МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ

ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

На тему: «Разработка математической модели обеспечения информационной безопасностив модельном бизнесе»

Исполнитель: Чижикова Полина Юрьевна
Руководитель: профессор Бурлов В.Г.

«Кзащите допускаю»
Заведующий кафедрой

_____
(подпись)

_____
(ученая степень, ученое звание)

_____
(фамилия, имя, отчество)

« » _____ 2024 г.

Санкт-Петербург
2024 г.

Оглавление

ВВЕДЕНИЕ

Современный этап общемирового развития характеризуется, особенно в последнее десятилетие, возрастающей ролью информационной сферы. Превращаясь в системообразующий фактор жизни общества, она все более активно влияет на политическую, экономическую, оборонную, личную, имущественную и другие составляющие безопасности.

Сотрудничество и соперничество государств и организаций из традиционной материальной сферы все более отчетливо смещаются в информационную область. Передовые информационные технологии существенно меняют не только структуру отношений, но и образ жизни людей, их мышление, механизмы функционирования семьи, общественных институтов, органов власти. Формирование цифрового общества способствует развитию общественных отношений в информационной сфере. Оно становится действенным фактором развития личности, общества и самого государства. В тоже время широкое распространение некоторых информационных технологий сопровождается проявлением новых угроз конституционным правам и свободам граждан, суверенитету, независимости, государственной и территориальной целостности, образованию, формированию здоровья, полноценной духовной жизни. Эти технологии уже используются для достижения целей в политике, в области обороны государства, в экономике, торговле, рекламе (индустрии моды – модельном бизнесе), активной политической борьбе, оказывая порой разрушительное воздействие на психику людей, в особенности молодежи и детей.

Информационное воздействие становится одним из главных инструментов управления людьми, все больше заменяя физическое воздействие, тысячелетиями считавшееся непременным средством управления. Именно поэтому сейчас как никогда актуален вопрос информационной безопасности во всех сферах деятельности общества.

В современном мире информационная безопасность – жизненно важное и необходимое условие обеспечения сбалансированных интересов человека, организации, предприятия, общества, государства.

Переход страны к рыночным отношениям, возникновение многочисленных частных предприятий различного профиля неминуемо привели к резкому усилению конкурентной борьбы между производителями товаров и услуг. С одной стороны это положительный момент. Однако вместе с добросовестной конкуренцией активизируется и недобросовестная, проявляющаяся в виде жесткой конфронтации с использованием противоправных средств и методов. Основная цель недобросовестной конкуренции заключается в стремлении укрепить свое положение за счет ослабления позиций конкурентов или обмана потребителей. Недобросовестная конкуренция реализуется в форме сбора, похищения и обработки конфиденциальной информации различными путями. Следовательно, защита информации, а также подбор и сохранение команды (коллектива) являются в настоящее время актуальными для любого руководителя.

Одно из важных мест в общей системе безопасности предприятия, модельного агентства, отводится защите информации. Практика деятельности российских и зарубежных предприятий– модельных агентств показывает, что основными положениями по защите информации, которыми необходимо руководствоваться являются следующие:

1. выработка критериев выделения ценной информации и необходимой ее защиты;

2. определение объектов интеллектуальной собственности, подлежащих охране;

3. выбор методов защиты (патентование, авторское право, определение сведений, относящихся к коммерческой тайне);

4. разработка для последующего утверждения перечня сведений, составляющих конфиденциальную информацию;

5. установление правил допуска к сведениям, составляющим конфиденциальную информацию и разработка разрешительной системы;

6. оформление списков лиц (перечней должностей), имеющих право работать с конкретными составляющими коммерческой тайны;

7. определение списка должностей (лиц), уполномоченных классифицировать информацию;

8. установление правил и процедур классификации, маркировки документов и других носителей информации, а также вывод их из сферы ограниченного доступа (рассекречивания);

9. разработка и ввод в действие единого порядка обращения с носителями информации (технология создания, учет, правила работы, хранение, пересылка, транспортировка, размножение, уничтожение);

10. составление плана размещения и учет помещений, в которых после соответствующей аттестации разрешено постоянное или временное хранение носителей конфиденциальной информации, работа с ними, а также проведение закрытых совещаний. Установление единого порядка прохода в эти помещения;

11. при непосредственном участии руководителей структурных подразделений и специалистов, имеющих доступ к конфиденциальной информации, планирование, осуществление и контроль за реализацией мероприятий при проведении всех видов работ, в которых используется закрытая (конфиденциальная, служебная) информация, классифицированные носители;

12. оказание методической помощи руководителям подразделений предприятия (фирмы) в разработке и осуществлении мер защиты сведений в процессе научной, конструкторской, производственной, творческой и иной деятельности. Необходимо конкретно определить какие технологические меры безопасности нужно использовать, какие изменения в технологию надо ввести, какие требования целесообразно включить в условия контракта, какую информацию стоит защищать даже при выходе товара (услуги) на рынок и т.п.;

13. разработка и осуществление совместно со специалистами мер по недопущению разглашения конфиденциальной информациина стадиях:

- оформления материалов, предназначенных к опубликованию в открытой печати, для использования на конференциях, выставках, в рекламной деятельности (аналогичные меры осуществляются в отношении образцов изделий, содержащих конфиденциальную информацию);

- оформление документов (образцов) для передачи заказчику (соисполнителю);

14. организация с участием руководителей и специалистов фирмы защитных мероприятий при испытаниях, хранении, транспортировке, уничтожении продукции, содержащей конфиденциальную информацию;

15. разработка порядка и организации контроля за проведением закрытых совещаний;

16. определение режимных мер приема представителей других фирм, командированных должностных лиц, представителей контрольных органов власти;

17. участие совместно со специалистами предприятия (фирмы) в разработке мер по обеспечению безопасности в процессе использования технических средств обработки и передачи информации – ЭВМ (ПЭВМ), а также системы противодействия техническим средствам промышленного шпионажа;

18. организация охраны предприятия (фирмы), спецпомещений, хранилищ, введение пропускного и внутриобъектового режима (разграничение доступа в помещения);

19. формирование предложений по установке технических средств охраны (ТСО), организация работ по их монтажу, эксплуатации и ремонту;

20. участие в подборке и расстановке сотрудников, допускаемых к конфиденциальной информации, выработке мер по снижению текучести кадров;

21. разработка положений, инструкций, правил, методик по обеспечению режима работы для исполнителей закрытых работ, специалистов информационного отдела (несовершенство разработанных норм – одно из главных обстоятельств утечки);

22. организация и участие в обеспечении лиц, допущенных к конфиденциальной информации (составление программы обучения, прием зачетов по знанию соответствующих требований режима);

23. формирование у сотрудников на плановой основе в процессе организационной и профилактической работы совместно с руководителями подразделений сознательного отношения к обеспечению защиты информации с учетом складывающихся условий обстановки;

24. разработка мер предупреждения несанкционированного уничтожения носителейинформации, в том числе в автоматизированных системах хранения, обработки и передачи информации;

25. контроль исполнения режимных требований: проведение аналитических исследований по оценке надежности принимаемых мер защиты конфиденциальной информации и выработка предложений по повышению эффективности охраны;

26. проведение служебных расследований по фактам нарушения режима обращения с конфиденциальной информацией и другие.

Принимая во внимание изложенное, а также личный опыт работы с организациями модельного бизнеса (модельными агентствами, индивидуальными предпринимателями) в качестве объекта исследования выбрана – деятельность организаций в области защиты информации. Предметом же исследования, через который предполагается улучшать качественные характеристики объекта является система информационной безопасности организации.

ОСНОВНАЯ ЧАСТЬ

ГЛАВА 1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1. Описание области исследования

Деятельность рассматриваемых в исследовании предприятий, которая видна всем через средства массовой информации, цифровые интернет платформы в основной своей массе представляет разного рода модельные фото и видео съемки, а также показы. В сознании большинства модельные съемки и показы воспринимаются исключительно как творческий процесс в индустрии модыи глянца.

Тем не менее, за всем этим, как правило, стоят регламентированные юридические отношения между участниками проводимых мероприятий. «Как правило» – не случайный оборот речи, так как зачастую разыгрывается противоположный сценарий, К примеру, ситуация, которая сложилась в работе модели Энджи Шербурн. Несколько лет назад модель снялась для лукбука бренда Vetements. За эту работу модель сразу получила оплату, при этом формально сотрудничество никак не было оформлено в силу дружественных отношений с брендом и "наивности" 19-летней модели, как она признается на своей странице в Instagram. Так вот, помимо лукбука, Vetements использовал фотографии с той съемки в своих рекламных кампаниях,промо-материалах и в оформлении магазинов и корнеров по всему миру.

На запросы агента модели оплатить использование фотографий бренд отвечал отказом, ссылаясь на отсутствие договора.

В процессе модной творческой съемки обычно участвует целая команда: фотограф, модель, продюсер, стилист, визажист, и это лишь минимальный состав участников. Главные роли, безусловно, принадлежат модели и фотографу, однако все зависит от того, на каких условиях работают участники: в рамках модельного агентства, которое и берет на себя все юридическое сопровождение модели, либо силами творческой команды журнала или бренда. Возникает целый ряд вопросов: имеет ли модель авторские права на изображения с ее участием; принадлежат ли они фотографу,

модельному агентству или вовсе бренду? Какие есть ограничения по использованию изображений?

Фоторедактор журнала «КиноРепортер» Олег Бурнаев,исходя из своего опыта работы, отмечает, что наличие документов обязательно для любого типа съемок:«Если это съемка для лукбука или любая коммерческая съемка с моделью, в любом случае должен подписываться модельный релиз, где модель пишет, что она не против использования ее фотографий в рекламных целях, а все права на их использование прописываются. Для нашего журнала «КиноРепортер» мы всегда берем у наших звезд разрешение на публикацию: сразу во время съемок они подписывают нам бумагу, в которой они дают разрешениена публикацию их фотографий и на использование этих фото на сайтеи в продвижении журнала. Там же и прописано, что никакое другое использование, в том числе коммерческое, невозможно без отдельного согласования со звездой».

Получение разрешений – ключевой момент в процессе съемок, считает и владелец юридической компании «Катков и партнеры» и член Совета Торгово-промышленной палаты Российской Федерации по интеллектуальной собственности Павел Катков:«Для «очистки» прав на фотографии необходимо получить разрешение как минимум у двух лиц. Первое – фотографа, чьим творческим трудом создан данный объект авторского права. Второе – модели, съемки которой осуществляются. При этом права модели довольно специфичны. С одной стороны, кажется, что можно ограничиться разрешением на изображение. Однако в случае, если модель позировала, играла роль, исполняла некий сценарий, то правомерно поставить вопрос о наличии у нее смежного права на исполнениепо аналогии с актерами. Кроме того, отдельной правовой оценки требует вклад остальных участников съемки, таких как продюсер съемки, сценарист, художник по свету. Если этот вклад был творческим, то для «очистки» прав на конечные фотографии необходимо будет получить разрешения и у этих лиц. Что касается совета, который можно дать моделям – это в первую очередь не подписывать, «где галочка», смотреть

документы, а лучше – поручать это грамотному юристу. Ведь единожды подписавшись не глядя, можно за копейки отдать права, которые стоят миллионы».

Взаимодействие профессионалов из разных в сфер в модной съемке характеризуется не только юридическими сложностями оформления отношений сторон, но и тем, что сам процесс организации полон разных непредсказуемых ситуаций, которые сложно предвидеть и обговорить заранее.

Креативный директор российского бренда одежды Cocos Moscow Анастасия Головешко рассказала, что в организации съемок есть масса как правовых, так и этических моментов: «Если фотограф может быть в штате команды бренда, то с моделями не так просто – использование одной модели считается дурным тоном и неуважением к клиенту и покупателю, так как необходимо показать, как выглядит одежда на разных типах фигуры и внешности. К тому же, у съемок довольно плотный график, поэтому сотрудничество с одним модельным агентством становится практически невозможным. Часто мы задействуем девушек и юношей, не закреплённых за каким-либо агентством, иногда это просто друзья и знакомые. Так вот в случае с моделями из агентства ситуация сложнее. При найме они порой не предоставляют свои договоры и не всегда озвучивают условия распространения и использования фотографий и видео. Поэтому могут случаться непредвиденные ситуации, как раз такие, как у бренда Vetements. Иногда модели сами не знают некоторых тонкостей в документации. У нас был подобный случай на практике, когда оказалось, что использовать лицо девушки в рекламных целях запрещено,и это было прописано в ее договоре. В этом случае есть несколько способов урегулировать конфликт интересов: выплатить компенсацию или дождаться окончания договора с модельным агентством. Либо – и это самый простой способ – не использовать всё лицо целиком. Насколько мне известно, если на фотографии или видео не будут фигурировать глаза, то это не считается использованием внешности в рекламных целях».

Очевидно, что только внимательно изучив юридические условия сотрудничества всех участников творческого процесса можно приступать к нему, но ритм жизни порой диктует иные условия. Вот мнение заместителя генерального директора цифрового сервиса n'RIS Валерия Брусникина, в котором предполагается, что одним из способов упростить процесс должно стать внедрение технологических решений,таких как использование смарт-контрактов и сервисов по депонированию всех объектов интеллектуальной собственности, включая фото и видео:«Договоренности между сторонами, безусловно, должны быть скреплены неким соглашением. Причем совершенно неважно, в какой форме будет это соглашение – в бумажном или электронном виде. В современном мире с бешеным темпом жизни бывает достаточно сложно быстро формализовать отношения. Здесь на помощь могут прийти такие сервисы как n’RIS, который позволяет задепонировать объекты интеллектуальной собственности и получить правовую охрану с одновременной публикацией сведений в IPChain – распределённый реестр объектов интеллектуальной собственности, который также может зафиксировать факт договорённостейс обеих сторон. Например, модель могла бы зафиксировать те права, которые она передала агентству или сотрудничавшей с ней компании, а компания или бренд, в свою очередь, задепонировать фотографии, которые являются их интеллектуальной собственностью с соответствующими правами. И дальше уже получить более простой способ урегулирования конфликта».

Очевидно, что все выше описанные ситуации, а также множество других из этой сферы деятельности имеют высокую степень зависимости от того кто из участников процессов и какой информацией обладает, где эта информация хранится и каким образом осуществляется обмен ею, на сколько циркулирующая информация актуальна и истинна.

В такой ситуации целесообразно рассмотреть существующую нормативно-правовую базу, регламентирующую взаимоотношения в деятельности исследуемых предприятий.

1.2. Анализ существующей нормативно-правовой базы.

Деятельность рассматриваемых в исследовании предприятий, не смотря на большую творческую составляющую, осуществляется в рамках законодательства государства, а также международного правового поля.

Те, кто хочет работать и строить карьеру в качестве фотографа, фотомодели, должны очень хорошо разбираться в законах, регулирующих этот вид деятельности. И не важно, где вы хотите работать – в России илиза рубежом. Законы, регламентирующие взаимоотношения заказчик – фотограф – модель, везде примерно одинаковые. Это законы об авторских правах и законы, защищающие изображения гражданина.

Соответственно законодательными актами устанавливается и ответственность участников указанных взаимоотношений, в том числе и области информационной безопасности.

По характеру принимаемых мер за совершаемые действия субъектом можно выделить следующие виды ответственности: материальную, моральную, юридическую (уголовную, административную), политическую, семейную и др.

Уголовная и административная ответственность за правонарушения в области информационной безопасности.

Уголовная ответственность – это наиболее жесткая мера государственного воздействия на лиц, совершивших преступления в области защиты информации, предусмотренная Уголовным кодексом Российской Федерации.

В Уголовном кодексе Российской Федерации, как наиболее «сильно-действующем» законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам защиты информации посвящены прямо или опосредованно более пятидесяти статей.

Известно, что к основным объектам безопасности, в том числе информационной безопасности, относятся: личность – ее права и свободы; общество – его материальные и духовные ценности; государство –

его конституционный строй, суверенитет и территориальная целостность. Следовательно, правонарушения в области информационной безопасности можно также подразделить на преступления против личности, общества и государства, с учетом определенной области деятельности исследуемых предприятий.

К преступлениям против личности можно отнести:

преступления против свободы, чести и достоинства личности – клевета (ст. 128.1);

преступления против конституционных прав и свобод человека и гражданина: нарушение неприкосновенности частной жизни (ст. 137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1), отказ в предоставлении гражданину информации (ст. 140), фальсификация избирательных документов, документов референдума (ст. 142), фальсификация итогов голосования (ст. 142.1), воспрепятствование законнойпрофессиональной деятельности журналистов (ст. 144), нарушение авторских и смежных прав (ст. 146), нарушение изобретательских и патентных прав (ст. 147).

К преступлениям против общества можно отнести:

преступления против здоровья и общественной нравственности: незаконная выдача либо подделка рецептов или иных документов, дающих право на получение наркотических средств или психотропных веществ (ст. 233), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст. 237); незаконное распространение порнографических материалов или предметов (ст. 242), изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1);

преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации (ст. 272), создание, использование

и распространение вредоносных компьютерных программ (ст. 273), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274).

К преступлениям против государства можно отнести:

преступления против общественной безопасностии общественного порядка – заведомо ложное сообщение об акте терроризма (ст. 207);

преступления против основ конституционного строя и безопасности государства: государственная измена (ст. 275), шпионаж (ст. 276), разглашение государственной тайны (ст. 283), незаконное получение сведений, составляющих государственную тайну (ст. 283.1), утрата документов, содержащих государственную тайну (ст. 284);

преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления: отказ в предоставлении информации Федеральному Собранию Российской Федерации или Счетной палате Российской Федерации (ст. 287), служебный подлог (ст. 292), незаконная выдача паспорта гражданина Российской Федерации, а равно внесение заведомо ложных сведений в документы, повлекшее незаконное приобретение гражданства Российской Федерации (ст. 292.1), заведомо ложный донос (ст. 306), заведомо ложные показания, заключение эксперта, специалиста или неправильный перевод (ст. 307), разглашение данных предварительного расследования (ст. 310), разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (ст. 311);

преступления против порядка управления: разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа (ст. 320), приобретение или сбыт официальных документов и государственных наград (ст. 324), похищение или повреждение документов, штампов, печатей либо похищение марок акцизного сбора, специальных марок или знаков соответствия (ст. 325), подделка или уничтожение идентификационного номера транспортного

средства (ст. 326), подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков (ст. 327), изготовление, сбыт поддельных марок акцизного сбора, специальных марок или знаков соответствия либо их использование(ст. 327.1). К экономическим преступлениям в области защиты информации, относящимся к преступлениям против личности, общества и государства, можно отнести: преступления против собственности – мошенничествов сфере компьютерной информации (ст. 159.6), хищение предметов, имеющих особую ценность (ст. 164), производство, приобретение, хранение, перевозку или сбыт немаркированных товаров и продукции (ст. 171.1), незаконное получение кредита (ст. 176), незаконное использование товарного знака (ст. 180), незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183), злоупотребление при эмиссии ценных бумаг (ст. 185), злостное уклонение от предоставления инвестору или контролирующему органу информации, определенной законодательством Российской Федерации о ценных бумагах (ст. 185.1), манипулирование рынком (ст. 185.3) неправомерное использование инсайдерской информации (ст. 185.6), изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг (ст. 186), изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов (ст. 187), незаконный экспорт или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники (ст. 189).

Административная ответственность за правонарушения в области информационной безопасности.

Лица, виновные в нарушении требований (норм) нормативных правовых актов в области информационной безопасности, кроме уголовной ответственности, несут административную ответственность, предусмотренную

законодательством Российской Федерации – Кодексом Российской Федерации (КоАП РФ) об административных правонарушениях.

