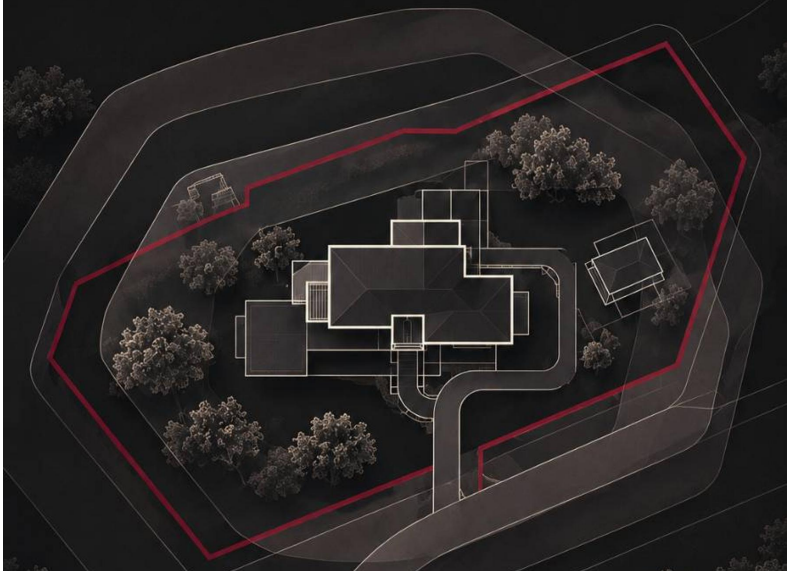
Олег Галямов

ОРГАНИЗАЦИЯ ПЕРСОНАЛЬНОЙ БЕЗОПАСНОСТИ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО



Олег Галямов

Организация персональной безопасности

https://litres.ru/74926982
SelfPub; 2026

Аннотация

Персональная безопасность — это не только личная охрана, высокий забор и бронированный автомобиль. Это система мер, которые должны соответствовать существующим угрозам, образу жизни человека и условиям его деятельности. Для её эффективной работы необходимо, чтобы все участники понимали свои задачи и действовали согласованно.

В практическом руководстве «Организация персональной безопасности» Олег Галямов представляет авторский взгляд на организацию защиты собственников бизнеса, первых лиц и членов их семей. В основе книги — профессиональный опыт автора в сфере безопасности и личной охраны, профильная литература и практические решения, применяемые в России и за рубежом.

Издание адресовано руководителям служб безопасности и подразделений личной охраны, представителям семейных офисов, а также собственникам бизнеса и другим

лицам, принимающим решения по вопросам персональной безопасности.

Содержание

Введение 6
1. Организация системы персональной безопасности 8
1.1. Что входит в систему защиты 8
1.2. Кто обеспечивает защиту 10
1.3. Полномочия на стыке служб 12
1.4. Описание того, что действует на практике 14
2. Анализ угроз и оценка рисков 16
2.1. Какие угрозы имеют значение 16
2.2. Качество исходных сведений 18
2.3. Сценарий, последствия и действующие меры 20
2.4. Шкалы, срочность и неполные данные 22
2.5. Как оценивают остаточный риск 25
3. Информационное обеспечение и конфиденциальность 26
3.1. Сведения, необходимые для работы 26
3.2. Как сообщать об изменениях 29
3.3. Доступ, хранение и прекращение полномочий 31
3.4. Публичная информация и сообщения об инцидентах 34
4. Цифровая безопасность 36

4.1. Цифровые сервисы, от которых зависит защита 36
4.2. Вход, восстановление и сохранность данных 38
4.3. Проверка запросов и распределение прав 40
4.4. Домашние системы и связь с физической защитой 42
4.5. Задача для специалиста по информационной безопасности 45
5. Безопасность мест пребывания 47
5.1. Повседневный режим и границы управления 48
5.2. Квартира в многоквартирном доме 49
5.3. Частный дом и резиденция 51
5.4. Офис и рабочие помещения 55
5.5. Гостиница и временное жильё 58
Конец ознакомительного фрагмента. 59

Олег Галямов
Организация персональной безопасности

Введение

Это руководство посвящено организации персональной безопасности собственников бизнеса, первых лиц и членов их семей. Его задача — систематизировать профессиональные знания и изложить комплексный подход к защите. В руководстве рассматривается, как оценивать угрозы, выбирать меры с учётом образа жизни человека и проверять, насколько эти меры работают на практике.

При подготовке руководства я опирался на свой опыт работы в сфере безопасности и личной охраны, профессиональную литературу и подходы к организации защиты, сложившиеся в России. В руководство также включены отдельные решения из международной практики, применимые в российских условиях.

Руководство адресовано прежде всего руководителям служб безопасности, руководителям подразделений личной охраны, представителям семейных офисов, руководителям компаний и заказчикам, принимающим решения об органи-

зации персональной безопасности.

Оно также может быть полезно телохранителям и другим специалистам, непосредственно участвующим в обеспечении персональной безопасности, для понимания принципов организации защиты и взаимодействия различных служб.

1. Организация системы персональной безопасности

1.1. Что входит в систему защиты

Персональную безопасность организуют с учётом образа жизни, распорядка и характера деятельности конкретного человека. У собственника бизнеса есть деловые встречи, публичные обязанности и частные планы; члены семьи могут жить по другому расписанию и самостоятельно принимать решения. Поэтому прежде всего определяют, кому необходима защита, где и при каких обстоятельствах она должна обеспечиваться.

В зависимости от условий различаются и задачи защиты. В офисе это может быть организация пропускного режима, порядок приёма посетителей и взаимодействие с охраной здания. В частном доме — контроль доступа на территорию, организация работы охраны и взаимодействие с домашним персоналом. При поездках и посещении мероприятий важны актуальная программа перемещений, условия пребывания на объектах и согласованность действий личной охраны с принимающей стороной.

