Безопасность организации - это такое состояние, которое достигается посредством обеспечения и поддержания защищенности ее персонала и жизненно важных интересов организации от внутренних и внешних угроз с целью уменьшения отрицательных последствий нежелательных событий и достижения наилучших результатов деятельности.

Угроза безопасности организации - это событие, действие или явление, которое посредством воздействия на персонал, финансовые, материальные ценности и информацию может привести к нанесению вреда здоровью работников и ущерба организации, нарушению или приостановке ее функционирования.

Обеспечение безопасности организации - это деятельность ее должностных лиц, персонала, специального подразделения по безопасности, государственных правоохранительных органов и иных структур, направленная на предотвращение возможного нарушения ее нормального функционирования.

Система безопасности организации - это комплекс организационно - управленческих, экономических, правовых, социально-психологических, профилактических, пропагандистских, режимных и инженерно-технических мер и мероприятий, направленных на обеспечение безопасности организации и ее персонала. Определяющим и изначальным при формировании системы безопасности является концепция безопасности организации, которая представляет собой свод основных документов, касающихся политики и стратегии безопасности, основных направлений, средств и методов ее обеспечения.

Рассмотрим сущность видов безопасности.

Физическая безопасность объекта - это охрана материальных и финансовых ресурсов от чрезвычайных обстоятельств (пожар, стихийное бедствие, терроризм) и от несанкционированного проникновения на территорию (вандализм, кража, хищение и т. д.). Обеспечение безопасности объектов регулируется Законом РФ от 11.03.1992 N 2487-1 "О частной детективной и охранной деятельности в Российской Федерации" (ред. от 27.12.2009), положениями и инструкциями, разрабатываемыми и вводимыми в действие Службой государственного пожарного надзора и Управления вневедомственной охраны МВД России.

Этот вид безопасности объекта обеспечивается деятельностью сотрудников службы охраны путем соблюдения пропускного объектового и внутриобъектового режимов с применением соответствующих охранных технических средств и систем. К техническим и инженерно-техническим охранным средствам и системам относятся: периметральные охранные системы; системы охранной сигнализации; системы пожарной сигнализации, пожаротушения и оповещения; системы охранного телевидения; системы ограничения доступа; системы управления доступом; средства оперативной связи; защитные инженерные средства (решетки, жалюзи, бронестекла и др.).

Физическая безопасность персонала подразделяется на личную безопасность руководства и ведущих специалистов и безопасность всего персонала в целом.

Личная безопасность руководства и ведущих специалистов - это их физическая охрана, а также охрана жилья и средств передвижения руководителей и ведущих специалистов организации и членов их семей. Личная безопасность обеспечивается целым комплексом оперативных и технических мер по охране лица как в обычных повседневных, так и экстремальных условиях. Проведение мероприятий по обеспечению личной безопасности охраняемого лица регулируется Законом РФ "О частной детективной и охранной деятельности".

Физическая безопасность персонала - это система охраны труда и техники безопасности в организации на основе производственной санитарии и психологии деловых отношений. Безопасные и здоровые условия труда в организации обеспечиваются комплексным взаимодействием как руководства организации, так и, не в последнюю очередь, усилиями самого персонала организации. Системы охраны труда и техники безопасности в организации регламентируются Трудовым кодексом РФ (разд. X), Законом РФ "Об основах охраны труда в Российской Федерации" и нормативными правовыми актами по охране труда.

Экономическая безопасность - это состояние защищенности экономических интересов организации от внутренних и внешних угроз посредством минимизации коммерческих рисков, системы мер экономического, правового и организационного характера, разработанной администрацией организации. Экономическая безопасность характеризуется совокупностью качественных и количественных показателей и включает в себя следующие функциональные составляющие: финансовую, имущественную, валютную, кредитную, политико-правовую и др. Экономическая безопасность выступает материальной основой решения практически всех задач, связанных с функционированием организации.

Информационная безопасность - это охрана каналов поступления, хранения, обработки и передачи информации, защита любых информационных ресурсов по уровням доступа. Защите подлежит любая документационная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты информации устанавливается в отношении конфиденциальной документационной информации собственником информационных ресурсов, т. е. самой организацией.

Результатами реализации угроз информации могут быть: утрата (разрушение, уничтожение), утечка (извлечение, копирование, подслушивание), искажение (модификация, подделка), блокирование.

Существует два основных принципа защиты информации: разделение обязанностей и минимизация привилегий. Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не смог нарушить критически важный для предприятия процесс. Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. При этом высокий уровень информационной безопасности организации обеспечивается целым комплексом административных мер и оперативно-технических мероприятий.