В Кодексе Российской Федерации об административных правонарушениях ответственность за проступки в области информационной безопасности, касающиеся вопросов неправомерного сбора, хранения, распространения, представления и иных неправомерных действий со сведениями (информацией), прямо или опосредованно определена в следующих статьях: нарушение права гражданина на ознакомление со списком избирателей, участников референдума (ст. 5.1), нарушение порядка представления сведений об избирателях, участниках референдума (ст. 5.4), непредоставление возможности обнародовать опровержение или иное разъяснение в защиту чести, достоинства или деловой репутации (ст. 5.13), предоставление информации, необходимой для проведения коллективных переговоров и осуществления контроля за соблюдением коллективного договора, соглашения (ст. 5.29), нарушение порядка или сроков предоставления сведений о несовершеннолетних, нуждающихся в передаче на воспитание в семью либо в учреждения для детей сирот или для детей, оставшихся без попечения родителей (ст. 5.36), незаконные действия по усыновлению (удочерению) ребенка, передаче его под опеку (попечительство) или в приемную семью (ст. 5.37), отказ в предоставлении информации (ст. 5.39), подделка подписей избирателей, участников референдума (ст. 5.46), незаконные действия по получению и (или) распространению информации, составляющей кредитную историю (персональные данные) (ст. 5.53), неисполнение обязанности по проведению проверки и (или) исправлению недостоверной информации, содержащейся в кредитной истории (кредитном отчете) (ст. 5.54), непредоставление кредитного отчета (ст. 5.55), сокрытие источника заражения ВИЧ-инфекцией, венерической болезнью и контактов, создающих опасность заражения (ст. 6.1), пропаганда наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры,

и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры (ст. 6.13), нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию (ст. 6.17), нарушение авторских и смежных прав, изобретательских и патентных прав (ст. 7.12), нарушение требований законодательства о раскрытии информации организациями, осуществляющими деятельность в сфере управления многоквартирными домами (ст. 7.23.1), утрата материалов и данных государственного картографо-геодезического фонда Российской Федерации (ст. 7.26), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 7.27.1), нарушение порядка ведения реестра контрактов, заключенных заказчиками, реестра контрактов, содержащего сведения, составляющие государственную тайну, реестра недобросовестных поставщиков (подрядчиков, исполнителей) (ст. 7.31), нарушение порядка и (или) сроков возврата денежных средств, внесенных в качестве обеспечения заявок на участие в определении поставщика (подрядчика, исполнителя), порядка и (или) сроков блокирования операций по счету участника закупки, порядка ведения реестра участников электронного аукциона, получивших аккредитацию на электронной площадке, правил документооборота при проведении электронного аукциона, разглашение оператором электронной площадки, должностным лицом оператора электронной площадки информации об участнике закупки до подведения результатов электронного аукциона (ст. 7.31.1), сокрытие или искажение экологической информации (ст. 8.5), нарушение стандартов раскрытия информации субъектами оптового рынка электрической энергиии мощности, розничных рынков электрической энергии (ст. 9.15), управление транспортным средством с нарушением правил установки на нем государственных регистрационных знаков(ст. 12.2), выпуск на линию транспортного средства, не зарегистрированного в установленном порядке, не прошедшего государственного технического осмотра, с заведомо подложными государственными регистрационными знаками, имеющего неисправности,

с которыми запрещена эксплуатация,с установленными без соответствующего разрешения устройствами для подачи специальных световых или звуковых сигналов либо с незаконно нанесенными специальными цветографическими схемами автомобилей оперативных служб (ст. 12.31), изготовление в целях сбыта либо сбыт заведомо поддельных государственных знаков почтовой оплаты, международных ответных купонов, использование заведомо поддельных клише франкировальных машин, почтовых штемпелей или иных именных вещей (ст. 13.10), нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11), распространение информациио свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера (ст. 13.11.1), нарушение правил защиты информации (ст. 13.12), незаконная деятельность в области защиты информации (ст. 13.13), разглашение информации с ограниченным доступом (ст. 13.14), злоупотребление свободой массовой информации (ст. 13.15), нарушение правил распространения обязательных сообщений (ст. 13.17), нарушение порядка представления статистической информации (ст. 13.19), нарушение порядка размещения информации в государственной информационной системе жилищно-коммунального хозяйства (ст. 13.19.1), нарушение правил хранения, комплектования, учета или использования архивных документов (ст. 13.20.), нарушение порядка изготовления или распространения продукции средства массовой информации (ст. 13.21), нарушение порядка объявления выходных данных (ст. 13.22), нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети Интернет (ст. 13.27), нарушение порядка предоставления информации о деятельности государственных органов и органов местного самоуправления (ст. 13.28), неисполнение обязанностей организатором распространения информации в сети Интернет (ст. 13.31), обман потребителей (ст. 14.7), нарушение иных прав потребителей (ст. 14.8), незаконное использование

товарного знака (ст. 14.10), незаконное получение кредита (ст. 14.11), нарушение законодательства об экспортном контроле(ст. 14.20), незаконное получение или предоставление кредитного отчета(ст. 14.29), нарушение установленного порядка сбора, хранения, защитыи обработки сведений, составляющих кредитную историю (ст. 14.30), недостоверное декларирование соответствия продукции (ст. 14.44), нарушение саморегулируемой организацией обязанностей но раскрытию информации (ст. 14.52), непредставление сведений, необходимых для осуществления налогового контроля (ст. 15.6), нарушение требований законодательства, касающихся представления и раскрытия информации на финансовых рынках (ст. 15.19), неправомерное использование инсайдерской информации(ст. 15.21), сокрытие страхового случая (ст. 15.34), нарушение требований законодательства о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком (ст. 15.35), представление недействительных документов при совершении таможенных операций (ст. 16.7), уничтожение, повреждение, удаление, изменение либо замена средств идентификации (ст. 16.11), представление недействительных документов для выпуска товаров до подачи таможенной декларации(ст. 16.17), заведомо ложные показания свидетеля, пояснение специалиста, заключение эксперта или заведомо неправильный перевод (ст. 17.9), разглашение сведений о мерах безопасности (ст. 17.13), непредставление сведений (информации) (ст. 19.7), представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта либо других документов, удостоверяющих личность или гражданство) (ст. 19.18), подделка документов, штампов, печатей или бланков, их использование, передача либо сбыт (ст. 19.23), заведомо ложное заключение эксперта (ст. 19.26), представление ложных сведений при осуществлении миграционного учета (ст. 19.27), нарушение пропускного режима охраняемого объекта (ст. 20.17), нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации (ст. 20.23), незаконное использование

специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности (ст. 20.24), несвоевременное представление сведений об изменениях состава постоянно проживающих граждан или граждан, пребывающих более трех месяцев в месте временного пребывания, состоящих или обязанных состоять на воинском учете (ст. 21.3).

Из выше изложенного следует, что Кодексом определен довольно значительный перечень статей в области информационной безопасности (более шестидесяти), по которым юридическое лицо, должностное лицои физическое лицо может привлекаться к административной ответственности. При этом так же разнообразен перечень ответственностиза проступки в области защиты информации – от предупрежденияДо административного приостановления деятельности на срок до девяноста суток, а также лиц, составляющих протоколы об административных правонарушениях и рассматривающих дела об административных нарушениях и выносящих решения по ним.

Дисциплинарная ответственность за нарушение законодательства Российской федерации в области информационной безопасности.

Дисциплина труда – обязательное для всех работников подчинение правилам поведения, определенным в соответствии с Трудовым кодексом Российской Федерации, иными федеральными законами, коллективным договором, соглашениями, локальными нормативными актами, трудовым договором.

Работодатель обязан в соответствии с трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, коллективным договором, соглашениями, локальными нормативными актами, трудовым договором создавать условия, необходимые для соблюдения работниками дисциплины труда. Важным условием в соблюдении дисциплины труда является наличие в организации правил внутреннего трудового распорядка. Правила внутреннего трудового распорядка – локальный нормативный акт, регламентирующий в соответствии с Трудовым кодексом

Российской Федерации и иными федеральными законами порядок приема и увольнения работников, основные права, обязанности и ответственность сторон трудового договора, режим работы, время отдыха, применяемые к работникам меры поощрения и взыскания, а также иные вопросы регулирования трудовых отношений у данного работодателя (ст. 189 ТК РФ). Для отдельных категорий работников действуют уставы и положения о дисциплине, устанавливаемые федеральными законами. Работодатель поощряет работников, добросовестно исполняющих трудовые обязанности (объявляет благодарность, выдает премию, награждает ценным подарком, почетной грамотой, представляет к званию лучшего по профессии). Другие виды поощрений работников за труд определяются коллективным договором или правилами внутреннего трудового распорядка, а также уставами и положениями о дисциплине.

За особые трудовые заслуги перед обществом и государством работники могут быть представлены к государственным наградам.

За совершенные дисциплинарные проступки, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить дисциплинарные взыскания.

За совершение правонарушений в информационной сфере при исполнении служебных обязанностей возможно наступление дисциплинарной ответственности в соответствии как с законодательством о государственной службе, гак и с трудовым законодательством.

В статье 192 ТК РФ определяются дисциплинарные взыскания, в том числе за нарушения в области защиты информации.

За совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям.

Федеральными законами, уставами и положениями о дисциплине (ч. 5 ст. 189 ТК РФ) для отдельных категорий работников могут быть предусмотрены также и другие дисциплинарные взыскания.

К дисциплинарным взысканиям, в частности, относится увольнение работника по основаниям, предусмотренным п. 5, 6, 9 или 10 ч. 1 ст. 81 ТК РФ, то есть расторжение трудового договора по инициативе работодателя.

Трудовой договор может быть расторгнут работодателем в случаях:

- неоднократного неисполнения работником без уважительных причин трудовых обязанностей, если он имеет дисциплинарное взыскание;

- однократного грубого нарушения работником трудовых обязанностей:

а) прогула, то есть отсутствия на рабочем месте без уважительных причин в течение всего рабочего дня (смены), независимо от его (ее) продолжительности, а также в случае отсутствия на рабочем месте без уважительных причин более четырех часов подряд в течение рабочего дня (смены);

б) появления работника на работе (на своем рабочем месте либо на территории организации-работодателя или объекта, где по поручению работодателя работник должен выполнять трудовую функцию) в состоянии алкогольного, наркотического или иного токсического опьянения;

в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника;

г) совершения по месту работы хищения (в том числе мелкого) чужого имущества, растраты, умышленного его уничтожения или повреждения, установленных вступившим в законную силу приговором суда или постановлением судьи, органа, должностного лица, уполномоченных рассматривать дела об административных правонарушениях;

д) установленного комиссией по охране труда или уполномоченным по охране труда нарушения работником требований охраны труда, если это

нарушение повлекло за собой тяжкие последствия (несчастный случай на производстве, авария, катастрофа) либо заведомо создавало реальную угрозу наступления таких последствий.

Согласно п. 7 ст. 243 ТК РФ за разглашение сведений, составляющих охраняемую законом тайну (государственную, служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, работника можно привлечь к материальной ответственности в полном размере причиненного ущерба. Кроме того, за причиненный ущерб работник может нести материальную ответственность в пределах своего среднего месячного заработка, если иное не предусмотрено ТК РФ или иными федеральными законами.

Следует заметить, что не допускается применение дисциплинарных взысканий, не предусмотренных федеральными законами, уставами и положениями о дисциплине. При наложении дисциплинарного взыскания должны учитываться тяжесть совершенного проступка и обстоятельства, при которых он был совершен.

Не допускается увольнение работника по инициативе работодателя (за исключением случая ликвидации организации либо прекращения деятельности индивидуальным предпринимателем) в период его временной нетрудоспособности и в период пребывания в отпуске.

За нарушение обязательных требований в области защиты информации возможно привлечение к дисциплинарной ответственности в установленном порядке.

Гражданско-правовая ответственность за нарушение законодательства Российской Федерации в области информационной безопасности.

Лица, виновные в нарушении обязательных требований нормативных правовых актов в области информационной безопасности, кроме уголовной, административной и дисциплинарной ответственности, несут гражданско-правовую ответственность, предусмотренную законодательством Российской Федерации – Гражданским кодексом Российской Федерации.

Гражданско-правовая ответственность является видом юридической ответственности, которая устанавливается нормами гражданского права.

Гражданско-правовая ответственность заключается в применении к правонарушителю (должнику) в интересах другого лица (потерпевшего, кредитора) либо государства (предприятия) установленных законом или договором мер воздействия, влекущих для него отрицательные, экономически невыгодные последствия имущественного характера – возмещение убытков, уплату неустойки (штрафа, пени), возмещение вреда.

Гражданско-правовая ответственность является имущественной, носит компенсационный характер и подразделяется на договорную и внедоговорную (в зависимости от основания возникновения обязательства), долевую, солидарную (при множественности должников) и субсидиарную.

Гражданское законодательство предусматривает различные формы ответственности. Ответственность, например, может наступать в форме возмещения убытков (ст. 15 ГК РФ), уплаты неустойки (штрафов, пеней) (ст. 330 ГК РФ), потери задатка (ст. 381 ГК РФ).

Кроме того, Гражданским кодексом предусмотрена защита нематериальных благ, в частности в виде:

- компенсации морального вреда гражданину (ст. 151 ГК РФ);

- защиты чести, достоинства и деловой репутации гражданина (ст. 152 ГК РФ);

- охраны интеллектуальной собственности (часть IV ГК РФ);

- охраны изображения гражданина (ст. 151.1 ГК РФ).

- Гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности. По требованию заинтересованных лиц допускается защита чести и достоинства гражданина и после его смерти.

Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, распространены в средствах массовой информации, они должны

быть опровергнуты в тех же средствах массовой информации. Если указанные сведения содержатся в документе, исходящем от организации, такой документ подлежит замене или отзыву.

Порядок опровержения в иных случаях устанавливается судом.

Гражданин, в отношении которого средствами массовой информации опубликованы сведения, ущемляющие его права или охраняемые законом интересы, имеет право на опубликование своего ответа в тех же средствах массовой информации.

Если решение суда не выполнено, суд вправе наложить на нарушителя штраф, взыскиваемый в размере и в порядке, предусмотренным процессуальным законодательством, в доход Российской Федерации. Уплата штрафа не освобождает нарушителя от обязанности выполнить предусмотренное решением суда действие.

Гражданин, в отношении которого распространены сведения, порочащие его честь, достоинство или деловую репутацию, вправе наряду с опровержением таких сведений требовать возмещения убытков и морального вреда, причиненных их распространением.

Если установить лицо, распространившее сведения, порочащие честь, достоинство или деловую репутацию гражданина, невозможно, лицо, в отношении которого такие сведения распространены, вправе обратиться в суд с заявлением о признании распространенных сведений не соответствующими действительности.

Правила о защите деловой репутации гражданина соответственно применяются к защите деловой репутации юридического лица.

Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. После смерти гражданина его изображение может использоваться только с согласия детей и пережившего супруга,

а приих отсутствии – с согласия родителей. Такое согласие не требуется в случаях, когда:

- использование изображения осуществляется в государственных, общественных или иных публичных интересах;

- изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования;

- гражданин позировал за плату.

Ответственность по гражданскому праву наступает за правонарушение, то есть действие (или бездействие), нарушающее требования закона или договора.

При этом составом гражданского правонарушения называется совокупность общих, типичных условий, наличие которых необходимо для возложения ответственности на нарушителя гражданских прав и обязанностей и которые в различных сочетаниях встречаются при любом гражданском правонарушении. К ним относятся условия:

- противоправное нарушение лицом возложенных на него обязанностей и субъективных прав других лиц;

- наличие вреда или убытков;

- причинная связь между противоправным поведением правонарушителя и наступившими вредоносными последствиями;

- вина правонарушителя.

Способы защиты гражданских прав (ст. 12 ГК РФ) могут осуществляться путем признания права; восстановления положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения; признания оспоримой сделки недействительной и применения последствий ее недействительности, применения последствий недействительности ничтожной сделки; признания

недействительным акта государственного органа или органа местного самоуправления; самозащиты права; присуждения к исполнению обязанности в натуре; возмещения убытков; взыскания неустойки; компенсации морального вреда; прекращения или изменения правоотношения; неприменения судом акта государственного органа или органа местного самоуправления, противоречащего закону; иными способами, предусмотренными законом.

Законом или договором может быть установлена обязанность причинителя вреда выплатить потерпевшим компенсацию сверх возмещения вреда.

За нарушение обязательных требований в области информационной безопасности возможно привлечение к гражданско-правовой ответственности. При этом меры гражданско-правовой ответственности предусмотрены в общем виде в законодательстве в области защиты информации и в Гражданском кодексе Российской Федерации.

В соответствии с ч. 2 ст. 17 Федерального закона «Об информации, информационных технологиях и о защите информации» лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

При этом требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования защиты информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

Согласно ч. 3 ст. 17 вышеприведенного Федерального закона в случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность

за распространение такой информации не несет лицо, оказывающее услуги: по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений; по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

В статьях 1100 и 1101 ГК РФ определено, в частности, что компенсация морального вреда осуществляется в случаях, когда вред причинен распространением сведений, порочащих честь, достоинство и деловую репутацию. Компенсация морального вреда осуществляется в денежной форме и независимо от вины причинителя вреда. Размер компенсации морального вреда определяется судом в зависимости от характера причиненных потерпевшему физических и нравственных страданий, а также степени вины причинителя вреда в случаях, когда вина является основанием возмещения вреда. При определении размера компенсации вреда должны учитываться требования разумности и справедливости.

Характер физических и нравственных страданий оценивается судом с учетом фактических обстоятельств, при которых был причинен моральный вред, и индивидуальных особенностей потерпевшего.

Гражданско-правовая ответственность за правонарушения в информационной сфере подразделяется на договорную и внедоговорную.

Договорная ответственность возникает при нарушении условий договора, которым предусмотрены санкции, прямо не обеспеченные нормами действующего законодательства. Внедоговорная ответственность возникает при причинении личности потерпевшего или его имуществу вреда, который не связан с неисполнением нарушителем договорных обязательств.

Внедоговорную ответственность обычно именуют деликтной. Примером деликтной ответственности будут являться меры по возмещению вреда, причиненного вследствие недостоверной или недостаточной информации о товаре (работе, услуге), предусмотренные ст. 1095 ГК РФ.

Для наступления ответственности должны существовать специфические основания. Применительно к гражданско-правовой ответственности такими основаниями будут являться условия, образующие в совокупности состав гражданского правонарушения. Эти условия были приведены выше.

Таким образом, юридическая ответственность, установленная в нормативных правовых актах Российской Федерации, играет важную роль в обеспечении выполнения обязательных требований (норм) в области информационной безопасности, определенных в нормах права.

Знание норм права в области юридической ответственности (уголовной, административной, гражданско-правовой, дисциплинарной) гражданами, юридическими и физическими лицами позволит им значительно уменьшить или исключить риски.

1.3. Факторы, влияющие на защиту информации в процессе деятельности предприятия (модельного агентства).

Информация (ГОСТ Р ИСО/МЭК 27000-2021 идентичен ISO/IEC 27000:2018, IDT).

Информация, согласно положениям указанного ГОСТ – это актив, который наряду с другими важными активами представляет собой огромную ценность для бизнеса предприятия (организации) и, следовательно, должен быть надежно защищен. Информация может существовать, особенно в современном мире, в различной форме, в том числев цифровом формате (например, в виде файлов с данными, записанныхна электронных или оптических носителях), в материальном виде (например, быть записанной или напечатанной на бумаге), а также в нематериальномвиде – знания сотрудников. Информация может передаваться различными способами: с помощью курьера, систем электронной почты или голосовой связи. Независимо от формы и способа передачи информации она должна быть надежно защищена.