Система персональной безопасности объединяет несколь-

ко взаимосвязанных направлений. К ним относятся безопасность мест пребывания и перемещений, организация личной охраны, информационное обеспечение, цифровая безопасность, технические средства защиты и готовность к происшествиям.

Каждое направление решает собственные задачи, но эффективность защиты во многом зависит от их согласованной работы. Для этого необходимо определить обязанности и полномочия участников, организовать обмен необходимой информацией и установить порядок взаимодействия при изменении обстановки. Особенности каждого направления подробно рассматриваются в последующих главах.

1.2. Кто обеспечивает защиту

Небольшой объём задач не всегда требует создания отдельного подразделения. Помощник может вести календарь, водитель — отвечать за транспорт, управляющая организация — выполнять обязанности по дому, профильный подрядчик — обслуживать оборудование. На отдельное мероприятие личную охрану привлекают по договору. При такой модели особенно важно заранее определить, кто ставит задания, передаёт программу и вправе согласовать изменение объёма услуг.

Корпоративная служба безопасности (СБ) выполняет порученные ей задачи внутри компании: например, организует пропускной режим, работу с подрядчиками, отдельные направления экономической и информационной безопасности. Подразделение личной охраны может входить в СБ либо непосредственно подчиняться собственнику. Если подразделение входит в состав СБ, взаимодействие строится в рамках установленной структуры управления; при непосредственном подчинении собственнику руководителям необходимо отдельно согласовать совместные вопросы — посещение офиса, использование ресурсов компании и привлечение её сотрудников. Полномочия и расходы определяют исходя из фактических задач и правовых оснований (глава 13).

В семейном офисе отдельный сотрудник может вести до-

говоры на обслуживание жилья и поездки семьи. Управляющий резиденцией организует работу домашнего персонала и согласует её с охраной объекта. Частная охранная организация (ЧОО) оказывает охранные услуги по договору, имея лицензию на соответствующий вид деятельности. Техническое обслуживание оборудования выполняют профильные специалисты. Конкретная структура может отличаться, но каждый участник должен знать, что решает самостоятельно, когда требуется согласование и от кого он вправе получать задания.

1.3. Полномочия на стыке служб

Взаимодействие служб удобно рассмотреть на примере обычного рабочего визита. В офис на встречу с собственником приезжает посетитель. Помощник подтверждает встречу, объектовая охрана сверяет сведения о посетителе с согласованной заявкой и обеспечивает его допуск в установленном порядке, при необходимости оформляя пропуск. Личная охрана учитывает предстоящую встречу при организации сопровождения первого лица.

Если посетитель прибывает раньше назначенного времени или встречу переносят в другое помещение, изменения согласовывают с уполномоченным лицом и доводят до всех участников. При этом передача информации сама по себе не даёт сотрудникам права самостоятельно изменять согласованные решения.

По каждой существенной задаче определяют три вещи: кто утверждает порядок, кто его выполняет и кому поручена подмена. Также определяют, в каких случаях сотрудник может самостоятельно приостановить выполнение задачи и когда необходимо обратиться за решением к руководителю. Так, водитель может отказаться выпускать неисправный автомобиль; решение о поездке другим способом принимает уполномоченный человек, располагающий сведениями о неисправности и доступной замене.

Повседневная работа показывает, как устроено взаимодействие, а изменение планов обнаруживает слабые места. Если вопрос решается только личным звонком собственника, следует проверить, достаточно ли у исполнителей полномочий и сведений. Когда два подрядчика полагают, что тревожный сигнал проверит другой, необходимо установить конкретного получателя сообщения и порядок реагирования.

Нового участника включают в эту систему на тех же основаниях.

1.4. Описание того, что действует на практике

Действующую защиту описывают через конкретные процессы: прибытие первого лица в офис, визит подрядчика в дом, вечернее изменение программы. Документы показывают установленный порядок, беседы с участниками — их представление о работе, а согласованное наблюдение — исполнение отдельной операции в определённый момент. Например, инструкция может предусматривать предварительное уведомление охраны о прибытии подрядчика. Однако только сопоставление установленного порядка с фактическими действиями позволяет выяснить, своевременно ли дежурный получает необходимые сведения и соблюдается ли предусмотренная процедура допуска. Эти источники не заменяют друг друга.

Сопоставление позволяет сохранить работающие меры и исправить слабые связи. Если службы ведут несогласованные списки посетителей, нужен порядок обновления сведений. Если после увольнения сотрудника его пропуск продолжает действовать, необходимо выяснить, кто отвечает за прекращение доступа и как проверяется выполнение этой процедуры. Не следует менять исправную функцию лишь потому, что перестраиваются соседние участки системы. Основания для оценки выводов рассмотрены в главе 2, порядок

внедрения — в главе 12.

2. Анализ угроз и оценка рисков

2.1. Какие угрозы имеют значение

Публичность, рабочий распорядок и круг контактов задают разные условия защиты. Руководитель, работающий преимущественно в знакомом офисе, и человек, регулярно выступающий на открытых мероприятиях, сталкиваются с различными обстоятельствами. Поэтому анализ начинают с определения его границ: кого он касается, какие ситуации охватывает и на какой период рассчитан. Затем учитывают характер деятельности, известные конфликты, доступность личных сведений, состав семьи, поездки и возможность получить помощь. Внимания может требовать как адресная угроза, так и совокупность повседневных факторов — например, частые поездки при чрезмерной нагрузке на одного водителя.

Умышленные угрозы включают противоправные посягательства, запугивание, давление, мошенничество и незаконное получение личных сведений. Неумышленные опасные события связаны, в частности, с дорожными происшествиями, пожаром, внезапным ухудшением здоровья, отказами связи и инфраструктуры. Одно событие способно нарушить несколько функций: утрата доступа к календарю и перепис-

ке может одновременно повлиять на подачу транспорта и встречу с принимающей стороной. Зависимость физической защиты от цифровых сервисов рассмотрена в главе 4.