Юридическая безопасность - это охрана прав, порядка и условий осуществления конкурентной предпринимательской деятельности организации в рамках законодательства Российской Федерации. Если рассматривать юридическую защиту более подробно, то условно ее можно подразделить на три основных направления:

- взаимоотношения с органами государственной власти;

- защита от действий недобросовестных партнеров, заказчиков или контрагентов;

- создание условий для успешной производственной деятельности организации.

Интеллектуальная безопасность - охрана прав на научные труды, промышленные образцы, товарные знаки, коммерческие наименования. На основе Гражданского кодекса РФ (ст. 138) "признается исключительное право (интеллектуальная собственность)... юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации. Использование результатов интеллектуальной деятельности и средств индивидуализации может осуществляться третьими лицами только с согласия правообладателя".

Экологическая безопасность - охрана окружающей среды, обеспечение безопасной работы экологически опасных объектов предприятия, предотвращение экологических катастроф. В общем виде вопросы экологической безопасности организаций регулируются соответствующими законами Российской Федерации. Экологическая составляющая безопасности в структуре безопасности предприятия является достаточно специфичным явлением и в основном значимо для предприятий, имеющих экологически опасные производства или занимающихся разработкой недр и т. д.

И наконец, кадровая безопасность - это процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом.

Виды угроз со стороны персонала:

1. Хищение имущества предприятия.

2. Использование ресурсов предприятия в собственных целях.

3. Умышленная порча и уничтожение имущества предприятия.

4. Получение заработной платы за невыполняемую работу.

5. Шантаж компетентностью (я - незаменимый работник).

6. Шантаж полномочиями (концентрация полномочий в одних руках).

7. Торговля коммерческими секретами.

8. Дисциплинарные нарушения.

9. Создание в коллективе невыносимого морально-психологического климата.

Очевидно, что кадровая безопасность занимает доминирующее положение по отношению к другим элементам системы безопасности организации, так как она имеет дело с персоналом, который в любой составляющей первичен.

Около 80% ущерба материальным активам компаний наносится их собственным персоналом. Только 20% попыток взлома сетей и получения несанкционированного доступа к компьютерной информации приходит извне. Остальные 80% случаев спровоцированы с участием персонала компаний.

Также невозможно обойти вниманием и общемировую статистику, применимую и к России: 10 - 15% всех людей являются нечестными по определению, 10 - 15% абсолютно честные, остальные 70 - 80% - колеблющиеся, то есть те, кто поступит нечестно, если риск попасться будет минимальным.

Еще немного американской статистики. Стоимость преступлений, совершенных должностными лицами и работниками американских компаний, в 1980 г. составила 50 млрд долл. США, в 1990 - 250 млрд долл. США, в 1998 - 400 млрд долл. США, в 2002 - 600 млрд долл. США.

Последняя цифра означает, что каждый работник каждой американской организации (в исследовании участвуют частные и государственные учреждения и предприятия) крадет у своего работодателя больше 12 долл. США в день круглый год.

Мошенничество сотрудников стало основной причиной вынужденного закрытия около 100 американских банков за последние 20 лет. 95% ущерба, понесенного в банковской сфере США, образуется при непосредственном участии персонала банков и только 5% - за счет действий клиентов и иных лиц.

Деловая репутация может оцениваться как качественными, так и количественными показателями. В качестве примера количественного показателя можно назвать стоимостную оценку деловой репутации, используемую в российской экономической практике при бухгалтерском учёте нематериальных активов: стоимость деловой репутации определяется как разница между текущей рыночной ценой, предлагаемой продавцу (владельцу) актива при приобретении предприятия как имущественного комплекса (в целом или его части), и стоимостью всех активов и обязательств по бухгалтерскому балансу на дату его покупки (приобретения), т. н. Гудвилл (понятие используемое в зарубежной деловой практике).

В эпоху массовых социальных коммуникаций и глобализации репутационный риск может возникнуть ниоткуда, как черт из табакерки, и развиваться молниеносно.

Поэтому, во-первых, важна скорость получения информации и реакции на нее, иначе информационную повестку будут определять другие. Во-вторых, важно помнить о сигналах, которые в случае кризиса необходимо коммуницировать вовне:

- озабоченность: «видимо, что-то пошло не так, мы сожалеем и озабочены»;

- все под контролем: «руководство все держит под контролем, взаимодействует с властями»;

- решимость: «мы исправим ситуацию, предпримем необходимые шаги, это не повторится».

