корпоративной безопасности многое зависит от позиции руководства предприятия - если оно заинтересовано в наведении порядка и поддерживает подразделение безопасности в их действиях, то состояние безопасности достигается быстрее;
* одной из главных угроз интересам бизнеса являются угрозы со стороны административного ресурса;
* все чаще приходится защищаться от черных PR-акций, направленных на подрыв авторитета (имиджа) предприятия;
* задачи по безопасности можно распределить по подразделениям, а можно сконцентрировать в подразделении безопасности. И тот и другой вариант имеют свои положительные и отрицательные стороны. То есть безопасность можно строить как отдельный бизнес-процесс, а можно встраивать в уже существующие бизнес процессы;
* острые вопросы деятельности подразделения безопасности – оценка ее деятельности и мотивация ее работников. Работа профессионально функционирующего подразделения безопасности не видна, так как действует на упреждение, оценка деятельности работников затруднена тем, что нет эффективных и наглядных методик оценок;
* любая система безопасности тормозит развитие организации в целом. Единственный выход – следовать за изменениями, меняться вслед за бизнесом. Наиболее эффективно управление безопасностью там, где оно непосредственно включено в бизнес-процессы;
* резко сократилось время от начала разработки продукта (услуги) до его выхода на рынок, а также время жизни товара. Безопасность не поспевает и поэтому думать о безопасности начинают после выхода на рынок товара (услуги). Также высокий темп развития технологий не позволяет должное время уделять безопасности;
* на корпоративную безопасность большое влияние оказывает цифровизация процессов и цифровые технические решения;
* блок безопасности превращается из подразделения, которое тратит деньги в подразделение, которое приносит прибыль;
* безопасник в современном мире должен изменить свое предложение бизнесу с «знаю как» на «знаю зачем»;
* безопасник в современном мире должен отслеживать тренды (изменения, продукты и т.д.)

*Аудит корпоративной безопасности*

*Цели аудита:*

* оценка соответствия защищенности организации существующим рискам;
* оценка выполнения требований законодательства в области корпоративной безопасности;
* анализ возможностей совершенствования системы корпоративной безопасности

*При проведении аудита корпоративной безопасности:*

* учитывать требования международного стандарта ИСО 19011 «Руководящие указания по аудиту систем менеджмента»;
* определить цель и область аудита, составить программу, план и критерии аудита. Аудит может проходить как всей системы безопасности, так и отдельных элементов;
* определить группу по аудиту, включив в нее аудиторов, а при необходимости включив в нее технических экспертов с дополнительной компетенцией. Назначить руководителя группы по аудиту. Учитывать, что в небольших организациях аудит корпоративной безопасности может проводиться и одним аудитором;
* определить лиц, сопровождающих группу по аудиту (наблюдателей);
* определить задачи каждого аудитора из аудиторской группы;
* учитывать основные принципы аудита – профессионализм, объективность, конфиденциальность, независимость, доказательность и т.д.;
* изучить предварительно бизнес процессы организации и существующую систему защиты бизнеса;
* учитывать систему корпоративной безопасности холдинга или группы компаний, если организация в них входит;
* учитывать инциденты в области корпоративной безопасности, произошедшие в компании за последнее время;
* определить тип аудита – документарный, выездной, комбинированный и т.д.;
* определить – будет ли аудит только системы корпоративной безопасности (бизнес-процессов, связанных с корпоративной безопасностью или где она присутствует) или еще и иных систем организации (бизнес-процессов);
* определить способы получения информации при проведении аудита (изучение документов, беседы, проверка действий в различных ситуациях, наблюдение, тестирование и т.д.);
* учитывать риски для организации при проведении аудита (отвлечение ресурсов, техника безопасности, приостановка отдельных бизнес-процессов и т.д.);
* определить возможность / невозможность пересмотра программы аудита в процессе работы аудиторов;
* учитывать результаты прошлых аудитов корпоративной безопасности (если они были) или результаты аудитов иных систем менеджмента;
* учитывать готовность организации к внедрению системы корпоративной безопасности (при ее отсутствии) или готовность к ее совершенствованию (готовность руководства, наличие финансовых ресурсов и т.д.);
* предусмотреть выделение аудиторам ресурсов для работы (помещения, компьютеры и т.д.);
* определить время работы аудиторов в организации;
* определить процедуры коммуникации аудиторов с руководителями и работниками организации;
* определить способы фиксации аудиторами нарушений (несоответствий) и их документарного подтверждения;
* согласовать программу аудита с заказчиком и с аудируемой организацией (если это разные лица);
* определить процедуры взаимоотношений аудиторов и безопасников организации (иными должностными лицами организации, в чьи должностные обязанности входит корпоративная безопасность);
* учитывать наличие информационно-коммуникационных технологий (например, технических ресурсов, необходимых для проведения дистанционного аудита с использованием технологий, обеспечивающих удаленную совместную работу);
* в процессе аудита проверять и оценивать возможность улучшения системы корпоративной безопасности;
* в процессе аудита проверять соответствие корпоративной безопасности стратегическим направлениям аудируемой организации;
* определить процедуры взаимодействия между аудиторами (при наличии группы аудиторов);
* определить алгоритм решения ситуаций, связанных с конфликтом интересов, возникших в процессе аудита;
* определить алгоритм решения ситуаций, связанных с недостаточной компетентностью аудитора в процессе работы;
* определить будет ли информация, получаемая в процессе аудита, предварительно обсуждаться с должностными лицами организации. А также требуется ли обсуждать с должностными лицами организации предварительные выводы;
* определить возможность устранения недостатков в процессе проведения аудита, требуется ли их указывать в выводах, если они устранены в процессе работы аудитора;
* определить вопросы безопасности аудиторов в процессе их работы на предприятии (личная безопасность, охрана труда и т.д.);
* определить процедуры перемещения аудиторов между территориально разрозненными объектами организации;
* определить требования, связанные с конфиденциальностью и правами доступа аудиторов к информации в процессе работы;
* определить - как будут предоставлены выводы аудита (форма заключения по аудиту);
* определить - кому будет предоставляться отчет об аудите корпоративной безопасности (руководителю организации или заказчику, если это разные лица);
* определить - как будет документироваться информация, полученная в процессе аудита;
* определить требования каких нормативных актов по корпоративной безопасности (законодательство, стандарты, акты вышестоящих организаций, локальные нормативные акты и т.д.) являются обязательными для организации, а какие носят рекомендательный характер;
* определить необходимость совещаний и состав присутствующих на них (открывающее совещание, текущие совещания, заключительное совещание, согласительное совещание и т.д.);
* определить рабочие документы для аудиторов (чек-листы, вопросы для беседы и т.д.);
* определить необходимость использования аудио и видео записей в процессе аудита;
* определить последовательность проведения аудита (по времени, по задачам, по направлениям, по территориально разрозненным объектам и т.д.);
* определить процедуры взаимодействия аудиторов и сопровождающих (наблюдателей);
* определить процедуры проверки информации, предоставляемой аудируемой организацией;
* определить - как будут доказываться выводы аудиторов;
* определить – будут ли в заключении аудиторской проверки предложения по устранению недостатков или о совершенствовании системы корпоративной безопасности;
* определить - будет ли осуществляться контроль за реализацией предложений аудиторов, изложенных в заключении аудита корпоративной безопасности;
* определить алгоритм действий в случаях несогласия должностных лиц аудируемой организации с выводами аудиторов;
* определить возможные действия после аудита (например, осуществление и анализ корректирующих действий, рассмотрение претензий по аудиту, процесс обжалования результатов и т.д.).