Угрозой в этом руководстве называется обстоятельство или источник, способные причинить вред. Уязвимость — слабое место в условиях или организации защиты, из-за которого вред становится возможным или усиливается. Риск оценивают применительно к определённому событию и его возможным последствиям с учётом действующих мер и неопределённости. Общую логику управления рисками и выбор методов оценки описывают ISO 31000 и IEC 31010. Здесь они используются как методические ориентиры для работы с неопределённостью [1, 2].

2.2. Качество исходных сведений

Достоверность вывода ограничена качеством исходных сведений. Подпись в журнале устанавливает наличие записи о передаче смены, но сама по себе не подтверждает, что сменщик узнал обо всех изменениях. Сообщение руководителя о доступной подмене остаётся сведением с его слов до проверки. Допущением называют условие, временно принятое для анализа: например, ожидаемую доступность резервного сотрудника в определённые дни до уточнения договора.

Профессиональное суждение связывает эти данные с выводом и показывает, от каких условий он зависит.

Сведения сопоставляют по документам, объяснениям уполномоченных участников, результатам согласованных проверок и относящимся к задаче официальным сообщениям. Для документа выясняют дату и область действия. В беседе уточняют, наблюдал ли человек событие сам или пересказывает чужие слова. Даже несколько пересказов одного сообщения не являются независимым подтверждением исходного события.

Подтверждённую угрозу, обоснованное предположение и тревогу заказчика с пока неустановленными основаниями нельзя описывать одинаково. Сам по себе деловой конфликт ещё не подтверждает подготовку нападения, хотя может потребовать внимания. Когда предполагаемые последствия тя-

жёлые, допустимо рассмотреть соразмерную временную защитную меру до завершения проверки. Для неё фиксируют основания, срок и условия пересмотра.

Сбор сведений ограничивают законной целью и полномочиями. Для организационного анализа объекта нередко достаточно информации администрации и официальных открытых данных о его работе. При оценке персонала действуют отдельные требования трудового законодательства и защиты частной жизни. Незаконные базы, доступ к чужой переписке и скрытое наблюдение не относятся к допустимым способам такого анализа. Неустановленные существенные обстоятельства следует обозначать прямо, одновременно указывая, какое решение возможно принять при сохраняющейся неопределённости.

2.3. Сценарий, последствия и действующие меры

Сценарий связывает определённое событие с возможными последствиями и позволяет установить, какие недостатки защиты способствуют развитию опасной ситуации.

Допустим, во время мероприятия посторонний пытается пройти в зону пребывания охраняемого лица без соответствующего разрешения. Попытка несанкционированного прохода — исходное событие; отсутствие установленного порядка проверки допуска и чёткого распределения обязанностей между охраной мероприятия и личной охраной — уязвимость. Риск заключается в возможном причинении вреда охраняемому лицу вследствие бесконтрольного приближения постороннего.

Для оценки такого сценария необходимо выяснить, как организован допуск, кто контролирует проход в соответствующую зону, как распределены обязанности между службами и какие действия предусмотрены при попытке нарушения установленного порядка.

Защитные меры по-разному влияют на развитие сценария. Порядок допуска снижает вероятность ошибочной выдачи доступа, своевременное оповещение позволяет раньше узнать о происшествии, подготовка персонала и доступность профессиональной помощи способны ограничить по-

следствия. Но служба реагирования не сможет выполнить свою задачу, если не получит сообщение или не попадёт на объект. Поэтому оценивают всю необходимую последовательность, а не отдельно взятую меру.

Последствия описывают конкретно: разглашение семейных сведений, тяжёлый вред здоровью, срыв встречи и кратковременная недоступность сервиса требуют разных решений. Если сценарий допускает несколько исходов, указывают, какой определяет срочность и почему. Количественную оценку применяют при наличии пригодных данных и обоснованного способа расчёта; в остальных случаях раскрывают основания качественного суждения.

2.4. Шкалы, срочность и неполные данные

Качественная шкала помогает расставить приоритеты, когда надёжных данных о частоте событий нет. Перед оценкой определяют уровни последствий и признаки актуальности угрозы: например, подтверждённые недавние сведения, повторяющиеся события или изменение обстановки. Матрица делает сопоставление наглядным, но её ячейка отражает выбранные экспертные оценки, а не вычисленную вероятность. Для каждого положения в матрице нужны объяснимые основания.

Рис. 1. Пример качественной матрицы оценки риска

Последствия / актуальность
Низкая
Средняя
Высокая

Тяжёлые
Средний
Высокий
Критический

Существенные
Низкий
Средний
Высокий

Ограниченные
Низкий
Низкий
Средний

Матрица используется для наглядного сопоставления сценариев по тяжести последствий и актуальности угрозы. Приоритеты в ячейках условны: конкретные критерии устанавливают до оценки. Матрица не заменяет профессионального суждения и не означает точного количественного расчёта риска.

Срочность мер не следует смешивать со степенью подтверждения угрозы. Сообщение о возможной опасности может оправдывать временный перенос визита до выяснения обстоятельств. Одновременно учитывают вред от самой задержки, особенно когда от своевременного действия зависит получение помощи. Временное ограничение вводят с заранее определённым сроком и условиями пересмотра.

Сообщение об угрозе конкретному человеку оценивают по содержанию, конкретности, повторяемости и связи с известными событиями. Исходные материалы сохраняют и

ограничивают круг получателей. При признаках непосредственной опасности принимают законные меры для защиты людей и обращаются в компетентные органы. Анализ продолжают с учётом срочности и рекомендаций уполномоченных служб.

Если вывод зависит от одного допущения, проверяют, как он изменится при других условиях. Например, в обычный день дежурная смена охраны резиденции справляется с контролем доступа и приёмом запланированных посетителей. Однако при проведении семейного мероприятия или официального приёма нагрузка на сотрудников возрастает: увеличивается количество гостей, обслуживающего персонала и транспорта, усложняется взаимодействие между объектовой и личной охраной. В таких условиях необходимо оценить, достаточно ли имеющихся сотрудников для выполнения всех задач или потребуется временное усиление.