Во многих организациях существует зависимость между информацией и информационно-коммуникационными технологиями (ИКТ). ИКТ-технологии являются важнейшим элементом любой организации. Они

облегчают создание, обработку, хранение, передачу, защиту и уничтожение информации.

Информационная безопасность (ИБ).

ИБ обеспечивает конфиденциальность, доступность и целостность информации. Чтобы гарантировать успешное ведение бизнеса в долгосрочной перспективе и свести к минимуму негативное воздействие, ИБ предусматривает применение и администрирование соответствующих мер обеспечения ИБ, учитывающих широкий диапазон угроз.

Таким образом, под **ИБ** целесообразно **понимать** состояние защищенности личности, организации (предприятия – модельного агентства), общества и государства, их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.

К факторам, оказывающим существенное влияние на состояние информационной безопасности организации в современных условиях целесообразно отнести:

- недостатки в организации обеспечения защиты информации;

- недостаточно проработанные требования к защите информации, неверный выбор программных продуктов, неточная система мониторинга;

- несоблюдение требований по защите данных, установленных регуляторами;

- неэффективная организация контроля защиты данных, отказ от создания службы внутреннего контроля, ведения журналов учета действий пользователей;

- ошибки персонала, администраторов, компаний, оказывающих IT-услуги;

- ошибки при использовании технических и программных средств.

Соответственно **обеспечение информационной безопасности** есть не что иное, как осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных

мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угрози ликвидации последствий их проявления.

ИБ достигается посредством внедрения соответствующих **мер обеспечения ИБ**, определенных в ходе выбранного процесса управления и создаваемой системы управления информационной безопасностью. Говоря языком ГОСТ-ов – **менеджмент рисков** и **система менеджмента информационной безопасности** (СМИБ).

Данные меры охватывают политику, процессы, процедуры, организационные структуры, программное и аппаратное обеспечение и предназначены для защиты идентифицированных информационных активов. Меры обеспечения ИБ необходимо определить, внедрить, проверить, проанализировать и при необходимости улучшить, чтобы гарантировать соответствие уровня ИБ бизнес-целям организации. Меры обеспечения ИБ должны быть интегрированы в бизнес-процессы организации.

Менеджмент.

Менеджмент представляет собой**действия по управлению организацией**,ее контролю и непрерывному совершенствованию в рамках соответствующих структур. Такая деятельность охватывает мероприятия (процессы), методыили практики формирования и обработки ресурсов, обращения с ресурсами, наблюдения за ними, а также управления ими. Масштаб управленческой структуры исследуемого предприятия, из личного опыта сотрудничества, варьируется от одного человекав небольших организацияхдо управленческой иерархии, состоящей из многих людей, в крупных организациях.

Применительно к СМИБ действия включают в себя наблюдение и принятие решений, необходимых для достижения бизнес-целей посредством защиты информационных активов организации. **Менеджмент или управление ИБ выражается** через формулирование и использование политик ИБ, стандартов, процедури рекомендаций, которые применяются повсеместно в организации всеми лицами, связанными с ней.

Система менеджмента (система управления).

Система менеджмента (управления) использует совокупность ресурсов для достижения целей организации. Она включает в себя организационную структуру, политику, планирование действий, обязательства, методы, процедуры, процессы и ресурсы.

В части ИБ система управления позволяет предприятию (организации, агентства):

а) удовлетворять требования безопасности потребителей и других заинтересованных сторон;

б) совершенствовать планы и деятельность организации;

в) обеспечивать соответствие целям ИБ организации;

г) соответствовать требованиям регулирующих и законодательных органов, а также отраслевым нормативным документам;

д) управлять информационными активами системным образом, чтобы упростить процессы непрерывного совершенствования и регулирования текущих организационных целей.

В рамках СМИБ организация должна выявить **риски**, связанные со своими информационными активами. Чтобы обеспечить ИБ, необходимо управлять рисками и учитывать относящиеся к угрозам физические, человеческие и технологические риски, применимые к любым формам информации внутри организации или используемые ею.

Внедрение СМИБ является стратегическим решением для организации. Необходимо сделать эту систему неотъемлемой частью организационной структуры организации, постоянно оценивать и обновлять в соответствии с текущими потребностями.

На разработку и внедрение СМИБ влияют задачи, цели, размер и структура организации, требования безопасности и используемые бизнес-процессы. То есть некоторая совокупность факторов. Разработка и функционирование СМИБ должны отражать интересы и требования ИБ всех

заинтересованных сторон организации, включая клиентов, поставщиков, деловых партнеров, акционеров и других третьих лиц.

Во взаимосвязанном мире информация и относящиеся к ней процессы, системы и сети составляют критически важные бизнес-активы. Организации, а также их информационные системы и сети сталкиваются с угрозами безопасности из широкого диапазона источников, включая компьютерное мошенничество, шпионаж, саботаж, вандализм, а также пожар и наводнение.

Повреждения информационных систем и сетей, вызванные вредоносным кодом, действиями хакеров и компьютерных атак типа "отказ в обслуживании", становятся более распространенными и более масштабными, а сами компьютерные атаки – все более изощренными.

СМИБ имеет огромную важность, как для государственного, так и для частного секторов бизнеса. В любой отрасли **СМИБ является фактором**, способствующим поддержке электронного бизнеса, а также важным компонентом мероприятий по управлению рисками. Взаимодействие общедоступных и частных сетей, а также совместное использование информационных активов повышают сложность управления доступом к информации и ее обработкой. Кроме того, широкое использование мобильных устройств хранения данных, на которые записываются информационные активы, способно ослабить эффективность традиционных средств управления. Когда организация внедряет семейство стандартов СМИБ, она может продемонстрировать деловым партнерам и другим заинтересованным сторонам свою способность последовательно применять широко известные принципы ИБ.

При проектировании и разработке информационных систем не всегда учитываются аспекты ИБ. Кроме того, ИБ зачастую считают сугубо технической задачей. Однако уровень безопасности, достигаемый с помощью технических средств, недостаточно высок. Подобная защита может быть неэффективной, не будучи поддерживаемой соответствующими мерами обеспечения ИБ и процедурами в контексте СМИБ. Последующее встраивание

системы безопасности в информационную систему бывает трудным и дорогостоящим. СМИБ включает в себя идентификацию имеющихся мер обеспечения ИБ и требует тщательного планирования и внимания к деталям. Например, средства управления доступом, которые могут быть техническими (логическими), физическими, административными (организационными) или их комбинацией, гарантируют, что доступ к информационным активам разрешен, но ограничен на основании потребностей бизнеса и требований безопасности.

Внедрение СМИБ имеет большое значение для защиты информационных активов, позволяя организации:

а) повысить гарантии того, что ее информационные активы в достаточной мере и на постоянной основе защищены от угроз ИБ;

б) поддерживать структурированную и всестороннюю систему идентификации и оценки угроз ИБ, выбора и применения соответствующих мер обеспечения ИБ, измерения и улучшения их эффективности;

в) непрерывно улучшать среду средств управления;

г) обеспечивать соответствие нормативным и регулятивным требованиям.

Чтобы успешно внедрить СМИБ и, таким образом, решить поставленные бизнес-задачи, следует учесть множество **критически важных факторов, к которым относятся:**

а) политика ИБ, цели и действия, ориентированные на решение поставленных задач;

б) методика и структура для разработки, внедрения, мониторинга, поддержки и улучшения ИБ, согласующиеся с корпоративной культурой;

в) значительная поддержка и заинтересованность со стороны всех уровней управления, в особенности высшего руководства;

г) понимание требований информационной защиты активов, достигаемое через применение менеджмента рисков ИБ (**риск информационной безопасности** (information security risk) – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации (ИСО/МЭК 27005);

е) эффективное просвещение персонала и других причастных сторон по вопросам ИБ, проведение тренингов и обучающих программ, доведение до сведения сотрудников их обязательств в сфере ИБ, сформулированных в политике ИБ, информации о стандартах и т.д., а также мотивирование сотрудников к соответствующим действиям;

ж) эффективный процесс управления инцидентами ИБ;

з) эффективный управленческий подход к обеспечению устойчивости и непрерывности бизнеса;

и) использование системы измерения, позволяющей оценивать управление ИБ;

к) поступление предложений по улучшению в формате обратной связи.

СМИБ увеличивает вероятность того, что организация будет последовательно реализовывать важнейшие факторы успеха, необходимые для защиты ее информационных активов.

ГЛАВА 2. ОПИСАНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТИПОВОГО МОДЕЛЬНОГО АГЕНТСТВА

Рассмотрение содержания предмета и объекта исследования делает очевидной целесообразность создания системы информационной безопасности деятельности организации (предприятия, модельного агентства). Функционирование создаваемой системы имеет смысл описать посредством математической модели.

При этом:

под **угрозой информационной безопасности** понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

под **уязвимостью**, являющейся источником угрозы, – свойство информационной системы, обусловливающее возникновение угрозы безопасности обрабатываемой в ней информации;

под **атакой** – попытка преодоления системы защиты информационной системы, т.е. попытка реализации угрозы, создаваемой уязвимостью.Естественно, что атака предполагает использование (эксплуатацию) уязвимостей.

С учетом того, что под безопасностью информации понимается состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность, имеет смысл соответствующим образом **классифицировать угрозы:** угроза конфиденциальности информации, угроза целостности и доступности информации; и **атаки:** по реализуемым целям осуществления несанкционированного доступа (НСД). Под НСД понимается доступ к информации или к ресурсам информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа. Т.е. несанкционированный доступ – это результат атаки, реализуемой

с некоторой целью, соответственно, с целью раскрытия конфиденциальности информации, нарушения ее целостности или доступности.

Большинство известных подходов к моделированию, отличающихся тем, какие параметры при моделировании ими используются в качестве входной информации и какие характеристики моделируемой системы рассчитываются и поступают на выход модели (строятся модели с использованием теории вероятностей, случайных процессов, сетей Петри, теории автоматов, теории графов, нечетких множеств, теории катастроф, энтропийного подхода и др.), предполагает использование в качестве **простейшего элемента безопасностиугрозу атаки** на информационную систему.

С использованием в качестве простейшего элемента безопасности угрозы атаки связан ряд принципиальных недостатков. Практическая применимость подобных моделей крайне осложняется в виду необходимости экспертного задания ключевой характеристики безопасности – вероятности возникновения угрозы атаки. При моделировании, основанном на использовании в качестве простейшего элемента безопасности угрозы атаки, возникновение различных угроз атак рассматривается в качестве независимых событий, исходя из чего используются соответствующие расчетные формулы. Однако подобный исходный посыл некорректен, т.к. реальные угрозы атак создаются выявляемыми в системе уязвимостями, при этом событиявозникновения угроз атак, как правило, зависимы по уязвимостям, поскольку многимиатаками эксплуатируются одни и те же уязвимости. Например, подавляющая часть угроз атак предполагает внедрение и последующее исполнение на защищаемом компьютере вредоносной программы: используется уязвимость системы, позволяющая исполнять создаваемые в процессе работы интерактивными пользователями файлы. Все эти угрозы атак зависимы по данной уязвимости, рассмотрение их возникновения как независимых событий не позволяет построить корректную математическую модель. Важным является и то, что оперируя при моделировании не **простейшим элементом** безопасности, каким является **уязвимость** (соответственно **угроза уязвимости**), аугрозой

атаки, невозможно обосновать требования к входным параметрам построенной модели. На практикепо причине простоты построения соответствующих моделей, как правило, используются марковские процессы (потоки без последействия). При проектировании системы защиты информационной системы важно то, что в конечном счете системой защита от угроз атак реализуется нивелированием именно соответствующих уязвимостей, создающих эти угрозы атак. При этом, поскольку, как правило, угроза атаки создается некоторой совокупностью угроз уязвимостей, существуют альтернативные варианты решения задачи защиты, как следствие, можно говорить об оптимизационной задаче при проектировании системы защиты информации.

Следовательно, можно сделать вывод о том, что в качестве **простейшего элемента безопасности** информационной системы следует рассматривать **уязвимость** (**угрозу уязвимости**), что логично, т.к., в конечном счете, угроза атаки создается выявляемыми в системе уязвимостями.

Под потенциальной угрозой уязвимости для информационной системы понимаем угрозу, возникновение которой потенциально возможно в системе, под реальной же – реально возникшую угрозу (угроза присутствует в системе, соответствующая уязвимость выявлена и не устранена).Угроза атаки, которая также может быть охарактеризована как потенциальная и реальная, как правило, создается соответствующей совокупностью угроз уязвимостей.

Например, угроза атаки на повышение привилегий создается следующей совокупностью угроз уязвимостей:

возможность несанкционированной установки на компьютер интерактивным пользователем (под его учетной записью без ведома пользователя) вредоносной программы, в том числеиз внешней сети (технологическая уязвимость);

выявление в программном системном средстве, запускаемом с системными правами, ошибки программирования;

возможность исполнения созданного интерактивным пользователем в процессе работы файла (технологическая уязвимость);

невозможность задания разграничений прав доступа к файловым объектам для процессов, запускаемых с системными правами (технологическая уязвимость), далее в зависимости от цели атаки.

Атака при этом состоит во внедрении нарушителем вредоносной программы, ее запуск с системными правами, реализация несанкционированного доступа с какой-либо целью к файловым объектам, используемым в системе для хранения конфиденциальных данных, в обход разграничительной политики доступа, реализуемой системой защиты для интерактивных пользователей.

То есть вырисовывается некоторая модель действий атаки на систему информационной безопасности.

На этом же примере возможно проиллюстрировать и реализацию системы защиты применительно к нивелированию отдельных угроз уязвимостей. Системой защиты может:

предотвращаться возможность установки на компьютер исполняемых файлов;

предотвращаться возможность исполнения созданных интерактивными пользователями файлов, в том числе и с системными правами;

быть реализована разграничительная политика доступа к файловым объектам для процессов, запускаемых с системными правами.

Как видно, задача нивелирования угрозы атаки при реализации системы защиты в любом случае сводится к задаче нивелирования какой-либо угрозы уязвимости. Следовательно, при проектировании системы защиты необходима оценка актуальности для нивелирования ее системой защиты именно угрозы уязвимости, естественно, применительно к актуальной угрозе атаки.

С точки зрения последующего моделирования важным является необходимость учета того, что в общем случае в системе одновременно может

присутствовать несколько выявленных и не устраненных однотипных уязвимостей – реальных угроз уязвимости.

2.1 Стохастические параметры угрозы уязвимости.

Информации в открытых источниках о выявляемых и устраняемых уязвимостях достаточно. Используя данную статистику, возможно определить соответствующие стохастические параметры угрозы уязвимости: **интенсивность возникновения** (выявления) $\boldsymbol{\lambda}$ и **интенсивность устранения** $\boldsymbol{\mu}$,и построить соответствующую **математическую модель**, позволяющую **определять вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозы уязвимости** $P_{0y} = f(\lambda, \mu)$. Данная характеристика угрозы уязвимости может позиционироваться в качестве количественной оценки ее актуальности.

В отношении угрозы уязвимости информационная система в определенном смысле может рассматриваться как система с отказами и восстановлениями характеристики безопасности. Отказом здесь выступает выявление уязвимости ($\boldsymbol{\lambda}$), а восстановлением –устранение выявленной уязвимости ($\boldsymbol{\mu}$).

Целесообразно проанализировать, что собою представляют уязвимости, выявление которых в системе создает реальную угрозу атак. Как уже отмечалось, возникновение уязвимости в информационной системе может быть вызвано двумя причинами: отсутствие, либо некорректность решения соответствующей задачи защиты, либо ошибки реализации средств информационной системы, например, ошибки программирования, которые могут эксплуатироваться нарушителем для обхода защиты. В качестве параметров угрозы уязвимости рассматривается интенсивность возникновения уязвимости $\boldsymbol{\lambda}$ и интенсивность устранения уязвимости $\boldsymbol{\mu}$. Под возникновением уязвимости естественно понимается ее выявление нарушителем безопасности.

В общем случае интенсивность возникновения уязвимости $\boldsymbol{\lambda}$ по прошествии некоторого времени будет снижаться, поскольку в первую

очередь нарушителем будут выявляться наиболее простые недочеты функциональной реализации защиты и ошибки в программном обеспечении (увеличение сложности выявления уязвимости естественно приведет к снижению интенсивности λ). В отношении же параметра **μ** можно сказать, что он никак не связан со сложностью выявления уязвимости нарушителем безопасности, определяется исключительно типом уязвимости (например, ошибки в системных драйверах и в приложениях требуют различной трудоемкости исправления), т.е. для каждого типа уязвимости можно принять: ***μ = const.***

2.2 Характеристика безопасности – стационарный коэффициент готовности.

Если допустить, что спроектирована система защиты, с применением формальной экстраполяции (прогнозная экстраполяция здесь мало применима ввиду высокой интенсивности переходов на новые версии программных средств в современныхинформационных системах) с использованием марковской модели, то поток без последействия, т.е. интенсивностивозникновения уязвимости λ и устранения уязвимости **μ** будут неизменными

в процессе последующей эксплуатации защищенной информационной системы. Очевидно, что с учетом изложенного ранее (что значение λ будет только уменьшаться, а μостанется неизменным в процессе последующей эксплуатации системы), используя подобную модель, возможно определить граничные (при худших для системы условиях) значения требуемых характеристик, учет которых гарантирует, что "хуже не будет". На самом же деле, определения значений именно таких характеристик при проектировании системы защиты в предположении невозможности корректного прогнозирования изменения их значений во временине требуется (нельзя же проектировать систему защиты, оперируя заниженными значениями параметров уязвимости). Вот если бы последействие приводило к увеличению λ в процессе эксплуатации

информационной системы, тогда другое дело, подобное последействие при моделировании необходимо было бы в обязательном порядке учитывать.

Отсюда можно сделать важный вывод о том, что при моделировании характеристик угрозы безопасности информационной системы могут использоваться марковские модели, которые позволяют в данном случае определять граничные значения характеристик безопасности, которые и должны использоваться при проектировании системызащиты в предположении невозможности построения корректного прогноза в отношении изменения значений параметров угроз уязвимостей во времени.

С учетом того, что вероятностью одномоментного появления в системе нескольких однотипных уязвимостей (не одновременного присутствия, именно возникновения реальных угроз уязвимостей) можно пренебречь, процесс возникновения и устранения в системе угрозы уязвимости может быть описан схемой "гибели и размножения". Тогда для случая одного обслуживающего прибора искомая характеристика безопасности – стационарный коэффициент готовности (в данном случае готовности к безопасной эксплуатации в отношении угрозы уязвимости)определяется следующим образом:

$$P_{0y} = 1 - \rho,$$

где

$$\rho = \lambda/\mu,$$

а вероятность наличия в системе одновременно **R не устраненных уязвимостей** (реальных угроз уязвимостей):

$$P_{Ry} = \rho^R(1 - \rho).$$

В качестве обслуживающего прибора в данном случае выступает коллектив разработчиков (сотрудников модельного агентства), устраняющих выявленную в системе уязвимость с интенсивностью **μ**.

На практике одновременно может устраняться несколько уязвимостей, т.е. в общем случае следует рассматривать схему "гибели и размножения" с **C**

обслуживающими приборами. Для такой модели искомая характеристика (стационарный коэффициент готовности) определяется следующим образом:

$$P_{0y} = \left(1 + \rho + \frac{\rho^2}{2!} + \cdots + \frac{\rho^C}{C!}\right)^{-1},$$

а вероятность наличия в системе одновременно R не устраненных уязвимостей:

$$P_{Ry} = \frac{\rho^C}{C!} P_{0y}$$

Таким образом, угроза уязвимости смоделирована в качестве простейшего или базового элемента информационной системы.