- Показательна недавняя история с инвалидом-колясочником, которую сотрудники «Аэрофлота» не пустили на рейс. Модель Светлана Нигматуллина, которая возвращалась в Калининград с московской Недели высокой моды, провела шесть часов в московском аэропорту из-за того, что ее коляска была признана слишком тяжелой. В результате домой она все-таки улетела, но на другом рейсе, и потом решала вопрос с поездкой из Калининграда до родного города, так как встречавшие ее уже уехали из аэропорта.

После того как эта история была обнародована, руководство «Аэрофлота» связалось с ней, принесло личные извинения и пригласило на заседание общественного совета, чтобы обсудить, как улучшить сервис для маломобильных пассажиров.

В некоторых случаях компаниям удается даже полностью взять на себя инициативу. Например, эксперты позитивно оценили действия Siemens AG в коррупционном строительном скандале в Бразилии. Компания сама обнаружила признаки нарушений, сообщила об этом властям и активно сотрудничала со следствием.

В каждом кризисе обычно есть возможность для успешного выхода из него, если его искать.

Еще один важный элемент защиты – обратная связь, позволяющая оперативно оценивать эффективность предпринимаемых в кризисной ситуации информационных шагов, КПД пресс-релизов и заявлений компаний.

Иногда первое ощущение, что кризис миновал и можно вздохнуть с облегчением, оказывается обманчивым. То, как компания на практике реагирует на критику, компенсирует убытки или отвечает на жалобы клиентов, может быть поводом для второй волны негатива, проблема может неожиданно вновь разрастись. Поэтому не стоит торопиться закрывать тему и прекращать мониторинг ситуации.

Полезны бывают и отвлекающие маневры. Например, хорошие информационные поводы: получение наград, спонсорские контракты, интервью руководства.

Однако следует всегда помнить, что ситуация может развиваться и по наихудшему сценарию.

Потенциальный масштаб вызовов можно проанализировать на примере киностудии Sony Pictures (владеет брендами Columbia Pictures, MetroGoldwyn-Mayer), которая подверглась в 2014 г. хакерской атаке. Самое первое публичное сообщение Sony Pictures об атаке было успокаивающим: «Мы ведем расследование одной IT-проблемы».

Проблема, однако, оказалась серьезной. Хакеры раскидали по Сети ворохи украденной информации. Стала достоянием гласности внутренняя переписка руководителей студии, финансовая отчетность, коммерческие секреты, график выхода лент – в общей сложности до 100 терабайт информации.

Среди появившихся в свободном доступе данных были телефонные номера более чем 47 тыс. человек, информация о зарплате о более чем 15 тыс. нынешних и бывших сотрудников компании. Оказались украдены 5 фильмов, включая один еще не вышедший в прокат.

Многие СМИ воспользовались утечкой данных Sony Pictures и опубликовали фрагменты внутренней переписки, в том числе те, где обсуждались такие кинозвезды, как Анджелина Джоли, Леонардо Ди Каприо и другие.

Сопредседатель совета директоров компании Эми Паскаль и продюсер Скотт Рудин вынуждены были принести извинения президенту США Обаме за шутки, допущенные ими в личной переписке. В своих письмах они, в частности, шутили о том, какие фильмы могли бы понравиться президенту и приводили в пример картины, главные роли в которых играли чернокожие актеры. С. Рудин извинился перед актрисой Анджелиной Джоли за то, что назвал ее «испорченным ребенком».

Оказалась нарушена работа 75 % серверов компании, были стерты важные данные, на полное восстановление работоспособности систем потребовалось несколько недель. Пришлось разбираться с сотрудниками, данные которых были скомпрометированы.

Sony Pictures, чтобы положить конец использованию в сети информации, полученной в результате кибератак, наняла адвоката и написала грозные предупреждения крупнейшим СМИ. Но эти шаги оказались запоздалыми и только вызвали еще одну волну язвительных комментариев со стороны журналистов.

Из-за угроз хакеров Sony Pictures решила отменить массовый показ фильма «Интервью» (The Interview), в котором рассказывается о попытке покушения на северокорейского лидера. За это решение она подверглась публичной критике со стороны самого президента США, звезд Голливуда и многих политиков. Ведь получилось, что компания пошла на поводу у тер- рористов. Руководству Sony Pictures пришлось отвечать на критику Обамы и оправдываться.

Как выяснилось, ряд своих действий Sony Pictures в спешке толком просто не объяснила. Так, сообщение об отмене показа ленты в крупных сетях все восприняли как полную капитуляцию компании (хотя Sony Pictures, как потом выяснилось, уже вела активные переговоры о прокате «Интервью» через интернет-кинотеатры).

На Западе эксперты говорят, что компании не должны бояться раскрывать информацию о хакерских атаках. Напротив, нужно ясно и оперативно заявлять о своей позиции в отношении интернет-преступников и защиты данных сотрудников, просить помощи у государства и т. д.