2.5. Как оценивают остаточный риск

Вывод об оценённом риске должен позволять принять решение. Для существенного сценария показывают установленные обстоятельства, действующие защитные меры, обнаруженные недостатки и возможный вред. Затем объясняют, как предлагаемое изменение повлияет на ситуацию, какие ресурсы для него нужны и в какие сроки оно выполнимо. Временное усиление предусматривает дату или событие, по наступлении которых его необходимость оценивают заново.

Остаточный риск оценивают с учётом уже действующих мер и подтверждённых условий их работы. Эффект ещё не реализованных решений показывают отдельно. Например, подписанный договор о резервном транспорте не означает, что машина доступна в любое время: важны срок подачи и реальная готовность исполнителя. Лицо, принимающее решение, должно знать такие ограничения. При изменении обстановки, происшествии или повторяющемся отказе соответствующие сценарии пересматривают.

3. Информационное обеспечение и конфиденциальность

3.1. Сведения, необходимые для работы

Информационное обеспечение персональной безопасности строится на принципе предоставления каждому участнику только тех сведений, которые необходимы для выполнения его обязанностей. Объём и содержание передаваемой информации зависят от роли сотрудника и характера поставленных перед ним задач.

Например, при организации рабочего дня первого лица сведения распределяются следующим образом:

Объектовая охрана — получает информацию о запланированных посетителях, времени их прибытия и подтверждении принимающей стороны, необходимую для организации допуска.

Водитель — получает сведения о времени и месте подачи автомобиля, запланированных перемещениях и контактах ответственных лиц на случай изменения программы.

Сотрудник личной охраны — получает актуальную программу перемещений, сведения об условиях прибытия и

пребывания на объектах, порядке допуска и контактах представителей принимающей стороны.

Руководитель личной охраны — располагает информацией о запланированных мероприятиях, задачах подразделения, составе дежурных смен и изменениях, способных повлиять на организацию сопровождения.

При этом подробности деловых переговоров, содержание личных встреч и причины частных решений не должны становиться доступными сотрудникам, если эти сведения не требуются для выполнения их обязанностей.

Информационные потоки различаются по назначению. Календари и распоряжения определяют предстоящую работу, сведения о местах пребывания и поездках позволяют организовать её выполнение, а информация об исполнителях необходима для распределения полномочий, допуска и взаимодействия. Отдельную категорию составляют сообщения об угрозах и происшествиях, которые используются для принятия решений и последующего анализа. Поскольку перечисленные категории могут пересекаться, доступ к ним предоставляют с учётом конкретных обязанностей сотрудника.

Например, руководителю службы безопасности могут потребоваться подробные обстоятельства происшествия для оценки ситуации и принятия решений, тогда как водителю достаточно получить информацию об изменении времени подачи автомобиля или пункта назначения.

Ответственность за ведение и обновление расписаний распределяют заранее. Опубликованная деловая программа может находиться в ведении пресс-службы, рабочее расписание сопровождения — обновляться ответственным сотрудником личной охраны, а изменения семейного распорядка — передаваться через уполномоченного представителя семьи. В каждом случае необходимо определить, кто вправе вносить изменения, кому они передаются и где хранится актуальная версия программы.

3.2. Как сообщать об изменениях

При изменении времени или места встречи участникам сообщают, что именно изменилось, с какого момента действует новый план и к кому обращаться при возникновении затруднений. Если изменение существенно влияет на организацию работы, получатель должен подтвердить не только получение информации, но и правильность понимания нового порядка действий. Это позволяет своевременно обнаружить возможные ошибки, например когда водитель неверно понял изменение времени подачи автомобиля.

Способ передачи информации выбирают с учётом её срочности и характера. Изменения, требующие немедленных действий, целесообразно сообщать непосредственно ответственному сотруднику, после чего обновлять рабочее расписание или соответствующую запись. Таким образом, оперативная связь позволяет своевременно согласовать действия, а письменная фиксация — сохранить актуальные сведения для последующих смен.

На случай отказа основного канала связи предусматривают резервный способ передачи информации, известный всем участникам взаимодействия. Его работоспособность необходимо проверять в обычных условиях эксплуатации, включая объекты, где использование мобильных телефонов ограничено.

Предварительные изменения программы следует обозначать как неподтверждённые. Например, если помощник сообщает о возможном переносе встречи, водитель может заранее уточнить возможность изменения времени подачи автомобиля, однако до окончательного подтверждения участники продолжают ориентироваться на действующий план.

Особого внимания требует передача сообщений об угрозах. Такие сведения должны сопровождаться указанием источника, даты получения и степени подтверждения. Если информация впоследствии подтверждается или опровергается, соответствующие изменения доводят до всех участников, решения которых зависели от первоначального сообщения.

3.3. Доступ, хранение и прекращение полномочий

В процессе работы одни и те же сведения могут одновременно находиться в календарях, рабочих чатах, электронных приглашениях, распечатанных документах и у внешних исполнителей. Поэтому порядок обращения с информацией необходимо определять заранее: устанавливать круг получателей, цели передачи, условия хранения и действия с материалами после завершения соответствующей задачи.

Сроки хранения зависят от целей обработки, договорных обязательств и предусмотренных законом требований. Отдельные материалы могут сохраняться для последующего разбора происшествий, однако наличие такой необходимости должно иметь конкретное обоснование. Хранение информационных копий без определённой цели и установленного срока требует самостоятельной правовой оценки [14].

При увольнении сотрудника или прекращении сотрудничества с подрядчиком необходимо организовать передачу его текущих задач и связанных с ними материалов другому уполномоченному лицу. Одновременно проверяют, какие доступы к помещениям, информационным системам и оборудованию были предоставлены исполнителю, после чего обеспечивают их своевременное прекращение или переоформление.