2.3 Угроза атаки

Далее необходимо смоделировать более сложный элемент – угрозу атаки, создаваемой угрозами уязвимости, а, в конечном счете, угрозу безопасности информационной системы в целом, создаваемой угрозами атак.

С учетом этого для упрощения последующих моделей необходимо оценить какое количество обслуживающих приборов **C** следует рассматривать при моделировании угрозы уязвимости и при каких условиях.

Если предположить, что при условии $\rho = \lambda/\mu \ll 1$ значение вероятности $P_{R>1y}$мало, то им можно пренебречь. Тогда чтобы оценить влияние на результаты моделирования характеристики **C**, необходимо рассмотреть измененииена интересующих интервалах значений характеристики P_{Ry} от изменения значений параметраρ для одноканальной (табл.1) и двухканальной (C=2) (табл.2) систем.

Таблица 1

Характеристики одноканальной системы

P_{Ry}	ρ				
	0,1	**0,2**	**0,3**	**0,4**	**0,5**
P_{0y}	**0,90**	**0,80**	**0,70**	**0,60**	**0,50**
P_{1y}	**0,09**	**0,16**	**0,21**	**0,24**	**0,25**
$P_{R\geq 2y}$	**0,01**	**0,04**	**0,09**	**0,16**	**0,25**

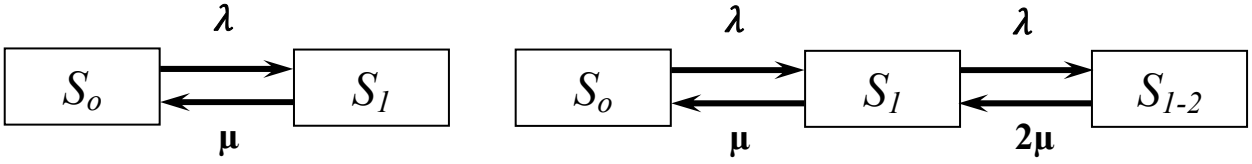
Таблица 2

Характеристики двухканальной системы

P_{Ry}	ρ						
	0,3	**0,4**	**0,5**	**0,6**	**0,7**	**0,8**	**0,9**
P_{0y}	**0,74**	**0,68**	**0,60**	**0,56**	**0,51**	**0,47**	**0,43**
P_{1y}	**0,23**	**0,27**	**0,32**	**0,34**	**0,36**	**0,38**	**0,39**
P_{2y}	**0,03**	**0,05**	**0,08**	**0,10**	**0,13**	**0,15**	**0,18**
$P_{R\geq 2y}$	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Проанализировав результаты, представленные в табл.1 и в табл.2, напрашиваются следующие выводы. При условии $\rho \leq 0{,}2$ при моделировании угрозы уязвимости может использоваться одноканальная схема "гибели и размножения", при условии же $\rho > 0{,}2$ должна использоваться, как минимум, двухканальная схема. Условие $\rho > 0{,}9$ не анализируется, поскольку при выполнении данного условия о какой-либо безопасности говорить совсем не приходится.

Графы состояний случайного процесса выявления и устранения уязвимостей (марковского процесса с дискретными состояниями и непрерывным временем), которые далее будут использоваться, представлены на рисунке 1, где S_0 – исходное состояние системы, S_1 − в системе выявлена и не устранена одна из уязвимостей, S_{1-2} − в системе выявлены и не устранены две уязвимости.



а) при условии $\rho \leq 0{,}2$ б) при условии$\rho > 0{,}2$

Рис. 1 Графы системы состояний случайного процесса для угрозы уязвимости

Рассмотрев интенсивности возникновения и устранения уязвимостей в системе информационной безопасности, нельзя оставить без внимания атаки, которые являются следствием неустранения уязвимостей.

Говоря об угрозе атаки, прежде всего следует напомнить, что информационная безопасность имеет несколько ключевых характеристик, к которым относятся конфиденциальность, целостность и доступность обрабатываемой информации. Атака на информационную систему реализуется с целью нарушения, как правило, одной из этих характеристик – с учетом этого строится и защита информационной системы в зависимости от ее назначения: защита от нарушения конфиденциальности информации (защита от ее хищения), защита от нарушения целостности информации (защита от ее несанкционированной модификации), защита от нарушения доступности информации. Естественно, говоря об угрозе атаки, подразумевается, что эта атака может быть реализована нарушителем с определенной целью.

В общем виде угрозу атаки на информационную систему можно представить соответствующим орграфом (рис. 2):

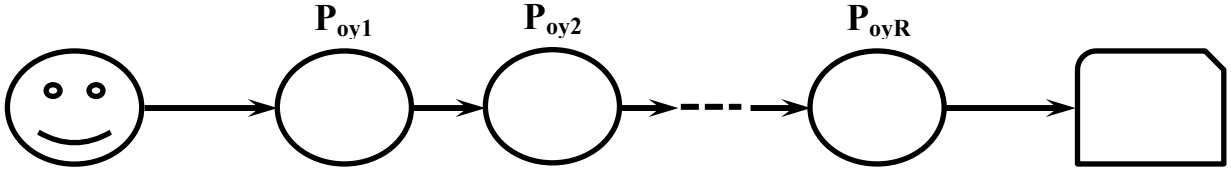


Рис. 2 Орграф угрозы атаки

На орграфе через P_{0yr}, r = 1, …, R, обозначена вероятность отсутствия в системе r-й уязвимости (информационная система готова к безопасной эксплуатации в отношении угрозы r-й уязвимости) – одной из R реальных угроз уязвимостей, последовательно (дуги графа определяют последовательность использования выявленных уязвимостей при реализации атаки) используемых атакой на информационную систему.

При подобном представлении угроза атаки на информационную систему может интерпретироваться схемой параллельного резервирования угроз уязвимостей, резервируемыми и резервирующими элементами которой

являются угрозы уязвимости (рис. 3) поскольку каждая угроза уязвимости, присутствующая в системе с вероятностью P_{0yr}, может рассматриваться в качестве резервирующего элемента (с вероятностью P_{0yr} предотвращает атаку).

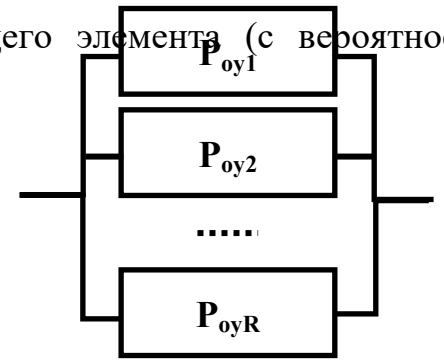


Рис. 3 Орграф интерпретацииугрозы атаки схемой параллельного резервирования угроз уязвимостей

Данная интерпретация позволяет представлять систему защиты информационной системы в виде отдельной вершины (отдельных вершин) на орграфе угрозы атаки с параметрами безопасности $\boldsymbol{\lambda_{сзи}}$ и $\boldsymbol{\mu_{сзи}}$ уже собственно системы защиты (это параметры угроз уязвимостей системы защиты). Подобная интерпретация угрозы атаки позволяет сделать выводо том, что угрозы уязвимостей, создающие угрозу атаки, с точки зрения их нивелирования системой защиты эквивалентны, поскольку при нивелировании любой из них угрозы системы защиты включаются в схему параллельного резерваодинаково с параметрами безопасности системы защиты$\boldsymbol{\lambda_{сзи}}$ и $\boldsymbol{\mu_{сзи}}$.

Если обозначить вероятность того, что система защиты, используемая для нивелирования уязвимости, готова к безопасной эксплуатации, через $P_{0сзи}$, то вероятность того, что защищенная в отношении угрозы уязвимости информационная система будет готова к безопасной эксплуатации, $P_{0узис}$ при использовании системы защиты, нивелирующей эту угрозу уязвимости, может быть определена следующим образом:

$$\mathbf{P_{0узис} = 1 – (1 – P_{0у})(1 – P_{0сзи}),}$$

а вероятность того, что защищенная информационная система готова к безопасной эксплуатации, $P_{0азис}$ в отношении угрозы атаки при использовании системы защиты, нивелирующей одну из R уязвимостей, используемых атакой:

$$\mathbf{P_{0азис} = 1 – (1 – P_{0сзи})\prod^{R}_{r=1}(1 – P_{0уг}).}$$

Данная формула, соответствующая схеме параллельного резерва, верна только в том случае, если резервируемый элемент (угроза атаки на информационную систему) и резервирующий ее элемент (угроза атаки на систему защиты) не зависимы по угрозам уязвимостей. Если же эти угрозы атак на информационную систему и на систему защиты создаются одними и теми же угрозами уязвимостей, то данные угрозы уязвимости должны интерпретироваться схемой последовательного резервирования.

С учетом приведенных расчетов можно сформировать важные требования к системе защиты.

Угрозы атак на информационную систему и на систему защиты должны быть независимы по угрозам уязвимостей. Обеспечение независимости угроз атак на информационную систему и на систему защиты по угрозам уязвимостей можно позиционировать в качестве фундаментального требования к средству защиты при его проектировании.

Теперь следует коснуться немного образа потенциального нарушителя информационной безопасности.

Риск реализации атаки на информационную систему невозможно оценить без построения модели потенциального нарушителя безопасности, без подобной оценки можно оценить лишь риск отказа безопасности информационной системы – возникновения реальной угрозы атаки. Естественно, что данной моделью должны учитываться заинтересованность злоумышленника в реализации атаки на конкретную информационную систему и его потенциальные возможности (очевидно, что эти характеристики взаимосвязаны).

2.4 Модель нарушителя

Построение модели нарушителя является ключевым вопросом при моделировании характеристик безопасности информационных систем. Без возможности количественного задания коэффициента $\mathbf{К}_{га}$ (*вероятности осуществить атаку (реализовать угрозу атаки) потенциальным нарушителем (реализовать создавшуюся в информационной системе реальную угрозу атаки*) расчет характеристик безопасности конкретной информационной системы, для которой проектируется система защиты, невозможен.

Модель потенциального нарушителя безопасности может формироваться как набор предположений о возможном нарушителе безопасности, его квалификации, технических и материальных возможностях и т.д. При этом строится неформальная модель нарушителя, отражающая причины и мотивы действий, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей: способы реализации исходящих от него угроз, место и характер действия, возможная тактика и т.п. В конечном счете подобная модель используется с целью выявления совокупности актуальных угроз атак для конкретной информационной системы, для которой проектируется система защиты информации, именно актуальных, поскольку потенциально возможные угрозы атак определяются возможностью их технической реализации на информационную систему (архитектура, используемые программные и аппаратные средства и т.д.).

При математическом моделировании нарушителя процесс сводится к моделированию воздействия нарушителя на защищаемую систему и представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, характеризующих результаты действий и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами защищаемого объекта.

Модель нарушителя должна учитывать достаточно много факторов, не все из которых поддаются формализованному описанию. Это, прежде всего, уровень заинтересованности в получении несанкционированного доступа к конкретной информации, это уровень квалификации нарушителя, позволяющий ему осуществить ту или иную атаку, его информированность о выявлении и устранении различно рода уязвимостей, наличие соответствующих инструментальных средств для осуществления атаки, информированность о реализованных в конкретной информационной системе технологиях (возможность получения подобной информации), в том числе технологиях защиты информации, используемом программном обеспечении, регламентах и другое. Сложность учета всех этих (трудно формализуемых) факторов обусловливается не только их количеством и разнородностью, но и сложностью формализации каких-либо зависимостей между ними (например, нарушитель может нанять высококвалифицированного специалиста для осуществления атаки, может приобрести соответствующие автоматизированные средства осуществления атаки – реализовать сложную атаку, не обладая при этом должной квалификацией, и т.д.). Вместе с тем, необходима некая интегральная оценка, причем количественная, позволяющая учесть все эти факторы, иначе невозможно приступить к проектированию системы защиты для конкретной информационной системы. Крайне важным является и следующий момент. Атаки разнородны по своей природе (локальные, сетевые, предполагающие внедрение вредоносной программы, использование ошибки в приложении, в системном драйвере и многое другое). Как следствие, необходим такой подход к оцениванию, который бы позволил ввести некую единую шкалу оценки актуальности угроз атак вне зависимости от их природы.

Согласно основам теории информации, для осуществления успешной атаки на отдельно взятую уязвимость нарушитель должен обладать соответствующей информацией в отношении угрозы этой уязвимости – информацией о том, что такая уязвимость выявленаи не устранена, т.е. неким

количеством информации в отношении угрозы уязвимости. При этом интерес представляет вероятность того, что уязвимость присутствует в информационной системе– угроза уязвимости реальна,при этом возможны два исхода события: уязвимость присутствует либо нет, количество информации в отношении уязвимости в данном случае следует рассматривать как вероятностную меру.

Вероятностная мера количества информации I (в рассматриваемом случае – в одном сообщении) определяется по формуле:

$$I = -\log_2 Pi,$$

где P_i – вероятность i -го исхода.

В таком случае неопределенность можно рассматривать в отношении любой угрозы уязвимости, которая может использоваться нарушителем при осуществлении атаки, вероятность присутствия которой (реальная угроза) в системе определяется как $1 - P_{0y}$. Нарушитель для осуществления успешной атаки должен обладать соответствующей информацией в отношении присутствия уязвимости в системе, т.е. получить сведения, уменьшающие неопределенность в отношении данной угрозы уязвимости. Очевидно, что чем выше для угрозы уязвимости значение P_{0y} (в общем случае уязвимость реже возникает и за меньшее время устраняется), тем сложнее нарушителю осуществить соответствующую атаку.

Учитывая это, сложность реализации угрозы уязвимости (S_y) может интерпретироваться как вероятностная мера количества информации$I(P_{0y})$, которым должен обладать злоумышленник для реализации этой угрозы, как следствие, может быть определена следующим образом:

$$S_y = I(P_{0y}) = -\log_2(1 - P_{0y})$$

Поскольку угрозу атаки создает соответствующая совокупность выявленных и не устраненных в системе уязвимостей (реальных угроз уязвимостей), сложность атаки для нарушителя в общем случае определяется совокупной сложностью атак на каждую создающую угрозу атаки угрозу уязвимости. Если рассмотреть атаку как последовательность использования

нарушителем выявленных и не устраненных в системе уязвимостей, имеющих характеристики P_{0yr} и S_{yr}, r = 1, …, R, можно ввести количественную характеристику сложности атаки $I(P_{0a})$ (S_a), где $S_a = I(P_{0a})$, которая определяется количеством информации, которым должен обладать нарушитель для осуществления успешной атаки, угрозу которой создают R выявленных в системе и не устраненных уязвимостей (с учетом того, что события возникновения (выявления)реальных угроз уязвимостей являются независимыми, а условием реализации нарушителем угрозы атаки является наличие в системе одновременно всех уязвимостей, создающих угрозу атаки):

$$S_a = I(P_{0a}) = -\log_2(1 - P_{0a}) = -\log_2 \prod_{r=1}^{R} (1 - P_{0yr}),$$

где $P_{0a} = 1 - \Pi_{r=1}^{R}(1 - P_{0yr})$ – вероятность того, что в любой момент времени угроза атаки реальна.

Используя соответствующее свойство логарифмов, можно записать:

$$S_a = I(P_{0a}) = \Sigma_{r=1}^{R} I(P_{0yr}) = \Sigma_{r=1}^{R} S_{yr}$$

При этом информация, получаемая нарушителем, рассматривается с точки зрения ее полезности (ценности) для достижения потребителем информации поставленной практической цели – в данном случае для осуществления нарушителем успешной атаки на информационную систему.

Коэффициент готовности нарушителя осуществить атаку $K_{га}$ требуется определять применительно к конкретной информационной системе при проектировании для нее системы защиты. На практике при решении задачи проектирования может рассматриваться некая подобная информационная система (аналог), характеризуемая обработкой аналогичной информации, что и определяет заинтересованность и возможности нарушителя. В отношении аналога, как правило, существует соответствующая статистика реализованных (в том числе и отраженных) на информационную систему атак в процессе ее эксплуатации.

С учетом сказанного математическая модель нарушителя (количественная интегральная оценка заинтересованности и возможности

реализации злоумышленником атаки на конкретную информационную систему) может быть представлена следующим образом:

$$S_{a_н} = \max\{S_{a_н m}, m = 1, \ldots, M\},$$

где $S_{a_н}$ – максимальная сложность реализованных (с учетом и отраженных) в подобной информационной системе атак, характеризуемых $P_{0a_н}$, определяемая на множестве выявленных совершенных атак на подобную информационную систему (аналог) в процессе ее эксплуатации $S_{a_н m}$, $m = 1, \ldots, M$.

Имея значение характеристики $S_а$ (характеристики сложности реализации какой-либо угрозы атаки на информационную систему), для которой проектируется система защиты, и значение характеристики $S_{a_н}$ (характеристики максимальной сложности реализованных (в том числе и отраженных) в подобной информационной системе атак)становится возможным определить искомую характеристику коэффициента готовности (или вероятности) нарушителя осуществить атаку сложности$S_а$на конкретную информационную систему (для которой проектируется система защиты) $K_{га}$:

$$K_{га} = \begin{cases} \dfrac{S_{ан}}{S_a}, \text{если } S_{ан} < S_a \\ 1, \text{если } S_{ан} \geq S_a \end{cases}$$

Исходя же из того, что

$$\mathbf{К_{га} = S_{ан}/S_а = (log_2(1 - P_{0ан}))/(log_2(1 - P_{0а})) = log_{1\text{-}P0а}(1 - P_{0ан}),}$$

коэффициент $K_{га}$ может интерпретироваться как значение степени, в которую надо возвести значение вероятности осуществления атаки на информационную систему $(1 - P_{0а})$, для получения значения вероятности атаки, которую может успешно реализовать нарушитель $(1 - P_{0a_н})$.

При этом, для расчета значений искомой характеристики не требуется использования каких-либо экспертных оценок. При рассмотренном подходе к моделированию используются только стохастические параметры угроз уязвимостей и статистика в отношении безопасности эксплуатации

аналогичных систем при проектировании системы защиты конкретной информационной системы.

С использованием введенного коэффициента готовности злоумышленника осуществить успешную атаку сложностиS_a на информационную систему $К_{га}$ (нарушитель готов осуществить подобную атаку – характеристика нарушителя, которая может рассматриваться как вероятность реализации нарушителем успешной атаки при условии неготовности информационной системы к безопасной эксплуатации в отношении атаки, что определяется условиемP_{0a}=0), с учетом того, что информационная система готова к безопасной эксплуатации в отношении угрозы атаки задается характеристикой P_{0a} (характеристика безопасности в отношении угрозы атаки), формула для расчета вероятности реализации в любой момент времени успешной атаки на информационную системуP_aбудет иметь следующий вид:

$$P_a = К_{га} \prod^{R}_{r=1}(1 - Р_{0уг})$$

Естественно, вероятность того, что успешная атака не будет осуществлена на информационную систему, определяется как P_{0a}:

$$P_{0a} = 1 - К_{га} \prod^{R}_{r=1}(1 - Р_{0уг})$$

Описав модель системы информационной безопасности организации и вероятного нарушителя системы, целесообразно уделить внимание резервированию элементов системы безопасности.

2.5 Резервирование элементов системы безопасности.

Резервирование является одним из эффективных способов повышения надежности функционирования информационной системы, при этом на практике резервируются наиболее критичные к отказу элементы информационной системы, как правило, серверы, на которых концентрируется обработка и хранение обрабатываемых данных.