Компании активно озабочены укреплением электронной защиты. Это правильно, но эксперты по безопасности, указывая на уроки истории с Sony, рекомендуют менеджерам вообще не пользоваться электронной почтой для обсуждения конфликтных или личных тем, говорить обо всем этом с глазу на глаз.

Уязвимость крупных бизнес-структур иногда связана также с чрезмерной сложностью и устареванием внутренних электронных систем. Здесь рецептом может быть разумное упрощение этих систем и их модернизация.

Еще один вывод: в компаниях должна действовать система уничтожения ненужной информации. «Лишние» электронные письма, чаты – все это дополнительный риск, показывает история с Sony.

Субъектом кадровой безопасности является служба управления персоналом, причем вопросы кадровой безопасности должны решаться на каждом этапе управления персоналом (поиск, отбор, прием, адаптация, развитие, оценка и т. д.). Любое действие менеджера по персоналу на любом этапе - это либо усиление, либо ослабление безопасности компании по главной ее составляющей - по персоналу.

Как показывает практический опыт, обеспечение безопасности организации должно соответствовать следующим принципам:

- непрерывность - осуществление мер по обеспечению безопасности должно быть основано на постоянной готовности к отражению как внутренних, так и внешних угроз безопасности организации. При этом руководители организаций должны ясно осознавать: процесс обеспечения безопасности не допускает перерывов, иначе придется все начинать сначала;

- комплексность - использование всех средств защиты финансовых, материальных, информационных и человеческих ресурсов во всех структурных подразделениях организации и на всех этапах ее деятельности. При этом комплексность реализуется через совокупность правовых, организационных и инженерно-технических мероприятий без их приоритетного выделения;

- своевременность - обеспечение безопасности с использованием упреждающих мер. При этом принцип своевременности предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности, а также разработку эффективных мер предупреждения посягательств на интересы организации;

- законность - обеспечение безопасности на основе законодательства РФ и других нормативных актов, утвержденных органами государственного управления в пределах их компетенции. При этом необходимо иметь в виду, что вопрос дозволенности тех или иных методов обнаружения и пресечения правонарушений в рамках действующего законодательства и большого количества ведомственных подзаконных актов в настоящее время в большинстве случаев остается открытым;

- активность - обеспечение безопасности организации с достаточной степенью настойчивости и с широким использованием маневра имеющихся сил и средств;

- универсальность - обеспечение безопасности посредством применения таких мер и проведения таких мероприятий, которые дают положительный эффект независимо от места их конкретного применения;

- экономическая целесообразность - сопоставление возможного ущерба и затрат на обеспечение безопасности. При этом во всех случаях стоимость системы безопасности должна не превышать размера возможного ущерба от любых видов риска;

- конкретность и надежность - определение конкретных видов ресурсов, выделяемых на обеспечение безопасности. При этом обязательным является достаточное дублирование методов, средств и форм защиты при обеспечении

безопасности организации;

- профессионализм - реализация мер безопасности должна осуществляться только профессионально подготовленными специалистами. При этом в условиях быстрого развития средств и систем безопасности необходимо постоянное совершенствование мер и средств защиты на базе обучения личного состава;

- взаимодействие и координация - осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений, служб и ответственных лиц. При этом вопрос о взаимодействии и координации касается не только подразделений и лиц, непосредственно отвечающих за безопасность, но и их связи с остальными подразделениями организации;

- централизация управления и автономность - обеспечение организационно-функциональной самостоятельности процесса организации защиты всех объектов охраны и централизованное управление обеспечением безопасности организации в целом.

Тесно связана с кадровой безопасностью безопасность труда и здоровья персонала - система обеспечения безопасности жизни и здоровья работников в процессе трудовой деятельности, включающая правовые, социально-экономические, организационно-технические, санитарно-гигиенические, лечебно-профилактические, реабилитационные и иные мероприятия (ст. 1 Основ законодательства РФ об охране труда).

Безопасность организации обеспечивается посредством взаимодействия администрации, подразделения охраны труда и техники безопасности и самого работника. С этой целью в организациях разрабатываются комплексные планы организационно-технических, социально-экономических и психологических мероприятий по обеспечению безопасности организации.

Список использованных источников:

1. Бадалова А. Г., Москвитин К. П. Управление кадровыми рисками предприятия // Российское предпринимательство. 2015. N 7.

2. Управление персоналом организации: Учеб. / Под ред. А. Я. Кибанова. М.: ИНФРА-М, 2016.

3. http://group.interfax.ru/lnt.asp?rbr=11&lnt=3&id=737