Особое внимание уделяют участию бывшего сотрудника в рабочих чатах, доступу к электронным календарям, документам и системам удалённого управления. При этом блокировка учётной записи не гарантирует прекращения доступа к сведениям, которые ранее были скопированы или переданы на другие устройства. Поэтому порядок возврата, удаления либо законного сохранения таких материалов должен определяться отдельно.

При использовании электронных календарей учитывают возможность автоматической синхронизации между личными и рабочими устройствами, сохранения информации в приглашениях и отображения уведомлений на общедоступных экранах. Если предоставленная подрядчику ссылка открывает доступ к лишним сведениям, его права ограничивают либо передают только информацию, необходимую для работы.

Правила конфиденциальности распространяются не только на сотрудников охраны, но и на членов семьи, помощников, домашний персонал и других участников, располагающих сведениями о частной жизни охраняемого лица.

Например, фотография, опубликованная во время отдыха, может раскрыть текущее местонахождение семьи, особенности её распорядка или состав сопровождающих сотрудников. Поэтому заранее согласуют, какие сведения о детях, местах проживания и поездках не подлежат публичному распространению, в каких случаях необходимо согласование

публикаций и кому следует сообщать о случайном раскрытии информации.

При этом требования конфиденциальности не должны препятствовать передаче необходимых сведений экстренным службам при возникновении обстоятельств, угрожающих жизни или здоровью людей.

Сотрудники должны соблюдать конфиденциальность сведений о семье, распорядке и условиях работы, обсуждая их исключительно с лицами, которым такая информация необходима для выполнения служебных обязанностей. При передаче сообщений и документов следует проверять правильность выбора получателя и соответствие объёма передаваемых сведений его полномочиям.

3.4. Публичная информация и сообщения об инцидентах

Публичная информация может раскрывать значительно больше сведений о человеке, чем предполагает автор публикации. Например, объявление о предстоящем мероприятии, фотографии с указанием местоположения и опубликованная деловая программа в совокупности позволяют установить особенности распорядка и предполагаемые места пребывания первого лица.

Поэтому при подготовке публичных материалов необходимо учитывать не только содержание отдельных публикаций, но и возможность сопоставления содержащихся в них сведений. Пресс-служба, представители семьи и другие уполномоченные лица должны согласовывать порядок и время раскрытия информации с учётом её назначения и возможных последствий для безопасности. При этом официальные сообщения должны оставаться достоверными, а публикацию сведений о частных поездках, когда она необходима, целесообразно по возможности откладывать до их завершения.

Правовые условия использования изображения человека и распространения сведений о его частной жизни рассматриваются в главе 13.

Отдельного порядка требует передача информации о про-

исшествиях. Содержание сообщения определяется ролью получателя и действиями, которые он должен предпринять. Например, сотруднику объектовой охраны могут потребоваться сведения об изменении пропускного режима, руководителю подразделения — подтверждённые обстоятельства происшествия и информация о затронутых функциях защиты, а специалистам, проводящим разбор, — более подробные материалы.

Аналогичным образом различается содержание сообщений, направляемых членам семьи, подрядчикам и компетентным государственным органам. В каждом случае учитывают цель передачи информации, полномочия получателя и требования законодательства. Для обеспечения согласованности действий необходимо подтверждать получение существенных сообщений и определять, какие решения или действия ожидаются от адресата.

4. Цифровая безопасность

4.1. Цифровые сервисы, от которых зависит защита

Современная организация персональной безопасности во многом зависит от цифровых устройств и информационных сервисов. Утрата или блокировка смартфона может привести не только к нарушению связи, но и к потере оперативного доступа к рабочему календарю, переписке, документам и системам управления доступом. Последствия подобных ситуаций особенно существенны, когда выполнение отдельных функций защиты зависит от одного устройства или учётной записи.

Поэтому при организации цифровой безопасности прежде всего определяют, какие устройства, аккаунты и сервисы используются в повседневной работе, кому они принадлежат и какие задачи обеспечивают. Особое внимание уделяют средствам связи, электронной почте, календарям, рабочим документам, системам контроля доступа и сервисам, необходимым для организации перемещений.

Для каждого значимого сервиса необходимо установить порядок предоставления и восстановления доступа, опре-

делить ответственных за его использование и оценить последствия возможного отказа. Такой подход позволяет выявить зависимости, при которых потеря одного устройства или прекращение работы отдельного сервиса способно нарушить сразу несколько процессов.

При этом следует учитывать различия между корпоративной и семейной цифровой инфраструктурой. Управление рабочими устройствами и корпоративной почтой обычно осуществляется организацией, тогда как домашние системы, личные аккаунты и семейные сервисы находятся под контролем собственников либо назначенных ими администраторов. Помощникам, управляющим и другим сотрудникам может требоваться доступ лишь к отдельным функциям, например к рабочему календарю или обмену документами.

Использование общих паролей затрудняет разграничение полномочий и их последующее прекращение, поскольку доступ сохраняется у каждого, кому известны соответствующие учётные данные. Предпочтительнее использовать индивидуальные учётные записи и предоставлять сотрудникам права, необходимые для выполнения конкретных обязанностей. При выборе новых цифровых сервисов следует заранее проверять возможность раздельного управления пользователями, изменения их полномочий и прекращения доступа без нарушения работы остальных участников.

4.2. Вход, восстановление и сохранность данных

Защита цифровых аккаунтов предполагает использование уникальных паролей, своевременное обновление программного обеспечения и применение многофакторной аутентификации там, где она поддерживается. Для наиболее значимых сервисов предпочтительны способы подтверждения личности, устойчивые к фишингу, поскольку обычные коды подтверждения могут быть получены злоумышленниками посредством обмана пользователя. Различия между способами аутентификации и требования к их устойчивости рассматриваются в рекомендациях NIST [3].