Однако в современных условиях информационные системы, требующие резервирования элементов, т.е. критичные к нарушению характеристики надежности функционирования, подвержены угрозам атак несанкционированного доступа, т.е. критичны и к нарушению характеристики безопасности. Исходя из этого целесообразно рассмотреть возможности применения резервирования элементов информационной системы применительно к решению задачи повышения уровня ее безопасности. С учетом того, что для современных информационных систем характеристики надежности и безопасности сопоставимо важны, целесообразно исследовать возможность комплексного решения задачи резервирования с использованием одних и тех же средствс целью повышения уровня интегрированной информационно-эксплуатационной безопасности информационных систем (для повышения уровня надежности, а также для повышения уровня безопасности в комплексе).

При этом, следует рассмотреть основные отличия в постановке задачи резервирования всистеме информационной безопасности:

1. исследуемым элементом безопасности является угроза атаки, при этом атаки, в отличие от отказов, никак не могут рассматриваться как независимые события, поскольку атака представляет собою не некое случайное, а осознанное деструктивное воздействие нарушителя безопасности на информационную систему, последствие сформировавшейся угрозы, реализуемое с целью несанкционированного доступа (НСД) к обрабатываемой в системе информации. Естественно предположить, что,если нарушитель совершил успешную атаку на элемент информационной системы, на резервирующий элемент он в первую очередь попытается совершить аналогичную апробированную им атаку. Как следствие, события деструктивного воздействия на зарезервированные элементы следует рассматривать как зависимые;

2. информационная безопасность имеет несколько ключевых характеристик, сопоставимо важных при решении задач повышения уровня информационной безопасности систем. К характеристикам информационной

безопасности относятся: защита от нарушения конфиденциальности информации (защита от ее хищения), защита от нарушения целостности информации (защита от ее несанкционированной модификации), защита от нарушения доступности информации. В общем случае при реализации защиты информационной системыданные задачи защиты, направленные на обеспечение требуемого уровня этих характеристик, должны решаться в комплексе.

Резервирование элементов системы с целью повышения уровня надежности (отказоустойчивости) функционирования информационной системы посредством резервирования наиболее критичных к отказам элементов.

Резервирующие элементы при этом в простейшем случае включаются по схеме параллельного резерва, в результате чего повышается вероятность того, что информационная система готова к эксплуатации $P_{гэ}$, определяемая в предположении того, что в системе используется V элементов с номерами $v = 1,\ldots, V$ ($V-1$ из которых являются резервирующими элементами) при вероятности готовности v-го элемента к эксплуатации в $P_{гэv}$, следующим образом (отказы коммутирующих элементов для простоты не рассматриваем):

$$P_{гэ} = 1 - \prod_{v=1}^{V}(1 - P_{гэv})$$

Эффект достигается за счет того, что при отказе одного из зарезервированных элементов информационная система продолжает свое функционирование.

В качестве резервирующих элементов, используемых с целью увеличения надежности (отказоустойчивости) функционирования информационной системы, могут применяться как полностью одинаковые (в этом случае для них будет совпадать значение характеристики $P_{гэv}$), так и различные (при соответствующем различии значений характеристики $P_{гэv}$) технические средства.

Это обусловливается тем, что в общем случае отказы резервируемого и резервирующих элементов можно рассматривать как независимые события (возможность отказов коммутирующих и переключающих элементов, используемых для создания схемы резервирования, не рассматриваем). Как следствие, в качестве резервирующих элементов (используемых) можно применять как полностью одинаковые с резервируемыми, так и отличные технические средства. Важным здесь является исключительно влияние характеристики резервирующего элемента $P_{\text{гэ}v}$ на характеристику $P_{\text{гэ}}$ информационной системы в целом.

Резервирование элементов системы с целью повышения уровня безопасности информационной системы.

При рассмотрении ключевых характеристик информационной безопасности в рамках повышении уровня информационной безопасности системы, для выявления соответствующих противоречий будет достаточно рассмотреть две из них: защита от нарушения конфиденциальности информации и защита от нарушения доступности информации.

Повышение уровня защиты от нарушения доступности информации резервированием возможно и достигается в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (по потенциально возможным атакам), т.е. в качестве зарезервированных элементов применяются различные технические средства.

Пусть каждый из V зарезервированных элементов с номерами $v=1,\ldots,V$ может быть определен соответствующей характеристикой –вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных угроз атак, образующих угрозу безопасности элемента информационной системы,$P_{0\text{уэ}v}$.

Если все угрозы атак для всех V резервируемых элементов системы не зависимы – различны, то вероятность того, что информационная система

готова к безопасной эксплуатации в отношении потенциально возможных угроз атак,$P_{0\text{Уэ}V}$ может быть определена следующим образом:

$$P_{0\text{Уэ}V} = 1 - \prod_{v=1}^{V}(1 - P_{0\text{Уэ}v})$$

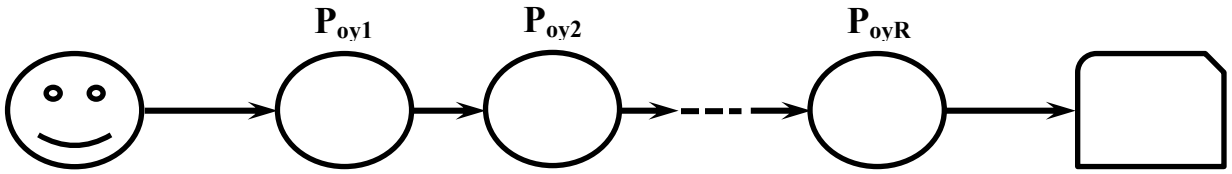
Если же с целью повышения уровня защиты от нарушения доступности информации резервированием применяются резервирующие элементы, полностью зависимые между собою и с резервируемым элементом по угрозам атак (по потенциально возможным атакам), т.е. в качестве зарезервированных элементов применяются одинаковые технические средства, резервирование элементов не реализуется. Это обусловливается следующим. Если все угрозы атак для всех V зарезервированных элементов системы зависимы – угрозы атак соответствующим образом совпадают для всех элементов, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных угроз атак, $P_{0\text{Уэ}V}$ с учетом того, что $P_{0\text{Уэ}v=1} = P_{0\text{Уэ}v=2} = \cdots = P_{0\text{Уэ}v=V}$, может быть определена следующим образом:

$$P_{0\text{Уэ}V} = P_{0\text{Уэ}v}$$

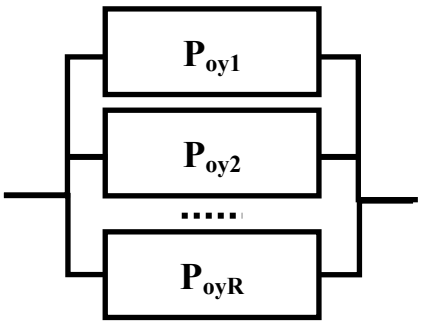
Резервирование элементов информационной системы в части повышения уровня безопасности можно интерпретировать соответствующей схемой резервирования в отношении угроз атак, при этом справедливо говорить о том, что задача резервирования элементов информационной системы сводится к задаче резервирования по угрозам атак.

Теперь к модели резервирования по угрозам атак. Для наглядности (простоты представления) справедливо предположить, что каждый из R зарезервированных элементов информационной системы подвержен только одной угрозе атаки. Если угрозы атак всех зарезервированных элементов системы уникальны (не зависимы) и характеризуются P_{0yr}, $r = 1, ..., R$(для соответствующихRзарезервированных элементов), вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможныхугрозатаки,

то для осуществления успешной атаки на информационную систему в целом должна быть осуществлена успешная атака на каждый из зарезервированных элементов (реализованы угрозы информационной безопасности всех резервирующих элементов)– выведены из строя (рассматриваетсяхарактеристика доступности информации) все зарезервированные элементы информационной системы. В результате получается орграф (рис. 4) "взвешенными" (значениями P_{0yr},$r=1,....,R$) вершинами которого выступают вершины угроз атак зарезервированных элементов, и соответствующую ему схему параллельного резервирования.



а) орграф угроз атак



б) схема параллельного резервирования

Рис. 4. Модель резервирования по угрозам атак при защите от нарушения доступности информации

В такой модели резервирования можно обозначить характеристику некой произвольной угрозы атаки как P_{0y} (пусть угроза подобной атаки на элемент системы $v=1$), для остальных элементов системы $v = 2, ..., V$ соответствующая характеристика – $P_{0Уэv}$. В данных предположениях соответствующая характеристика зарезервированной информационной системы $P_{0УэV}$может быть представлена следующим образом:

$$P_{0УэV} = 1 - (1 - P_{0y}) \prod_{v=2}^{V} (1 - P_{0Уэv})$$

Если же одна и та же угроза атаки с характеристикой $P_{0у}$ совпадает, например, для элементов $v = 1$, $v = 2$, $v = 3$ из V зарезервированных элементов, то для $P_{0УэV}$ уже получится:

$$P_{0УэV} = 1 - (1 - P_{0у})\prod^{V}_{v=4}(1 - P_{0Уэv})$$

В пределе – угроза атаки совпадает для всех зарезервированных элементов V, следовательно:

$$P_{0УэV} = P_{0у},$$

т.е. в данном случае (применительно к подобной угрозе атаки) все угрозы атак зарезервированного и резервирующих элементов информационной системы зависимы – задача резервирования не решается.

Следовательно задача резервирования элементов информационной системы применительно к решению задач повышения уровня информационной безопасности информационных систем в части защиты от нарушения доступности информации сводится к задаче резервирования угроз атак на элемент информационной системы посредством резервирования данного элемента элементом (элементами), характеризуемым отличными (независимыми) угрозами атак. При полном совпадении резервируемого и резервирующего элементов информационной системы задача резервирования элементов информационной системы с целью повышения уровня информационной безопасности в части защиты от нарушения доступности информации резервированием не решается, поскольку не реализуется резервирование по угрозам атак.

Такая ситуация позволяет ввести понятие и количественную оценку актуальности угрозы атаки, но уже на зарезервированную информационную систему (на зарезервированный элемент информационной системы).

Под количественной оценкой актуальности угрозы атаки на зарезервированную информационную систему (на зарезервированный элемент информационной системы) целесообразно понимать значение вероятности готовности к безопасной эксплуатации зарезервированной

информационной системы в отношении угрозы этой атаки $P_{0\text{Уэ}v}$. К наиболее актуальным угрозам атак при результате резервирования элементов информационной системы будут отнесены незарезервированные угрозы атак – угрозы атак, актуальные и для резервируемого, и для резервирующих элементов информационной системы. Именно в отношении подобных угроз атак при резервировании элементов информационной системы в первую очередь потребуется применение средств защиты, направленных на повышение значения характеристики $P_{0\text{Уэ}v}$.

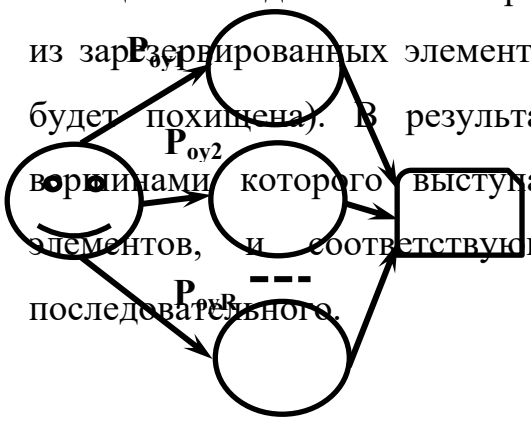
Значит задачи защиты от нарушения доступности информации, которое может быть вызвано как отказом элемента системы, так и реализацией атаки на этот элемент нарушителем безопасности, могут решаться в комплексе, при этом можно говорить о решении задачи повышения уровня интегрированной информационно-эксплуатационной безопасности информационных систем в части данных характеристик. При этом задача повышения уровня интегрированной информационно-эксплуатационной безопасности информационных систем позволяет определить и вполне определенную постановку задачи повышения уровня надежности (отказоустойчивости) информационных систем, предполагающую обеспечение максимального различия технических средств, используемых в качестве резервируемого и резервирующих элементов, что обеспечивает их максимальное различие по угрозам атак.

Резервирование элементов системы информационной безопасности с целью защиты от нарушения конфиденциальности обрабатываемой в информационной системе информации.

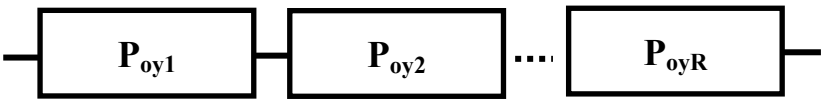
Нарушение характеристики конфиденциальности информации также может быть достигнуто в результате реализации нарушителем атаки на информационную систему, но уже с целью хищения обрабатываемой в ней информации.

В модели резервирования по угрозам атак при решении данной задачи резервирования для наглядности (простоты представления) целесообразно

предположить, что каждый из R зарезервированных элементов информационной системы подвержен только одной угрозе атаки. Если угрозы атак всех зарезервированных элементов системы уникальны (не зависимы) и характеризуются $P_{0уr}$, $r = 1, ..., R$ (для соответствующих R зарезервированных элементов), вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможной угрозы атаки, то для осуществления успешной атаки на информационную систему в целом достаточно реализации успешной атаки на любой из зарезервированных элементов (в этом случае обрабатываемая информация будет похищена). В результате получатся орграф (рис. 5) взвешенными вершинами которого выступают вершины угроз атак зарезервированных элементов, и соответствующая ему схема резервирования, но уже последовательного.



а) орграф угроз атак



б) схема последовательного резервирования

Рис. 5. Модель резервирования по угрозам атак при защите от нарушения конфиденциальности информации

Повышение уровня защищенности информационной системы от нарушения конфиденциальности информации резервированием принципиально невозможно, поскольку в данном случае невозможно резервирование по угрозам атак.

Если считать, что каждый из V зарезервированных элементов с номерами $v = 1, ..., V$может быть представлен соответствующей характеристикой – вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, образующих угрозу безопасности элемента информационной системы,$P_{0Уэv}$, то в случае если все

угрозы атак в V резервируемых элементах системы зависимы (полностью совпадают), при этом для хищения информации достаточно осуществить успешную атаку на любой из V зарезервированных элементов, вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, $P_{0\text{Уэ}V}$ с учетом того, что $P_{0\text{Уэ}v=1} = P_{0\text{Уэ}v=2} = \cdots = P_{0\text{Уэ}v=V}$,в данных предположениях может быть определена следующим образом:

$$P_{0\text{Уэ}V} = P_{0\text{Уэ}v}$$

В случае же если все угрозы атак в V зарезервированных элементах системы независимы (соответствующим образом различаются во всех элементах), при этом для хищенияинформации достаточно осуществить успешную атаку на любой из V зарезервированных элементов, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак,$P_{0\text{Уэ}V}$:

$$P_{0\text{Уэ}V} = \prod_{v=1}^{V} P_{0\text{Уэ}v}$$

Как показало моделирование, попытка решения задачи повышения уровня безопасности информационной системы в части, касающейся защиты от нарушения конфиденциальности информации резервированиемможет привести лишь к снижению уровня безопасности. Причемповышение уровня защиты от нарушения доступности информации резервированием возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (в случае реализации резервирования по угрозам атак), но именно при этих условиях снижается уровень безопасности информационной системы в части защиты от нарушения конфиденциальности информации.

То есть при создании и развертывании системы информационной безопасности со стороны должностных лиц организации – модельного

агентства, требуется некий компромисс, как в организационных, так и технических мероприятиях.

Проведенное исследование показало, что резервирование для решения задачи повышения уровня конфиденциальности обрабатываемой в информационной системе информации с использованием известных из теории надежности только методов резервирования не может использоваться в полной мере, что, прежде всего, и делает неэффективным применение известных методов резервирования элементов информационных систем в области информационной безопасности.

В такой ситуации целесообразно рассмотреть задачу повышения уровня безопасности в части обеспечения конфиденциальности информации с позиций оценки риска потенциальных потерь. Риск потенциальных потерь $\boldsymbol{R_{C\text{Уинф}}}$ применительно к угрозе информационной безопасности информационной системы (характеристика угрозы информационной безопасности информационной системы $P_{0\text{УэИ}V}$) в простейшем случае (без учета изменения даннойхарактеристики в процессе эксплуатации информационной системы) возможно оценить следующим образом:

$$\boldsymbol{R_{C\text{Уинф}} = C_{\text{инф}}\,(1 - P_{0\text{УэИ}V})}$$

Характеристика потерь $C_{\text{инф}}$ зависит от объема похищенной информации.Здесь следует ввести характеристику удельной стоимости $C_{\text{уинф}}$ единицы информации. Исходя из того, что в информационной системе обрабатывается

N единиц информации, характеризуемых удельной стоимостью $C_{\text{уинф}}$, величину потерь, обусловливаемых хищением обрабатываемой в информационной системе информации, можно представить следующим образом:

$$\boldsymbol{C_{\text{инф}} = C_{\text{уинф}} N/V}$$

Следовательно, потери от реализации успешной атаки на один из зарезервированных элементов информационной системы составят $C_{\text{инф}v}$, что снизит потери от успешной атаки на элемент информационной системы в V раз.

Подобный метод резервирования вполне можно назвать "методом резервирования с разделением обработки информации между элементами системы".

Повышение уровня безопасности информационной системы в частихарактеристики нарушения конфиденциальности информации методом резервирования с разделением обработки информации между элементами системывозможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (по потенциально возможным атакам).

В случае если все угрозы атак в Vзарезервированных элементах системы зависимы – соответствующим образом полностью совпадают, т.е. одна и та же атака может быть реализована на все V зарезервированных элементах (резервирования по угрозам атак не реализовано), риск потерь от реализации угрозы атаки на элемент системы (характеристика угрозы атаки на любой элемент системы $P_{0\text{Уэ}v}$) $R_{C\text{Уинф}}$ рассчитывается следующим образом:

$$\boldsymbol{R_{C\text{Уинф}} = C_{\text{инф}}\,(1 - P_{0\text{Уэ}v})}$$

Если же все угрозы атак в V резервируемых элементах системы не зависимы –соответствующим образом различаются во всех элементах (зарезервированы), одна и та же атака может быть реализована только на один из Vзарезервированный элемент, для $R_{C\text{Уинф}}$получится:

$$\boldsymbol{R_{C\text{Уинф}} = C_{\text{инф}}\,(1 - P_{0\text{Уэ}v})/V}$$

Представленные выше формулы для альтернативных рассмотренных случаев доказывают, что повышение уровня безопасности от нарушения конфиденциальности информации резервированием возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (по потенциально возможным атакам); при этом резервирование элемента полностью идентичными по угрозам атак элементами не может использоваться винформационной системе с целью повышения уровня безопасности от нарушения конфиденциальности информации.

Применение метода резервирования с разделением обработки информации между элементами системы в случае реализации резервирования по угрозам атак (используются различные технические средства для построения зарезервированных элементов информационной системы), позволяющего снизить риск потенциальных потерь от реализации успешной атаки на информационную систему (в V раз),приводит к увеличению риска частичных потерь обрабатываемой в информационной системе информации – риска потерьинформациив объеме, обрабатываемом однимиз зарезервированных элементов системы.

Данное заключение подтверждается следующим. Расчеты показали, что в случае, если все угрозы атак в V зарезервированных элементах системы независимы (зарезервированы) –соответствующим образом различаются во всех зарезервированных элементах, для хищения информации в объеме, обрабатываемом одним из зарезервированных элементов системы, достаточно осуществить успешную атаку на любой из V зарезервированных элементов.