*Комплаенс и корпоративная безопасность*

* комплаенс переводится как соответствие (оценка соответствия);
* комплаенс делится на банковский комплаенс (в РФ это соответствие ФЗ-115) и небанковский комплаенс;
* структура комплаенс:
* антикоррупционный комплаенс;
* антимонопольный комплаенс;
* комплаенс в сфере обеспечения конфиденциальности информации;
* комплаенс в сфере защиты персональных данных;
* комплаенс в области промышленной безопасности и охраны труда;
* этический комплаенс;
* комплаенс в области противодействия отмыванию доходов, полученных незаконным путем и служащих для финансирования терроризма;
* комплаенс в области экологии и охраны окружающей среды;
* комплаенс в сфере маркетинга и рекламы;
* санкционный комплаенс
* комплаенс это оценка соответствия:
* требованиям законодательства;
* требованиям государственных регуляторов;
* нормам этики;
* внутренним регламентам и политикам;
* требованиям акционеров и владельцев предприятия
* комплаенс - обеспечение соответствия деятельности организации требованиям, налагаемым на нее российским и зарубежным законодательством, иными обязательными для исполнения регулирующими документами, а также создание в организации механизмов анализа, выявления и оценки рисков коррупционно опасных сфер деятельности и обеспечение комплексной защиты организации;
* существует международный стандарт по комплаенсу ИСО 37301;
* комплаенс в системе риск-менеджмента относится в первую очередь к теме регуляторных рисков;
* комплаенс в отличии от внутреннего контроля и аудита работает не только по прошедшим событиям, но и по предполагаемым. То есть это оценка соответствия планируемых действий требованиям законодательства и нормативным документам;
* комплаенс менеджер в отличие от юристов оценивает не только юридическую сторону, но и оценивает те вопросы, которые выходят за нормы права – этика, социальная ответственность и т.д.;
* в комплаенс применяют такой термин как амбассадор. То есть проповедник и популяризатор идей комплаенс. В западных компаниях термин применяется, в российских его не очень понимают;
* желательно продумать получение информации для функций комплаенс. Это может быть горячая линия, телефон доверия, анкеты, беседы при увольнении и т.д.;
* ответственность комплаенс менеджера в основном только дисциплинарная;
* один из самых сложно создаваемых элементов в комплаенс это санкционный комплаенс. Нужно ли в работе учитывать иностранные санкции или только российские санкции?

**Информация об авторе:**

**Панкратьев Вячеслав Вячеславович –** полковник юстиции в запасе, заведующий кафедрой безопасности в Университете государственного и муниципального управления, эксперт в области корпоративной безопасности, защите активов и управлению рисками. Преподаватель - консультант, автор и ведущий обучающих семинаров и курсов повышения квалификации по тематикам, связанных с корпоративной безопасностью. Опыт преподавания и консалтинга с 1997 года. Автор книг и методических пособий по безопасности предпринимательской деятельности. Независимый консультант. Разработчик методик аудита безопасности предприятия и создания КСБ – корпоративных стандартов безопасности.

**www.vvpankrat.ru**

**vv\_pankrat@mail.ru**

**+7-963-632-41-20**