Однако надёжная аутентификация должна сочетаться с возможностью восстановления доступа в случае утраты основного устройства. Поэтому заранее выясняют, какие резервные способы подтверждения личности предусмотрены конкретным сервисом, кто уполномочен ими воспользоваться и каким образом можно связаться с администратором, если привычные средства связи недоступны.

Резервные коды и устройства для восстановления доступа следует хранить в защищённом месте, обеспечивая их доступность только уполномоченным лицам. Работоспособность предусмотренных способов восстановления целесообразно периодически проверять с использованием резервно-

го устройства или специально выделенной учётной записи. В корпоративных системах такие действия необходимо предварительно согласовывать с владельцем или ответственным администратором.

Отдельное значение имеет резервное копирование информации. Само наличие копий ещё не гарантирует возможность восстановления работы: необходимо учитывать доступность резервных данных, порядок их использования и время, требуемое для возвращения к обычному режиму.

При организации поездок и сопровождения первого лица дополнительно предусматривают возможность получения необходимых контактов, документов и сведений о программе при отсутствии основного устройства или доступа к сети.

При организации резервного копирования необходимо заранее определить, какие данные требуют сохранения, насколько допустима потеря последних изменений и за какое время должна восстанавливаться работа соответствующих сервисов. Например, если при сбое удалось восстановить рабочий календарь только по состоянию на предыдущий день, потребуется дополнительно уточнить все изменения, внесённые после создания резервной копии. Поэтому эффективность резервного копирования определяется не только наличием сохранённых данных, но и возможностью своевременно восстановить необходимую информацию [4].

4.3. Проверка запросов и распределение прав

Одним из важных условий цифровой безопасности является проверка подлинности распоряжений и запросов, особенно если они поступают неожиданно, требуют срочного выполнения или предполагают изменение установленного порядка работы.

Например, сотрудник может получить сообщение с просьбой предоставить доступ посетителю, передать служебные документы или изменить время подачи автомобиля. Даже если отправитель представляется знакомым человеком, подобные распоряжения при наличии сомнений следует подтверждать через ранее известный и проверенный канал связи. Особую осторожность необходимо соблюдать при запросах паролей, кодов подтверждения и других данных, позволяющих получить доступ к цифровым сервисам: такие сведения не должны передаваться посторонним.

В организации должен действовать понятный порядок, позволяющий сотруднику приостановить выполнение сомнительного распоряжения до подтверждения его подлинности. Это особенно важно в ситуациях, когда отправитель ссылается на срочность, авторитет руководителя или обстоятельства, не позволяющие провести обычное согласование.

Не менее важен регулярный пересмотр предоставленных

цифровых полномочий. Доступ помощников, членов семьи, сотрудников и подрядчиков должен соответствовать их фактическим обязанностям и прекращаться, когда необходимость в нём отпадает. При передаче устройств на обслуживание дополнительно учитывают, какие сведения и функции могут стать доступны техническому исполнителю.

В случае утраты телефона или другого устройства, используемого для работы, необходимо своевременно уведомить владельца соответствующих аккаунтов и уполномоченного администратора. Порядок блокировки устройства, прекращения доступа к сервисам и последующего восстановления работы должен быть определён заранее.

При этом необходимо учитывать, что удаление данных или полный сброс устройства может затруднить установление обстоятельств происшествия. Поэтому решения о подобных действиях принимают с учётом необходимости сохранения значимых материалов, восстановления работы и требований законодательства.

4.4. Домашние системы и связь с физической защитой

Современные системы управления домом позволяют дистанционно открывать двери, управлять домофонией, просматривать изображения с камер видеонаблюдения и получать уведомления о различных событиях. Использование таких решений расширяет возможности управления объектом, но одновременно создаёт зависимость отдельных функций безопасности от цифровых сервисов, электроснабжения и связи.

При вводе оборудования в эксплуатацию необходимо установить, кому принадлежат основные учётные записи, кто вправе предоставлять доступ другим пользователям и каким образом прекращаются полномочия установщиков и обслуживающих организаций. Отдельно определяют получателей сообщений о неисправностях и тревожных событиях, а также порядок взаимодействия с техническими специалистами.

Особое внимание уделяют работе систем при отсутствии интернета или электропитания. Совместно с профильными специалистами выясняют, какие функции сохраняются в подобных условиях, какие становятся недоступными и как должны действовать проживающие, домашний персонал и охрана объекта. При этом технические решения не долж-

ны препятствовать безопасному выходу людей и получению необходимой помощи.

Если домашний персонал использует электронные системы управления, каждому сотруднику открывают доступ только к тем функциям, которые необходимы для его работы. При использовании общих устройств дополнительно определяют порядок их обслуживания, обновления и защиты от несанкционированного доступа.

При смене сотрудника необходимо своевременно прекратить его цифровые полномочия и предоставить необходимые права новому исполнителю, не нарушая работу остальных пользователей. После изменения настроек или состава получателей уведомлений проверяют, поступают ли тревожные сообщения назначенным лицам и сохраняется ли возможность связаться с обслуживающей организацией.

Цифровые происшествия могут непосредственно влиять на физическую безопасность. Например, нарушение работы электронного календаря способно привести к несогласованным изменениям программы перемещений, а отказ домашней системы управления — ограничить доступ к отдельным помещениям или функциям объекта.

В подобных ситуациях руководитель определяет, какие процессы затронуты и какие временные меры необходимы для продолжения работы. Если достоверность рабочего расписания вызывает сомнения, информацию уточняют у организаторов встреч, а при неисправности домашней систе-

мы совместно с обслуживающей организацией устанавливают сохранившиеся функции и допустимый порядок эксплуатации. До блокировки или сброса оборудования необходимо убедиться, что проживающие смогут беспрепятственно входить в помещения, покидать их и получать помощь.