Вероятность того, что в этом случае информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак,$P_{0\text{УэV}}$:

$$\boldsymbol{P_{0\text{УэV}} = \prod^{V}_{v=1} P_{0\text{Уэ}v}}$$

Если же все угрозы атак в V резервируемых элементах системы зависимы –полностью совпадают (не зарезервированы), при этом для хищения информации в объеме, обрабатываемом одним из зарезервированных элементов системы, достаточно осуществить успешную атаку на любой из V зарезервированных элементов, вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, $P_{0\text{УэV}}$ с учетом того, что $P_{0\text{Уэ}v=1} = P_{0\text{Уэ}v=2} = \cdots = P_{0\text{Уэ}v=V}$, может быть определена следующим образом:

$$\boldsymbol{P_{0\text{УэV}} = P_{0\text{Уэ}v}}$$

Однако в этом случаерезервирования по угрозам атак не будет реализовано, поскольку одна и та же успешная атака может быть осуществлена

на всеV зарезервированных элемента системы. В этом случае уже следует говорить о риске хищения всей обрабатываемой в информационной системе информации и о соответствующем для этого случае риске потерь, связанным с хищением информации стоимостью $C_{\text{инф}}$.

Данное противоречие – снижение риска хищения информации обрабатываемой в информационной системе в полном объеме при одновременном увеличении риска хищения информации в объеме, обрабатываемом одним из зарезервированных элементов системы, можно считать принципиальным противоречием метода резервирования с разделением обработки информации между элементами системы.

Это важное противоречие данного метода резервирования в обязательном порядке должно учитываться при разработке требований к характеристикам и параметрам средств защиты информации, реализуемых (при необходимости) в резервируемых элементах информационной системы.

ГЛАВА 3. ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ РУКОВОДСТВУ ТИПОВОГО МОДЕЛЬНОГО АГЕНТСТВА ПО ФОРМИРОВАНИЮ И ПОДДЕРЖАНИЮ ЭФФЕКТИВНОГО ФУНКЦИОНИРОВАНИЯ ЕГО СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ ВЫСОКОЙ АГРЕССИВНОСТИ ИНФОРМАЦИОННОЙ СФЕРЫ

Итак, обеспечение информационной безопасности предприятия – модельногоагентства – это масштабная комплексная задача, успешность которой зависит от множества факторов.

Руководство агентства должно четко понимать:

- какие события в вопросах информационной безопасности (ИБ-события) нельзя допустить;

- удар по каким бизнес-процессам станет для агентства критическим;

- какие ИТ-системы обеспечивают или поддерживают эти процессы.

При этом нельзя забывать о требованиях регуляторов, которые у каждой отрасли свои. В составлении таких требований должны участвовать ведущие специалисты агентства с привлечением, если требуется, профильных компаний.

3.1 Угрозы информационной безопасности при использовании должностными агентства ресурсов информационно-телекоммуникационной сети Интернет.

Информационно-телекоммуникационная сеть Интернет (далее – ИТКС Интернет) уникальна тем, что она не имеет территориальных границ. Это во многом способствует развитию многочисленных веб-ресурсов и обмену информацией.

В современном мире любой человек – любое должностное лицо может получить доступ к данным, хранящимся в ИТКС Интернет, или создать свой собственный веб-ресурс. Интернет как совокупность информационных ресурсов, информационных систем и коммуникационной среды в соответствии со складывающейся терминологией в области информационной безопасности можно рассматривать как информационное пространство или как часть

информационной сферы. Так или иначе, ИТКС Интернет позволяет в значительной степени реализовать как профессиональные, так и личные интересы субъектов в информационной сфере.

Сегодня личными интересами (или интересами личности в информационной сфере) являются реализация конституционных прав человека и гражданина на доступ к информации, использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающей, в том числе и личную безопасность. Очевидно, что практически реализуются эти интересы, посредством использования различных компонентов ИТКС Интернет: обмен информацией с близкими, знакомыми людьми, коллегами; осуществление поиска, просмотра и копирования текстовой, графической и видеоинформации, программных средств; формирование и размещение информации в социальных сетях и т.д. С другой стороны, информация, размещаемая в сети, хоть и формально не считается конфиденциальной, но может нанести вред при использовании ее злоумышленниками, причем как личной безопасности, так и безопасности профессиональной деятельности.

Исходя из этого в Российской Федерации был издан Федеральный закон от 29 июля 2017 г. № 241–ФЗ «О внесении измененийв статьи 10.1 и 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации». Положения этих изменений касаются информационной безопасности при использовании должностными лицами ресурсов информационно-телекоммуникационных сетей.

При этом использование информационно-телекоммуникационного пространства должностным лицом имеет специфические особенности и связанные с этим специфические угрозы.

Должностным лицам необходимо понимать, кто или что выступает источником угрозпри использовании ИТКС Интернет. Источниками угроз, то есть источниками появления новых уязвимостей (параметр λ) в системе

информационной безопасности, могут быть: нарушитель, вредоносная программа.

Нарушители, как правило, подразделяются на два типа: внешние и внутренние. Под внешними нарушителями (далее злоумышленники) понимаются: разведывательные службы государств, криминальные структуры, недобросовестные партнеры организаций, оказывающих услуги агентству в рамках соответствующих контрактов (договоров), внешние субъекты (физические лица), например хакеры, конкуренты и др. Также к источникам внешних угроз необходимо отнести деятельность террористических организаций.

Внутренние нарушители – это различные категории должностных лиц агентства, которые имеют определенные полномочия доступа к информации, а также сами пользователи.

Следующий источник угроз — это вредоносная программа, которая может ассоциироваться с какой-либо прикладной программой, с файлами, имеющими определенное расширение или иные атрибуты, с сообщениями, передаваемыми по сети. Ее носителями могут быть пакеты передаваемых по телекоммуникационной сети сообщений и файлы (текстовые, графические, исполняемые и др.).

Целесообразно рассмотреть некоторые из источников угроз, прежде всего разведывательные службы иностранных государств, фирм-конкурентов и, не исключено, соответствующие службы фирм-партнеров. Разведывательные службы ведут активную работу по добыванию и реализации информации, связанной с деятельностью должностных лиц организации, взаимодействующих структур, в том числе и государственных, госкорпораций, финансово-кредитных учреждений и иных организаций, а также персональной информации с использованием возможностей сети Интернет. Особый интерес для них представляет компрометирующая информация, которая может быть использована при вербовке должностного лица.

Специалисты таких служб рассматривают разведку в ИТКС Интернет как нулевую фазу своей внешней стратегии.

Главная цель – обнаружение уязвимостей в системе информационной безопасности противника-конкурента. В рамках первой фазы через выявленные «дыры» специалистам предписывается проникать внутрь с помощью «тайных имплантатов».

Вторая фаза – получение «постоянных доступов». С помощью полученной информации спецслужбы могут осуществлять информационно-психологические воздействия на нужных должностных лиц организации с целью нарушения их морально-психологического состояния, что, в свою очередь, может привести к неспособности их к эффективной деятельности по предназначению. В ряде случаев такие состоянияи процессы могут приводить к деструктивной деятельности должностных лиц в интересах противоборствующей стороны.

Компрометирующая информация для них представляет особый интерес, поскольку может быть использована в акциях и действияхпо дискредитации как рядовых сотрудников, так и руководства и самой организации в целом.

Особо остро может встать вопрос о деятельности представителей террористических организаций, заинтересованных в добывании\ и использовании персональной информации о должностных лицах организации, ведущих свою деятельность как на территории Российской Федерации, так и за ее пределами (в том числе о их близких и родных).

Представители организованных преступных сообществ заинтересованы, прежде всего, в извлечении материальной выгоды при добывании и использовании информации, связанной с деятельностью должностных лиц, а также их персональной информации. Добытая ими компрометирующая информация может быть реализована в целях подкупа и шантажа должностных лиц, связанных с принятием решений относительно распределения различных ресурсов.

Необходимо отметить, что перечисленные группы злоумышленников имеют соответствующие организационно-технические возможности по добыванию информации и осуществлению информационных воздействий, а их намерения очевидны и вытекают из их предназначения (либо мотивов деятельности) и решаемых ими задач. При этом применяются классические приемы как воздействия на информацию, так и информационно-технические, информационно-психологические воздействия.

Например, информационно-психологическое воздействие. Сегодня на Западе успешно функционирует целая сеть информационных агентств, интернет-порталов и блогерских площадок, являющихся частью огромной пропагандистской машины. Они фактически занимаются продвижением западных ценностей, интересов и взглядов при активной демонизации России и работающих здесь организаций. ИТКС Интернет является идеальной системой, которая активно используется различными спецслужбами и мировыми СМИ против России и российских организаций: вбросы ложной информации, замалчивание одних фактов и выпячивание других, дезинформация, клевета, подмена понятий, отвлечение вниманияна второстепенные проблемы и т.д. Цель – разрушение организаций и самого государства Российская Федерация изнутри путем целенаправленного воздействия на сознание работников организаций, населения страны, в первую очередь молодежь, подростков.

Сегодня воздействие с использованием ИТКС Интернет идет через головные структуры в Вашингтоне, которые непосредственно финансируют собственные СМИ, ведущие пропагандистскую работув России, и активно проникают в российские социальные сети, запускают специализированные мониторинговые и медийные проекты в них, а также расширяют технологические платформы и возможности для трансляции собственных медиа в ИТКС Интернет, чтобы обойти ограничения, накладываемые российским законодательством.

Государственный Совет управляющих по вопросам вещания США (BBO) присоединился к Британской вещательной корпорации (BBC), Deutsche Welle

(DW), France Medias Monde (FMM) и стал спонсором специализированного портала по обходу блокировок в Интернете bypasscensorship.org. Цели и задачи совместного проекта западных государственных медиакорпораций на самом сайте выражены предельно откровенно и недвусмысленно: «Представители отделов этих СМИпо противодействию цензуре намерены способствовать расширению свободы «Интернета» для людей, живущих в странах с репрессивными режимами, пытающихся заблокировать доступ к информации и угрожающих свободе самовыражения».

В повседневной деятельности должностные лица агентства и привлекаемые к работе модели могут столкнуться с таким явлением, как социальная инженерия, которую активно используют злоумышленники. Этот термин обозначает способ получать нужную информацию путем обыкновенного обмана, лжи и хитрости.

Злоумышленники применяют психологические методы воздействия на людей, используя ИТКС Интернет: электронную почту, социальные сети, службы мгновенного обмена сообщениями и др. В результате их умелой работы пользователи сами выдают свои данные, не всегда понимая, что их обманули. При этом распространены:

- претекстинг – атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию выуживает конфиденциальную информацию;

- фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей.

Так основные угрозы информационной безопасности при использовании должностными лицами ИТКС Интернет можно классифицировать по следующим основаниям:

- по видам возможных источников;

- по виду нарушаемого свойства информации;

- по способу реализации;

- по используемой уязвимости;

- по объекту воздействия.

По видам возможных источников выделяются следующие угрозы:

- связанные с преднамеренными или непреднамеренными действиями внутренних или внешних нарушителей;

- источником которых являются технические и (или) программные средства (технические средства разведки, техническое средство воздействия, аппаратная закладка, вредоносная программа).

Например, деятельность Агентства национальной безопасности США (АНБ). В рамках операции Passionatepolka («страстная полька» – англ.) агенты АНБ в 2015 г. смогли получить подробные чертежи устройства интересующих их сетей. Программа Berserker позволяла устанавливать на взломанные компьютеры «устойчивые бэкдоры» и «паразитные драйверы». С помощью вируса Barnfire агенты способны стереть BIOS (загрузочный сектор компьютера) на удаленном сервере. В арсенале спецслужб также программы для проникновения в чаты «Фейсбук» и Yahoo, эксплойт для уязвимости в iOS-браузере Safari и масса другого оружия, поражающего в том числе электронику массового потребления. И это лишь малая часть американского кибероружия. В некоторых новых программах присутствует код кейлоггера Querty. Сама по себе программа не отличается от множества себе подобных, однако исходя из особенностей кода, специалисты считают, что это лишь один модуль полноценной системы Warriorpride. Они полагают, что комплекс позволяет АНБ США проникать в смартфоны iPhoneи осуществлять доступ другим странам группы «Пять глаз», военного альянса в киберпространстве – США, Великобритании, Канаде, Австралиии Новой Зеландии (система «Эшелон»). Используя систему «Эшелон», АНБ США совместно с Центром правительственной связи Великобритании в режиме реального масштаба времени перехватывает и обрабатывает до 181 млн сообщений в день, передаваемых между облачными хранилищами Google. Кроме того, АНБ США активно размещает специальное разведывательное оборудование на каналах связи, проложенных по дну морей и океанов, через которые проходит

значительная часть международного интернет-трафика. Таким образом, АНБ и Центр правительственной связи Великобритании имеют практически неограниченные возможности для сбора информации из социальных сетей в Интернете.

Следующая угроза – это вредоносные вирусы. Они распространяются злоумышленниками под видом различных программ, внедряются в оперативную память и программное обеспечение, практически не оставляя следов. Опыт 2017 г. показал, что в 40 странах, включая Россию, были зафиксированы так называемые незаметные целевые атаки с использованием ИТКС Интернет. По данным «Лаборатории Касперского», для проникновения в корпоративные сети 140 государственных и коммерческих организаций неизвестные злоумышленники использовали исключительно легитимное программное обеспечение, а любые вредоносные файлы хранили в памяти системы, не оставляя никаких следов на жестких дисках.

Чаще всего атакующие применяют специализированное программное обеспечение для тестирования на проникновение, инструменты администрирования и утилиты для автоматизации задач в Windows, например PowerShell.

Практика показывает, что вирусы используются для следующих целей:

- несанкционированный съем (хищение, перехват) информации с мобильного телефона, смартфона, планшета, ноутбука, компьютераи других устройств пользователей. А ими и являются рядовые сотрудники и должностные лица модельного агентства;

- блокирование работы (вывод из строя) устройства (например, вирусы-шифровальщики);

- использование данного устройства для проникновения в другие технические устройства (принцип «форточки»);

- контроль и управление устройством, используя удаленный доступ.

Следующие – это угрозы по виду нарушаемого свойства информации (виду несанкционированных действий), где выделяются:

- угрозы доступности (блокирование) информации;

- угрозы конфиденциальности информации (утечка, перехват, съем, хищение, разглашение);

- угрозы целостности информации (утрата, уничтожение, модификация).

Перечисленные угрозы относятся как к служебной, так и персональной информации, которая размещена в компьютере или на различных персональных мобильных устройствах (телефон, смартфон, планшет и т.д.).

Одной из внутренних угроз информационной безопасности является несанкционированное распространение информации ограниченного хождения в результате использования должностными лицами, гражданами личных технических средств. Данная угроза может быть реализованапри размещении должностными лицами информации в ИТКС Интернет,в том числе в социальных медиаресурсах.

Социальные медиаресурсы сети Интернет – вид массовой коммуникации, осуществляемый посредством сети Интернети предоставляющий возможность публикации, обмена и обсуждения информации широким кругам пользователей.

Угрозы информационной безопасности в социальных медиаресурсах ИТКС Интернет, следующие:

- несанкционированный доступ к персональным компьютерам и мобильным устройствам должностных лиц, с которых осуществляется посещение социальных сетей ИТКС Интернет;

- несанкционированный доступ к контенту, размещаемому должностными лицами в социальных медиаресурсах ИТКС Интернет;

- определение актуального местоположения должностных лиц, мест расположения стратегических объектов агентства;

- утечка информации ограниченного доступа через ИТКС Интернет при размещении данной информации должностными лицамив социальных сетях ИТКС Интернет;

- идентификация должностных лиц и членов их семейв социальных сетях ИТКС Интернет;

- размещение информации, содержащей сведения, компрометирующие или дискредитирующие деятельность должностного лица.

Последствиями реализации угроз, связанных с несанкционированным доступом к персональным компьютерам и мобильным устройствам должностных лиц, с которых осуществляется посещение социальных сетей ИТКС Интернет, являются следующие:

1. Определение конфигурации персональных компьютеров и мобильных устройств должностных лиц, подключенных к ИТКС Интернет, используемого ими программного обеспечения. Указанная информация облегчает злоумышленникам в дальнейшем проводить компьютерные атаки для получения несанкционированного удаленного контроля над устройством и, как следствие, доступа к фото-, аудио- и видеозаписывающим устройствам, а также личным данным должностных лиц (SMS, e-mail-переписка, фотографии, аудио- и видеозаписи, а также любой другой информации, обрабатываемой на ПЭВМ или мобильном устройстве);

2. Установка программного обеспечения, имеющего недекларируемые (вредоносные и шпионские) возможности, позволяющие устанавливать удаленное несанкционированное подключение к ПЭВМи мобильным устройствам должностных лиц.

Большинство администраций социальных сетей ИТКС Интернет разработали для пользователей специальные мобильные приложения, а в некоторых случаях и приложения для персональных компьютеров.

При этом такие приложения имеют широкий доступ к большинству оборудования мобильного телефона (GPS-модулю, фото-, видео-, аудиоданным). Большая часть информации, собираемой этими устройствами, передается на серверы социальных сетей, например координаты передвижения с GPS-модуля. Facebook, Twitter, Amazon и множество других крупных IT-компаний по крупицам собирают персональную информациюи так

называемые «цифровые отпечатки» и знают о пользователях намного больше,чем они бы хотели. Facebook наблюдает за поведением каждого пользователя
в сети. Естественно, что такая информация вызывает особый интерес различных спецслужб и правительственных организаций, занимающихся шпионажем.

Сегодня серьезной проблемой стало массовое выкладывание в социальных сетях как должностными лицами, так и просто гражданами личных фотографий и комментариев к ним, раскрывающих определенные действия. Появление в социальных сетях информационных материалов (фотографий, статей и различных комментариев) об определенных мероприятиях позволяет спецслужбам использовать данные материалы в разведывательных целях.

Любую информацию, попавшую в Интернет, практически невозможно удалить. Многие поисковые системы («Гугл», «Яндекс» и др.) сохраняют (кэшируют) информацию, и в случае ее удаления все равно можно получить к ней доступ. Кроме того, существуют специальные сайты – архиваторы Интернета, которые сохраняют всю информацию на наиболее посещаемых ресурсах в ИТКС Интернет. В таких архивах можно найти все изменения информации, которые были внесены. Если задуматься: выкладывая какую-либо информацию сейчас, например фотографию, человек не может точно предсказать, как она будет использована против него через 5 – 10 лет.

Администраторы также имеют доступ к личной информации, которая может являться служебной, о существовании которой большинство из пользователей даже и не догадываются. Для этого используются:

- оборудование и программное обеспечение для доступа в ИТКС Интернет;
- языковые настройки программного обеспечения;
- настройки часовых поясов;
- разрешение монитора;

- зарядка аккумуляторной батареи мобильного устройства и т.д.

Данная информация может быть использована с различными целями.

Последствиями реализации угроз, связанных с возможностью определения актуального местоположения должностных лиц, граждан, мест расположения различных объектов, которые представляют интерес для спецслужб, а также для лиц, совершающих противоправные действия, является неконтролируемое распространение в ИТКС Интернетличной фото-, аудио- и видеоинформации должностных лиц, граждан, содержащей информацию об их местоположении в текущий момент времени (географические координаты).

Большинство современных фото- и видеокамер, в том числе встроенных в мобильный телефон, привязывают снимок к географическим координатам и добавляют эту информацию к снимку. В дальнейшем при размещении данных снимков в социальных сетях информация о месте съемки автоматически накладывается на карту мира, и определяется уже территориальная и государственная принадлежность места съемки.

Стоит быть более бдительным и при подключении к точкам доступа Wi-Fi, ведь помимо возможности определения местоположения по IP-адресу, сами устройства могут обладать функциями слежения или другими незаявленными возможностями.

В 2013 году была опубликована часть документов бывшего сотрудника АНБ Эдварда Сноудена, из которых стало известно, что американские спецслужбы ежедневно обрабатывают более пяти миллионов единиц информации о местоположении мобильных телефонов, по всему миру.

Угрозами, создающими предпосылки к утечке информации ограниченного доступа в сеть Интернет при ее размещении должностными лицами, гражданами в социальных сетях, являются:

- размещение в социальных сетях информации ограниченного доступа;

- участие в интернет-сообществах по определенным принадлежностям к различным группам, которые могут быть созданы искусственно для сбора нужной информации.

Следующей угрозой, создающей предпосылки к идентификации должностных лиц в социальных сетях, является размещение в социальных медиаресурсах сети Интернет персональных данных, фото-, аудио- и видеоматериалов, которые могут нанести репутационный вред конкретным должностным лицам.

К таким угрозам относятся:

- принятие разрешений при установке развлекательных приложений на персональные мобильные устройства, обеспечивающих возможность несанкционированного скрытного сбора информациио пользователе (его персональных данных), а также информации о его местоположении в режиме реального времени;

- неумышленное размещение в социальных сетях близкими родственниками, партнерами, коллегами и совместными участниками различных интернет-сообществ (спортивных, туристических, коммерческих и т.д.) персональных данных должностных лиц, которые могут стать источником информации для нанесения им вреда.

Также необходимо знать перечень сведений, опубликование которых создает предпосылки к разглашению информации и дискредитации имиджа руководства и агентства в целом:

- сведения, компрометирующие руководство агентства, конкретных должностных лиц;

- сведения, пропагандирующие насилие, порнографию, унижение человеческого достоинства, безнравственное поведение, нецензурную брань и др.;

- информация третьих лиц (родственников, друзей, знакомыхи др.), содержащая сведения, персонифицирующие должностных лиц.

Что касается персональных данных должностного лица, то эта информация всегда актуальна для злоумышленников. К ним относятся: фамилия, имя отчество; год, месяц, дата и место рождения; адрес проживания (регистрации); номер телефона (мобильный, рабочий, служебный, домашний и т.п.); адрес электронной почты; семейное, социальное, имущественное положение; образование (где и когда получено образование, полученные специальности); прохождение военной службы (сроки службы, место службы, наименование воинской части); профессия, должность, место работы или государственной службы; сведения о доходах, банковских счетах и картах; сведения о состоянии здоровья; фото-, аудио- и видеоматериалы, сделанные на рабочем месте, в местах командировок, а также с указанием информации, содержащей географические координаты местонахождения этого лица и определенных объектов. Данный перечень позволяет идентифицировать должностное лицо или гражданина и выполняемую им служебную деятельность.

3.2. Меры по обеспечению информационной безопасности при использовании должностными лицами ресурсов информационно-телекоммуникационной сети Интернет

Рассмотренные угрозы при использовании должностными лицами, гражданами ресурсов ИТКС Интернет позволяют сформулировать ряд основных принципов обеспечения информационной безопасности, позволяющих создать систему информационной безопасности организации – модельного агентства:

- недоверие, исключающее излишнюю восприимчивостьк информации (фактам, суждениям), полученной в ИТКС Интернет,как рациональной, достоверной из всей возможной информации;

- анонимность – исключение утечки персональных идентификационных данных должностных лиц, граждан, а также их близких через ИТКС Интернет;

- скрытность – исключение утечки координатной, технической, семантической и признаковой информации о служебной и бытовой

деятельности должностных лиц, граждан, а также их близких через ИТКС Интернет;

- умеренность – заключается в самоограничении при получении информации и возможности по ее осмыслению.

Основными направлениями обеспечения информационной безопасности являются защитаи комплексное противодействие угрозам при использовании должностными лицами, гражданами ресурсов ИТКС Интернет.

Мерами по предотвращению угроз в ИТКС Интернет являются: мероприятия правового обеспечения, организационные, технические мероприятия, мероприятия морально-психологического обеспечения.

Некоторые технические меры:

- меры по ограничению программной среды должны обеспечивать установку и (или) запуск разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения;

- меры по антивирусной защите должны обеспечить обнаружение компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Основными задачами обеспечения информационной безопасности при использовании должностными лицами, пользователями персональных компьютеров и мобильных устройств в ИТКС Интернет, являются:

- предотвращение утечки информации ограниченного доступа;

- порядок соблюдения должностными лицами, гражданами правил размещения информации.

В основе культуры использовании социальных медиаресурсов ИТКС Интернет должностными лицами, пользователями лежат программные и этические принципы, то есть основные правила деятельности.

К программным принципам обеспечения безопасности можно отнести следующее:

1. Настройка свойств безопасности аккаунтов в социальных сетях Интернет, ограничивающих общий доступ к ним;

2. Мониторинг содержания персональной страницы на предмет выявления действий посторонних лиц;

3. Периодическая проверка настройки свойств безопасности аккаунтов на предмет ограничения доступа неизвестных пользователей к просмотру персональной информации должностных лиц, граждан в социальных сетях;

4. Использование сложных паролей (длиной не менее 14 символов, включая буквы разных регистров и цифры), не совпадающих с паролями к другим сервисам и не состоящих из словарных слов на любом языке, слов в обратном порядке, известных сокращений, повторов букв или их последовательности, а также персональных данных (даты рождения, имена детей и др.), и обеспечение сохранности паролей в тайне;

5. Ограничение возможности использования социальных сетей при подключении к общественным беспроводным сетям и т.д.;

6. Установка антивирусного и антишпионского программного обеспечения на персональных компьютерах и мобильных устройствах, периодическое их обновление;

7. Отказ от запуска приложений при отсутствии уверенности в их надежности и легитимности и дальнейшего перехода по ссылкам;

8. Ограничения в использовании функций геопривязки (геолокации) в персональных мобильных устройствах при исполнении служебных обязанностей и размещении в ИТКС Интернет фото-, аудио-и видеоматериалов с координатной информацией и географической привязкой.

К этическим принципам обеспечения безопасности при использовании социальных сетей ИТКС Интернет можно отнести следующие:

1. Соблюдение требований законодательства Российской Федерации, нормативных правовых актов Президента Российской Федерации и правовых актов в области защиты информации: недопущение публикации информации двойного толкования; недопущение размещения материалов, которые могут содержать компрометирующий, клеветнический, оскорбительный, непристойный или угрожающий характер и способствовать подрыву имиджа государственной власти и государства в целом;

2. Осознание того, что информация, которая попала в социальные сети ИТКС Интернет, мгновенно распространяется и выходит из-под контроля пользователя. Информацию удалить с серверного оборудования социальных сетей невозможно, и она может быть использована злоумышленниками, недоброжелателями в любое время в своих интересах;

3. Оценка содержания подготовленного к опубликованию материала на предмет наличия информации ограниченного доступаи возможных последствий для собственной безопасности, безопасности государственной или иной организации;

4. Понимание личной ответственности, а также возможных последствий своих действий в социальных сетях ИТКС Интернет;

5. Периодическая проверка через поисковые системы наличия информации о себе, своей семье, своей работе; в случае обнаружения такой информации – принять меры для се удаления;

6. Недопущение работниками, сотрудниками, должностными лицами агентства пересылки в социальных сетях ИТКС Интернет информации ограниченного доступа;

7. Недопущение обсуждений в социальных сетях своей служебной деятельности;

8. Выполнение требований работниками, сотрудниками модельного агентства общения при использовании социальных сетей ИТКС Интернет;

9. Недопущение размещения комментариев, направленных на компрометацию и дискредитацию государственной власти, разжигание религиозной и межнациональной ненависти, поддержку расизма, экстремизма, терроризма, порнографии и иной антиобщественной деятельности;

10. Осознание того, что размещение определенной информации может нарушить неприкосновенность частной жизни других лиц и создавать угрозу для безопасности, здоровья, репутации, свободы личности;

11. Понимание неотвратимости наказания (уголовного, гражданско-правового, административного, дисциплинарного) за нарушение законодательства Российской Федерации, нормативных правовых актов Президента Российской Федерации в области защиты информации при использовании социальных сетей ИТКС Интернет;

12. Соблюдение уважения к обычаям и традициям народов, различных этнических, социальных групп и конфессий, способствование межнациональному и межконфессиональному согласию;

13. Недопущение включения в список друзей в социальных сетях ИТКС Интернет посторонних и подозрительных лиц;

14. Не допускать общения с пользователями социальных сетей ИТКС Интернет (блогов, форумов), которые провоцируют сотрудников и должностных лиц модельного агентства к размещению информации ограниченного доступа.

15. Вести переписку и общаться только с теми людьми или должностными лицами организаций-партнеров, с которыми реально знакомы.

16. Периодически доводить до членов коллектива, а также членов семей коллег, а также близких родственников, друзей и знакомых возможные угрозы и меры, направленные на их предотвращение, при использовании социальных сетей ИТКС Интернет.

Проведение руководством или соответствующими должностными лицами модельного агентства работы в интересах обеспечения информационной безопасности в организационном плане выражается в издании

регламентирующих документов. Одним из них является издание приказа по организации – агентству о принятии инструкции по работе с конфиденциальной информацией (прил. 1). Этот приказ является обязательным изданием по работе с конфиденциальной информацией.

Разработка инструкции с приложениями, как правило, возлагается на специальное структурное подразделение агентства, как вариант, – отдел по защите информации (прил. 2) Если такой отдел отсутствует, то документы разрабатываются службой безопасности агентства (или аналогичным подразделением) с привлечением отдела по работе с персоналом.

Другим обязательным документом является перечень конфиденциальной информации, разработанный в агентстве и утвержденный его руководителем (прил. 3).

Следующим обязательным документом следует считать обязательство сотрудника агентства, допущенного к конфиденциальной информации, о неразглашении коммерческой тайны. К примеру,на одном из крупных коммерческих предприятий Подмосковья два года назад произошла утечка информации: одним из сотрудников этого предприятия была продана конкурентам технология изготовления нового напитка (ноу-хау). Служба контроля (СК) предприятия быстро определила, кто совершил хищение информации и ее передачу. Однако привлечь по закону расхитителя информации не удалось. Представители правоохранительных органов отказали в иске и высказали законные претензии в адрес предприятия, так как отсутствовали необходимые документы по закрытию конфиденциальной информации. Руководитель предприятия утверждал, что он лично инструктировал сотрудников, однако отсутствие требуемых обязательных документов не позволило решить вопросв интересах предприятия. Сотрудник был уволен и наказан, но тольков границах законодательной базы предприятия.

ЗАКЛЮЧЕНИЕ

Мировая практика показывает, что неправомерному овладению конфиденциальной информацией любой организации способствуют следующие действия:

- разглашение;
- утечка;
- несанкционированный доступ.

Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других способах обмена деловой и научной информацией. Реализуется разглашение по формальным и неформальным каналам распространения. К формальным коммуникациям относятся деловые встречи, совещания, переговоры и другие формы общения, обмен официальными деловыми и научными документами, средствами передачи официальной информации (почта (в том числе электронная), телефон, телеграф и др.).

Неформальные коммуникации включают: личное общение (встречи, переписка и т.д.), выставки; семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газеты, интервью, радио, телевидение и др.). Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Тут важно отметить, что главным субъектом в этом процессе выступает источник (владелец) охраняемых секретов.

Утечка информации осуществляется по различным техническим каналам. Известно, что информация вообще переносится или передается либо энергией, либо веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги (написанный, напечатанный текст, схема, рисунок).

С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому классифицируются и каналы утечки информации: визуально-оптические, акустические, электромагнитные и материально-вещественные. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям.

Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

Несанкционированный доступ к источникам конфиденциальной информации реализуется различными способами: к примеру, такими, как инициативное сотрудничество, склонение к сотрудничеству, выведывание (выпытывание), подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, подключение к линиям связи, негласное ознакомление, фотографирование и сбор и аналитическая обработка. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения в виде стационара или в подвижном варианте. Это и есть тот самый поток уязвимостей λ, который был описан в исследовании математически. Такое многообразие способов несанкционированного доступа к источникам конфиденциальной информации требует некоторой оценки их распространенности. В зарубежных и отечественных материалах приводятся лишь отдельные показатели соотношения способов несанкционированных действий. Отдельные данные из них приведены в табл. 3.

Как видно из приведенных данных, 52% способов несанкционированного доступа реализуется посредством технических средств промышленного

шпионажа, 43% – с использованием человеческого фактора и 5 % приходится на съем информации через другие случайные каналы.

Таблица 3

Показатели несанкционированного съема информации

Способы несанкционированного съема информации	%
1. Подкуп, шантаж, переманивание сотрудников, внедрение агентов	43
2. Подслушивание телефонных переговоров	5
3. Кража документов	10
4. Проникновение в ПЭВМ	13
5. Съем информации с линии связи	24

Может ли организация– модельное агентство противостоять этому? Да, может. В целях защиты конфиденциальной информации агентствомдолжно предприниматься следующее:

- создавать организационные структуры по защите конфиденциальной информации;

- издавать нормативные и распорядительные документы, относящие информацию к конфиденциальной и механизмы ее защиты;

- включать требования защиты информации в договорыи контракты по всем видам деятельности;

- распоряжаться своей информацией в целях извлечения выгоды и недопущения ущерба предприятию;

- требовать защиты интересов агентства со стороны государственных и судебных органов.

Кроме того, создаваемое специализированное подразделение агентства должно выполнить решать следующие задачи:

- определить круг сотрудников, которым необходим доступ к конфиденциальной информации для выполнения служебных задач;

- определить перечень сторонних организаций, использующих информацию агентства для решения совместных задач;

- выявлять лиц не допущенных, но проявляющих к конфиденциальной информации повышенный интерес;

- выявлять источники внешних угроз со стороны конкурентов, криминальных структур и т.п.;

- определять уязвимые участки (параметр **μ**) в системе информационной безопасности агентства с точки зрения утраты секретов;

- определять зоны, закрытые для посещения посторонними лицами;

- определять меры правовой, организационной и технической защиты секретов;

- обучать сотрудников агентства мерам безопасностии сохранению конфиденциальной информации;

- давать оценку состояния информационной безопасности агентства и вносить предложенияпо ее совершенствованию и внедрению в жизнь.

Руководству модельного агентства следует помнить, что в основу защиты информации должны быть положены принципы: максимального ограничения числа сотрудников, допущенных к конфиденциальной информации; персональной ответственности за сохранность информации и разработку мер ее защиты; воспитательной работы с кадрами в плане сохранения коммерческой тайны организации.

Исходя из практики деятельности ведущих организаций России, можно сказать, что главными направлениями защиты информации при работе с персоналом являются:

- привитие сотрудникам навыков сохранения тайны;

- создание обстановки нетерпимости к болтунам;

- контроль за всеми видами переговоров со сторонними лицами;

- контроль открытых публикаций, выступлений, интервью;

- контроль телефонных разговоров сотрудников на служебные темы;

- изучение поведения сотрудников во внеслужебное время, если оно вызывает подозрения.

Естественно, что при этом не должны нарушаться конституционные нрава и свободы личности. Лучшим средством сохранения секретов является лояльность служащих своейорганизации – модельному агентству и сообщение руководству о всех случаях нарушения правил безопасности и утечки секретов.

Соответственно вся работа по обеспечению информационной безопасности, включая создание и развертывание системы информационной безопасности, должна осуществляться на основе не только личного опыта должностного лица ведущего ее и требований нормативных правовых документов. В этой работе просто необходимо применять наработанный человечеством математический аппарат, как вариант – примененный в данном исследовании.

Математический аппарат позволит осуществить формальное проектирование системы защиты информационных систем и произвести оценку их эффективности. К основным преимуществам рассмотренного метода моделирования и проектирования систем защиты можно отнести то, что для решения рассматриваемых задач выявления и нивелирования угроз информационной безопасности не требуются какие-либо экспертные оценки – при моделировании используются лишь стохастические значения параметров безопасности уязвимостей (угроз уязвимостей), в отношении которых имеется вся необходимая статистика.

Важность этого подхода становится очевидной, если понять суть экспертных оценок.

Для этого, прежде всего, следует ответить на вопрос: при каких условиях и с какой цельюиспользуются экспертные оценки? Ответ крайне прост: в том случае, когда разработчикам соответствующих математических моделей не удается математически смоделировать какиелибо параметры или характеристики системы, цель также очевидна – хоть как-то количественно задать значения требуемых параметров/характеристик. Другими словами,использование экспертных оценок – это от «безысходности» – от невозможности решения требуемых задач математическими методами.

При этом одна неопределенность подменяется другой, причем порою возникает вопрос: что сложнее экспертно оценить –некое моделируемое совокупное качество системы либо некое ее локальное качество?

Ключевой недостаток использования экспертных оценок в математических моделях обусловливается принципиальной невозможностью какого-либо оценивания адекватности получаемых в итоге результатов, т.е. проектные решения должны приниматься, исходя из принципиальной невозможности ответа на вопрос:на сколько результаты моделирования соответствуют действительности?

Дело в том, что основную погрешность в подобных эвристически-математических (математическими их назвать никак нельзя) методах моделирования несет в себе именноэкспертное задание значений требуемыхпараметров/характеристик, причем каким-либо образом оценить подобную погрешность не представляется возможным. Исходить же при моделировании из концепции «абсолютно квалифицированного эксперта» не совсем разумно. Где ж такого найти, особенно в такой сложной области знаний, как информационная безопасность?

На практике методы моделирования, предполагающие экспертное оценивание каких-либо параметров/характеристик системы, могут и осознано эксплуатироваться недобросовестными проектировщиками систем защиты информационных систем. Ввиду того, что современная концепция построения системы защиты информационной системы предполагает реализацию защиты от актуальных угроз, к которым экспертным путем относятся соответствующие угрозы из набора потенциально возможных угроз, экспертным путем ту или иную угрозу при проектировании системы защиты можно и не отнести к актуальным для какой-либо информационной системы, ведь нет единой формальной количественной оценки актуальности угрозы – все основывается на некой оценке некоего эксперта, а мнения различных экспертов могут сильно отличаться либо вообще быть противоположными, снизив тем самым затраты на реализацию защиты, естественно, снизив при этом и эффективность защиты.

При наличии же формальной количественной оценки актуальности угрозы подобное становится уже невозможным.

Важнейшим результатом проведенного исследования является обоснование невозможности эффективного использования известных из теории надежности методов резервирования элементов информационной системы для решения как задач повышения уровня информационной безопасности, так и задачи повышения уровня интегрированной информационно-эксплуатационной безопасности информационной системы.

В качестве компромиссного решения смоделирована возможность резервирования с разделением обработки информации между элементами системы. Вместе с тем недостатки данного метода резервирования обусловливают необходимость дальнейшего исследования этих ключевых вопросов (вопросов резервирования элементов) построения защищенных информационных систем.

Таким образом, результаты исследования позволяют заключить, что вопросы информационной безопасности деятельности организации являются сложными, объемными по проводимым мероприятиям и многогранными. Следовательно, подходить к решению этих вопросов необходимо комплексно, с ведением непрерывного отслеживания изменений в текущей обстановке и проведением ее объективной оценки.

Проведенные исследования нельзя назвать окончательными. Работу в данной области целесообразно продолжить для выработки новых подходов к реализации эффективной и корректной защиты информации в рамах деятельности модельного агентства.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые акты:

1. Военная доктрина Российской Федерации. Утверждена Президентом Российской Федерации 25 декабря 2014 г. № Пр-2976 // КонсультантПлюс. 2018. Режим доступа: http:// consultant.ru

2. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 5 декабря 2016 г. № 646 // КонсультантПлюс. 2018. Режим доступа: http:// consultant.ru

3. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утверждены Президентом Российской Федерации 24 июля 2013 г. № Ир-1753 // КонсультантПлюс. 2018. Режим доступа: http://consultant.ru

4. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена Президентом Российской Федерации 9 мая 2017 года № 203 // КонсультантПлюс. 2018. Режим доступа: http:// consultant.ru

5. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации, 2009.