4.5. Задача для специалиста по информационной безопасности

Для решения технических вопросов, выходящих за пределы компетенции руководителя службы безопасности, привлекают профильных специалистов по информационной безопасности. Их работа должна основываться на конкретном задании, в котором определяются проверяемые системы, допустимые действия, ограничения доступа и ожидаемые результаты.

Например, специалисту можно поручить оценить защищённость домашней сети и подключённых к ней систем видеонаблюдения и управления доступом. В рамках согласованного обследования он проверяет настройки безопасности, разграничение прав пользователей, наличие неиспользуемых учётных записей и возможность несанкционированного удалённого доступа. По результатам проверки специалист определяет выявленные недостатки и предлагает меры по их устранению. Все работы проводятся с разрешения владельца систем и в заранее согласованных пределах.

По результатам работы специалист должен представить понятные выводы о проверенных функциях, обнаруженных недостатках и необходимых мерах. При этом важно разграничивать подтверждённые результаты проверки и вопросы, которые не удалось исследовать в рамках согласованного за-

дания.

Если специалист или подрядчик осуществляет постоянное администрирование цифровых систем, отдельно определяют его полномочия, порядок регистрации действий, доступ к техническим журналам и условия передачи управления при прекращении сотрудничества.

Сотрудникам, использующим соответствующие сервисы, предоставляют необходимые инструкции на случай неисправности или потери доступа. Техническая документация, сведения об администрировании и средства восстановления должны храниться в установленном порядке и передаваться заказчику в объёме, предусмотренном договором.

5. Безопасность мест пребывания

Организация защиты места пребывания зависит от того, кто управляет помещением и территорией, обслуживает системы и отвечает на сообщения о происшествиях. В многоквартирном доме часть функций относится к общему имуществу, в частной резиденции их распределяет собственник, а в гостинице — администрация. Условия непосредственного сопровождения согласовывают для каждого объекта отдельно.

5.1. Повседневный режим и границы управления

Повседневная безопасность начинается с разграничения доступа: необходимо определить, кто подтверждает визиты, разрешает проход в общие, служебные и личные помещения и к кому обращаться в отсутствие ответственного. Для членов семьи, работников, гостей и подрядчиков устанавливают разные права, соответствующие характеру их пребывания на объекте.

При выдаче ключей, карт или кодов указывают основание, доступные помещения и срок действия разрешения. Замену работника подрядной организации подтверждает её уполномоченный представитель, а после завершения работ временный доступ прекращают.

Правила доступа не должны препятствовать безопасному выходу людей и прибытию экстренных служб. Поэтому заранее определяют, кто вызовет помощь, обеспечит вход и встретит прибывшую бригаду при пожаре, аварии или необходимости медицинского вмешательства. Требования к эвакуации, дверям и воротам проверяют с профильными специалистами; отдельно предусматривают помощь детям и маломобильным людям. Технические средства защиты рассмотрены в главе 6, подготовка к происшествиям — в главе 10.

5.2. Квартира в многоквартирном доме

Организация безопасности квартиры связана с разграничением ответственности за личное помещение и общее имущество дома. Последнее регулируется жилищным законодательством, поэтому условия пользования подъездами, общими зонами и парковкой, а также порядок встречи экстренных служб уточняют у управляющей организации или другого уполномоченного представителя с учётом действующих решений и договоров [7].

При подготовке защиты выясняют, как организован проход от входа в дом до квартиры и кто контролирует соответствующие участки. В одном жилом комплексе посетителей принимает охрана, в другом действует только домофон, а консьерж может заниматься исключительно обслуживанием здания. Поэтому необходимо различать реальную охранную услугу и присутствие сотрудника, выполняющего другие функции: уточнять, кто организует допуск, принимает сообщения о происшествиях и вызывает помощь.

Для семьи согласовывают порядок допуска гостей, курьеров и домашнего персонала. Плановые посещения подтверждают заранее, а незапланированные — у человека, который вправе разрешить вход. Сотрудникам, встречающим посетителей, передают необходимые сведения и контакт принима-

ющей стороны, не раскрывая подробное расписание и частные привычки семьи.

Если человек постоянно проживает в квартире и пользуется услугами личной охраны, необходимо определить порядок взаимодействия сопровождающих сотрудников с охраной жилого комплекса, если она предусмотрена. В частности, согласовывают условия прохода через общие зоны, порядок допуска сопровождающих и способы связи с ответственными сотрудниками комплекса.

Заранее выясняют, как вызвать и встретить помощь: для этого должны быть известны точный подъезд, этаж, доступный вход и возможность связаться с семьёй. Состояние общих эвакуационных путей и противопожарных систем проверяют уполномоченные специалисты; при обнаружении препятствий обращаются в управляющую организацию, а при необходимости — в компетентные органы. Самостоятельное изменение общего имущества требует соответствующих правовых оснований.

5.3. Частный дом и резиденция

Частный дом может использоваться для постоянного проживания, сезонного отдыха или кратковременного пребывания. Сама категория объекта не определяет необходимый объём охраны: организационную модель выбирают с учётом образа жизни семьи, состава персонала, актуальных угроз и возможности своевременного получения помощи. Существенное значение имеют также подъездные пути, связь, электроснабжение, отопление и водоснабжение.

В доме без постоянной объектовой охраны контроль доступа организуют проживающие или их уполномоченный представитель. Технические средства могут использоваться для обнаружения отдельных событий и передачи тревожных сообщений, однако их эффективность зависит от того, кто получает такие сообщения и какие действия предпринимает.

Если реагирование обеспечивает внешняя служба, заранее уточняют, обслуживает ли она конкретный адрес, в какие часы принимает сообщения, как организован выезд сотрудников и какие сроки прибытия предусмотрены договором. Отдельно согласовывают порядок доступа на территорию резиденции.

На случай неисправностей инженерных систем определяют ответственных за взаимодействие с обслуживающими организациями и порядок обращения за аварийной помощью.

С появлением домашнего и обслуживающего персонала усложняется управление доступом. Управляющий резиденцией, если такая роль предусмотрена, координирует работы, подтверждает посещения подрядчиков и согласует использование жилых и служебных помещений.

При отсутствии управляющего его обязанности распределяют между другими уполномоченными сотрудниками, чтобы вопросы допуска персонала, организации работ и взаимодействия с подрядчиками не оставались без ответственных. При этом каждый исполнитель должен располагать только теми сведениями о семье и резиденции, которые необходимы ему для работы. Вопросы подбора и контроля домашнего персонала подробнее рассматриваются в главе 9.

При наличии постоянной объектовой охраны её основными задачами становятся контроль доступа людей и транспорта, наблюдение за территорией и отдельными участками объекта, приём сигналов технических средств и реагирование на происшествия. Конкретные обязанности сотрудников определяются организацией охраны резиденции и условиями договора.

В повседневной работе сотрудники охраны поддерживают связь с ответственными лицами, сообщают о существенных изменениях обстановки и при необходимости организуют вызов экстренных служб. При этом важно разграничивать охранные и хозяйственные функции: охрана не должна подменять управляющего резиденцией при органи-

зации обслуживания дома или технических специалистов при устранении неисправностей. Порядок предоставления доступа и разрешения спорных ситуаций также устанавливают заранее, чтобы сотрудники не оказывались перед необходимостью самостоятельно выбирать между противоречащими распоряжениями.

Организация безопасности резиденции зависит и от того, находится ли семья дома. Во время проживания особое внимание уделяют соблюдению приватности, приёму гостей, взаимодействию с домашним персоналом и поддержанию установленного режима охраны. В отсутствие собственников на первый план выходят контроль запланированных посещений, своевременное обнаружение неисправностей и взаимодействие с обслуживающими организациями.

Перед возвращением семьи необходимо убедиться, что помещения готовы к проживанию, основные системы функционируют, а существенные изменения, произошедшие за время отсутствия, известны ответственным сотрудникам. Для нештатных ситуаций предусматривают возможность доступа к инженерным помещениям и привлечения специалистов даже при отсутствии основного управляющего.

Отдельного согласования требует взаимодействие объектовой и личной охраны. В зависимости от принятой модели непосредственное сопровождение собственника может продолжаться на территории резиденции либо завершаться после его прибытия домой. Во втором случае объектовая охра-

на продолжает выполнять свои обычные обязанности, но не принимает автоматически функции личной охраны. Поэтому необходимо заранее определить порядок завершения сопровождения, обмена значимой информацией и взаимодействия руководителей соответствующих подразделений. Организация личной охраны подробно рассматривается в главе 8.

5.4. Офис и рабочие помещения

Организация персональной безопасности в офисе зависит от особенностей здания, действующего пропускного режима и распределения ответственности между собственником помещений, управляющей организацией, арендаторами и службами безопасности. Компания может самостоятельно устанавливать правила доступа в принадлежащие ей или арендуемые помещения, однако использование общих зон, парковки и других элементов инфраструктуры требует взаимодействия с администрацией здания.

При организации сопровождения первого лица важно заранее определить, каким образом сотрудники личной охраны взаимодействуют с охраной офисного комплекса, кто отвечает за допуск посетителей и какие условия действуют в отдельных помещениях.

Например, порядок посещения приёмной, переговорных комнат и служебных зон может различаться. Помощник собственника подтверждает запланированную встречу, объектовая охрана организует допуск посетителя по действующим правилам, а принимающий сотрудник обеспечивает его встречу. При изменении программы соответствующая информация своевременно передаётся всем участникам, чья работа зависит от принятого решения.

Необходимо учитывать, что охрана офисного здания и

личная охрана выполняют разные задачи. Первая обеспечивает установленный режим объекта, вторая отвечает за непосредственное сопровождение охраняемого лица. Если для организации защиты требуется дополнительное взаимодействие, например при прибытии собственника, встрече посетителей или сопровождении до автомобиля, соответствующий порядок согласовывают между руководителями служб.

Изменения в работе офисного здания также могут влиять на организацию персональной безопасности. Ремонт входных групп, ограничение доступа к парковке, изменение пропускного режима или проведение массового мероприятия требуют своевременного уведомления сотрудников личной охраны и при необходимости корректировки порядка сопровождения.

Если изменение режима связано с конкретной угрозой, необходимые меры согласовывают с администрацией здания и ответственными руководителями. Особенности подготовки отдельных визитов рассматриваются в § 7.3.

В представительских офисах и помещениях для конфиденциальных переговоров дополнительное значение приобретает защита информации. Доступ к рабочим календарям, сведениям о посетителях, записям видеонаблюдения и материалам переговоров предоставляют с учётом служебных обязанностей. Например, сотруднику, обеспечивающему допуск посетителя, обычно достаточно подтверждения встречи и контакта принимающей стороны, тогда как содержание

переговоров не имеет отношения к его работе.

Вопросы конфиденциальности и защиты цифровой информации подробно рассматриваются в главах 3 и 4, а защита помещений от скрытого технического наблюдения — в § 6.5.

5.5. Гостиница и временное жильё

При организации проживания первого лица в гостинице необходимо учитывать не только комфорт и расположение объекта, но и возможности обеспечения необходимого уровня безопасности. Значение имеют действующий порядок доступа в жилые помещения, организация работы обслуживающего персонала, взаимодействие с администрацией и условия получения помощи в нештатной ситуации.

До прибытия уточняют, кто из представителей гостиницы отвечает за взаимодействие с сопровождающими, какие службы доступны в ночное время и какие дополнительные условия проживания можно согласовать. Деятельность гостиниц и иных средств размещения регулируется, в частности, Правилами, утверждёнными постановлением Правительства РФ № 1912 [8]. Для краткосрочной аренды квартир и частных домов могут действовать другие правовые условия.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, купив полную легальную версию на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.