6. ГОСТ Р ИСО/МЭК 27005 – 2010. Информационные технологии. Методы и средства обеспечения безопасности. Менеджментрискаинформационнойбезопасности. ISO/IEC 27005:2008 Information technology – Security techniques — Information security risk management (IDT). Издание официальное. М.: Стандартинформ – 2011.

7. ГОСТ Р ИСО/МЭК 27000 – 2021. Информационные технологии. Методы и средства обеспечения безопасности системы менеджмента информационной безопасности. Общийобзоритерминология. (Information technology. Security techniques. Information security management systems. Overview and vocabulary. ISO/IEC 27000:2018, IDT).

8. ГОСТ Р ИСО/МЭК 27001 – 2021. Информационные технологии. Методы и средства обеспечения безопасности. Системыменеджментаинформационнойбезопасности. Требования (Information technology. Security techniques. Information security management systems. Requirements).

9. ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения (Protection ofinformation. Object of informatization. Factorsinfluencingtheinformation. Generaloutlines)

10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Нормативный документ ФСТЭК России, 2008.

11. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. № 17.

12. Конституция Российской Федерации от 12 декабря 1993 г. (с поправками от 30 декабря 2008 г., 5 февраля, 21 июля 2014 г.) // КонсультантПлюс. 2018. Режим доступа: http://consultant.ru

13. Федеральный закон от 26 января 1996 года № 14-ФЗ «Гражданский кодекс Российской Федерации» (ред. от 03.08.2018) // КонсультантПлюс. 2018. Режим доступа: http://consultant.ru

14. Федеральный закон от 13 июня 1996 года № 63-ФЗ «Уголовный кодекс Российской Федерации» (ред. от 02.10.2018) // КонсультантПлюс. 2018. Режим доступа: http:// consultant.ru

15. Федеральный закон от 18 декабря 2001 года № 174-ФЗ «Уголовно-процессуальный кодекс Российской Федерации» (ред. от 02.10.2018) // КонсультантПлюс. 2018. Режим доступа: http:// consultant.ru

16. Федеральный закон от 30 декабря 2001 года № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях»

(ред. от 02.10. 2018) // Консультант! 1люс. 2018. Режим доступа: http:// consultant.ru

17. Федеральный закон от 30 декабря 2001 года № 197-ФЗ «Трудовой кодекс Российской Федерации» (ред. от 03.10.2018) // КонсультантПлюс. 2018. Режим доступа: http://consultant.ru

18. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (ред. от 19.07. 2018) // КонсультантПлюс. 2018. Режим доступа: http:// consultant.ru

19. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // КонсультантПлюс. 2018. Режим доступа: http://consultant.ru

20. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» (ред. от 5 октября 2015 г.) // КонсультантПлюс. 2018.Режим доступа: http://consultant.ru

21. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» (ред. от 5 октября 2015 г.) // КонсультантПлюс. 2018.Режим доступа: http:// consultant.ru

22. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «Об утверждении Стратегии национальной безопасности Российской Федерации» // КонсультантПлюс. 2018. Режим доступа: http:// consultant.ru

23. Федеральный закон от 26 июля 2017 № 178-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Гарант. 2018. Режим доступа: http:// www.garant.ru

24. Указ Президента Российской Федерации от 10 ноября 2018 г. № 648 «Об утверждении состава Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям»// КонсультантПлюс. 2019. Режим доступа: http:// consultant.ru

Книги и периодические издания:

25. Аксенов С.В., Галушкин И.Б., Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Ч. II. Правовые и организационные основы информационной безопасности (защиты информации): учеб, пособие. М.: ВА РВСН им. Петра Великого, 2015. 395 с.

26. Андрей Смирнов. Дональд Трамп создал комиссию по вопросам искусственного интеллекта. Режим доступа: http://high-tcch.plus

27. Большая советская энциклопедия (в 30 т.) / гл. ред. А.М. Прохоров. 3-е изд. М.: Советская энциклопедия, 1975. Т. 20. 608 с.

28. Буренок Василий. Убить интеллектом. Режим доступа: http://vpk-news.ru/articlcs/39I04

29. Василий Пискарев. Безопасность требует ответственности. Режим доступа: http://journal.ib-bank.ru/2018/X2 4 (31)

30. Выступление Владимира Путина на Пленарном заседании Международного конгресса по кибербезопасности. Режим доступа: http://www. kremlin.ru/events/president/news/57957/

31. Выступление Н.И. Касперской на Цифровом форуме 2018 Санкт-Петербург. Режим доступа: http://aftershock.news

32. Выступление Н.Н. Мурашова на 21-м Большом национальном форуме информационной безопасности «Инфофорум-2019». Москва. Режим доступа: http://www.infoforum2019.ru/ 30.04.2019.

33. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учеб, пособие. СПб.: СПбГУ ИТМО, 2009.84 с.

34. Доронин А.И. Бизнес-разведка. 2-е изд., перераб. и доп. М.: Ось-89, 2003. 384 с.

35. Козлов Е.С. К вопросу о применении искусственного интеллекта в военной сфере (по опыту США)//Научный сборник ВАГШ ВС РФ. 2019. № 79. С. 131-141.

36. Литвиненко В.И. Безопасность торговли. М.: Баярд, 2005./ 246 с.

37. Наталья Касперская: Интернет вещей – катастрофическая штука с точки зрения информационной безопасности // Российская газета. Федеральный выпуск № 7298 (132), 2018.

38. Национальная стратегия кибербезопасности США. М.: ГШ ВС РФ, 2018.25 с.

39. Новиков В.К. Организационное и правовое обеспечение информационной безопасности. Ч. I. Правовое обеспечение информационной безопасности: учеб, пособие. М.: МИЭТ, 2013.184 с.

40. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. М.: Азъ, 1994,928 с.

41. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения: учеб, пособие. М.: Горячая линия – Телеком, 2015. 176с.

42. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» /[Рогозин В.Ю. и др.]. М.: ЮНИТИ-ДАНА, 2016.287 с.

43. Отчет «Kaspersky Lab» об угрозах информационной безопасности промышленных предприятий. 28 марта 2018 г. // РИА «Новости».

44. Словарь-справочник по информационной безопасности. Минск: Ин-г нац. безопасности Республики Беларусь, 2015. Т. 2. 248 с.

45. Советский энциклопедический словарь / гл. ред. А.М. Прохоров. 4-е изд. М.: Советская энциклопедия, 1989. 1632 с.

46. Философский словарь / под ред. И.Т. Фролова. 4-е изд. М.: Политиздат, 1980.444 с.

47. Щеглов А.Ю., Щеглов К.А. Математическое моделирование и методы формального проектирования систем защиты информационных систем. Учебное пособие. – СПб: Университет ИТМО, 2015.

Издания на иностранных языках:

48. Summary of the 2018 Department of defense artificial intelligence strategy. Washington, U.S. Department of Defense, 2018.

Интернет-источники:

49. Итоги 2013: угрозы и эксплуатация Windows [Электронный ресурс]. Режим доступа http://www.habrahabr.ru/company/eset/blog/209694/, свободный (02.04.2014).

50. Отчет по уязвимостям 20.02-26.02 2012 [Электронный ресурс]. Режим доступа: URL:/ http://www.securitylab.ru/vulnerability/reports/420676.php, свободный (02.04.2014).

51. Шебанова Н.А. «Модное» право. Норма, 2018. 176 с. ISBN: 978-5-91768-892-3.

52. Дорофеева А.М. Интеллектуальная собственность в шоу-бизнесе, моде и спорте. Проспект, 2021. 144 с. ISBN: 978-5-392-33404-9.

53. Let Know. URL: https://letknow.news/news/ssha-vozmut-na-vooruzhenie-iskusstvennyy-intellekt-17940.html

54. Путин призвал российские IT-компании окончательно отказаться от иностранного программного обеспечения и «железа». Режим доступа: http:// classic.newsru.com/nissia/08sep2017/ rusoftware.html/8 сентября 2017 г.

55. Топ-10 стратегических трендов в области технологий па 2019 год. Режим доступа: http://cismag.ru/2018/X2 4.

ПРИЛОЖЕНИЯ

Приложение 1

ПРИКАЗ

№ ___

« » _____ 20___ г. г. Москва

Об утверждении «Инструкции о порядке учета, обращения и хранения документов и дел, содержащих конфиденциальные сведения»

В целях обеспечения сохранности конфиденциальной информации на предприятиях группы ПРИКАЗЫВАЮ:

1 Утвердить «Инструкцию о порядке учета, обращения и хранения документов и дел, содержащих конфиденциальные сведения» (далее – Инструкция) и Приложения №№ 1, 2 к ней.

2. Руководителям структурных подразделений агентства:

2.1. Принять к руководству и исполнению Инструкцию и Перечень.

2.2. Назначить своим приказом (решением) лиц, ответственных за учет и хранение конфиденциальных документов и других носителей конфиденциальных документов и носителей конфиденциальной информации.

2.3. Определить в месячный срок перечень основных документов, на которых должны проставляться грифы «Конфиденциально» или «Строго конфиденциально». Утвержденные перечни представить в Отдел по защите информации.

2.4.Внести в должностные инструкции работников записи об их обязанностях и ответственности за соблюдение установленных требований обращения с конфиденциальной информацией.

Срок – 2 недели (к __ _____ 20__ г.).

2.5.Организовать в декадный срок ознакомление с Инструкцией работников подразделений под роспись.

3. Контроль за соблюдением установленных Инструкцией требований при работе с документами с грифом «Конфиденциально»и «Строго конфиденциально» возложить на Отдел по защите информации. Для документов в электронном виде – на Технический отдел.

Генеральный директор модельного агентства

Приложение 2

ИНСТРУКЦИЯ

о порядке учета, обращения и хранения документов и дел, содержащих конфиденциальные сведения

1.Общие положения

1.1. Настоящая Инструкция разработана в соответствиис требованиями Гражданского Кодекса Российской Федерации, Федеральною Закона «Об информации, информатизации и защите информации»от 20.02.1995 г. № 24-ФЗ, Указа Президента Российской Федерации«Об учреждении перечня сведений конфиденциального характера»от 06.03.1996 г.№ 188, Постановлений Правительства Российской Федерации, Федерального закона от 29.07.2004 г. № 98-ФЗ и Устава модельного агентства.

1.2. Инструкция устанавливает единый порядок работыс документами и другими материальными носителями информации (далее «документами»), содержащими конфиденциальную информацию, и является документом, обязательным для выполнения всеми работниками агентства.

1.3. К конфиденциальной информации относится документированная информация, содержащая служебную, коммерческую тайну или персональные данные, доступ к которой ограничивается в соответствиис законодательством Российской Федерации.

Порядок отнесения сведений к категории конфиденциальных определяется разделом 2 настоящей Инструкции.

Требования Инструкции не распространяется на порядок обращения с документами, содержащими сведения, составляющие государственную тайну.

На документах, содержащих конфиденциальные сведения, проставляется гриф «Конфиденциально» или «Строго конфиденциально».

1.4. Запрещается публиковать материалы с грифом «Конфиденциально» или «Строго конфиденциально» в открытой печати, переписке, использовать в передачах по радио и телевидению, в публичных выступлениях до снятия

в установленном порядке грифа «Конфиденциально» или «Строго конфиденциально» или без разрешения руководства.

1.5. Передача материалов с грифом «Конфиденциально» или «Строго конфиденциально» иностранным учреждениям, фирмам или направление их за границу допускается в каждом конкретном случае только на основании письменного разрешения руководства.

1.6. Руководители подразделений несут персональную ответственность за обеспечение сохранности сведений, содержащихсяв документах с грифом «Конфиденциально» или «Строго конфиденциально» в вверенных им подразделениях.

1.7. Непосредственное ведение делопроизводства документовс грифом «Конфиденциально» или «Строго конфиденциально» и контроль за сохранностью документов на предприятиях возлагается на лиц, ответственных за ведение делопроизводства.

1.8. Контроль за соблюдением предусмотренных настоящей Инструкцией требований при работе с документами с грифом «Конфиденциально» или «Строго конфиденциально» возлагается на делопроизводителей и Отдел по защите информации.

2. Порядок отнесения сведений к категории конфиденциальных

2.1. Присвоение грифа «Конфиденциально» или «Строго конфиденциально» производится исполнителем на основании «Перечня конфиденциальных сведений» (далее «Перечня сведений» – Приложение № 3).

2.2. Перечень сведений создается на основе предложений руководителей подразделений агентства.

Перечень сведений (дополнения и изменения к нему) утверждается и вводится в действие приказом Генерального директора модельного агентства.

2.3. Конфиденциальные сведения, возникшие в результате совместной деятельности подразделений агентства и его партнеров, должны быть оговорены в договоре (отдельном протоколе), где также отражаются взаимные обязательства и ответственность сторон за их сохранность. Решение о снятии

с документов грифа «Конфиденциально» или «Строго конфиденциально» в этом случае может быть принято толькопо согласованию сторон.

2.4. Если сведения не предусмотрены указанным Перечнем, но, по мнению исполнителя, их разглашение может быть использованов ущерб интересам агентства, он совместно с руководителем подразделения представляет Генеральному директору аргументированные предложения о необходимости защиты этих сведений и внесении соответствующих дополнений в Перечень. До принятия окончательного решения защита данных сведений должна быть обеспечена в соответствиис требованиями настоящей Инструкции.

2.5. Конфиденциальные сведения утрачивают необходимость защиты:

- по окончании установленного Перечнем сведений срока;

- по соглашению заинтересованных сторон, установивших эти ограничения;

- в иных случаях, определяемых лицом, подписавшим (утвердившим) документ, содержащий эти сведения.

Исполнителям документов с грифом «Конфиденциально» или «Строго конфиденциально» предоставляется право по истечении срока действия грифа снимать документы с особого учета. При этом зачеркивается гриф «Конфиденциально» или «Строго конфиденциально», что заверяется подписями исполнителя и работника, ответственного за учет.

Решение о снятии грифа до истечения срока его действия принимает должностное лицо, подписавшее (утвердившее) этот документ или его правопреемник, что заверяется его подписью на документе с указанием даты.

Аннулирование грифа «Конфиденциально» или «Строго конфиденциально» отражается в журнале регистрации.

О снятии грифа извещаются подразделения агентства (партнеры), в которые рассылался этот документ.

3. Доступ работников к конфиденциальным сведениям

3.1. Работники, поступившие на работу в модельное агентство, дают письменное обязательство о неразглашении конфиденциальных сведений, которое хранится в их личных делах.

3.2. Руководитель подразделения, в которое принимается на работу работник, или уполномоченное руководителем лицо проводят инструктаж работника о требованиях по сохранению конфиденциальных сведений, предусмотренных настоящей Инструкцией.

3.3. Обязанность работника соблюдать требования настоящей Инструкции, а также ответственность за разглашение конфиденциальных сведений предусматривается в должностных инструкциях работников агентства.

4. Обязанности работников, допущенных к конфиденциальным сведениям

4.1. Работники агентства обязаны:

- знать и выполнять требования настоящей Инструкции;

- знать Перечень сведений по подразделениям агентства;

- хранить в тайне известные им конфиденциальные сведения, информировать руководителя подразделения и Отдел по защите информации о фактах нарушения порядка обращения с конфиденциальными сведениями, о попытках несанкционированного доступа к информации;

- соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц;

- знакомиться только с теми служебными документами, к которым получен доступ в силу исполнения прямых служебных обязанностей;

- о допущенных нарушениях установленного порядка работы, учета и хранения документов, а также о фактах разглашения конфиденциальных сведений представлять письменные объяснения.

4.2. Работникам подразделений запрещается:

- использовать конфиденциальные сведения при ведении телефонных переговоров, передавать документы с грифом «Конфиденциально» и «Строго конфиденциально» но каналам факсимильной связи;

- использовать конфиденциальные сведения в личных интересах;

- снимать копии с документов и других носителей информации, содержащих конфиденциальные сведения, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру) для записи конфиденциальных сведений без разрешения руководителя предприятия;

- выполнять на дому работы, связанные с конфиденциальными сведениями;

- выносить документы и другие носители информации с грифом «Конфиденциально» шли «Строго конфиденциально» из здания агентства без письменного разрешения руководства.

5. Порядок обращения с документами, содержащими конфиденциальные сведения:

5.1. Делопроизводство документов, содержащих конфиденциальные сведения, осуществляется в соответствии с требованиями настоящей Инструкции, а также Инструкции по делопроизводству предприятий.

5.2. На документах и на их проектах, содержащих конфиденциальные сведения, проставляется гриф «Конфиденциально» или «Строго конфиденциально».

Указанный гриф и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также па первой странице сопроводительного письма к таким документам.

Использовать другие ограничительные пометки или грифы («Коммерческая тайна» и т.п.) запрещается.

5.3. Документы (письма, справки, организационно-распорядительные документы) с грифом «Конфиденциально» или «Строго конфиденциально» –

регистрируются в журналах входящей или исходящей корреспонденции. При этом к номеру добавляется пометка «К» или «СК»;

- на последнем листе (как правило, на обратной стороне) должно быть указано: количество отпечатанных экземпляров, фамилия исполнителя, номер его телефона и дата печати. Отпечатанныеи подписанные документы вместе с черновиками передаютсядля регистрации работнику, осуществляющему их учет. Черновикии варианты уничтожаются этим работником с отметкой об уничтожении в журнале регистрации. Неподписанные по каким-либо причинам документы уничтожаются лично исполнителем;

- после регистрации передаются работникам предприятий под расписку в журнале или по реестру, подписанному руководителями предприятий;

- размножаются (тиражируются) на основании подписи руководителей подразделений. Учет размноженных документов осуществляется поэкземплярно;

- хранятся в надежно запираемых и опечатываемых шкафах.

5.4. Требования пунктов 5.1 – 5.3 настоящей Инструкции распространяются на машинные носители информации, содержащие конфиденциальные сведения.

5.5. При необходимости направления документов с грифом «Конфиденциально» или «Строго конфиденциально» в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Рассылка подписывается руководителем подразделения, готовившего документ.

5.6. Исполненные документы с грифом «Конфиденциально» или «Строго конфиденциально» группируются в дела в соответствии с номенклатурой дел общего делопроизводства. На обложке дела, в которое помещены такие документы, также проставляется гриф «Конфиденциально» или «Строго конфиденциально», и соответствующее уточнение вносится в номенклатуру дел.

5.7. Уничтожение дел и документов с грифом «Конфиденциально» или «Строго конфиденциально», утративших свое практическое значение и актуальность, производится по актам, утвержденным руководителем подразделения. В журнале регистрации об этом делается отметка со ссылкой на соответствующий акт.

5.8. Передача документов и дел с грифом «Конфиденциально» или «Строго конфиденциально» между подразделениями осуществляется:

- во временное пользование — с разрешения соответствующего руководителя с отметкой в журнале регистрации;

- для исполнения в другие подразделения – через делопроизводителей.

При увольнении работника все находящиеся у него неисполненные документы передаются по указанию руководителя подразделения по акту другому исполнителю с обязательной отметкойв журнале регистрации.

5.9. Проверка наличия документов и дел с грифом «Конфиденциально» или «Строго конфиденциально» проводится один разв год комиссией, назначаемой Генеральным директором. В состав таких комиссий обязательно включаются работники, ответственные за учети хранение этих материалов.

Результаты проверки оформляются актом.

6. Защита конфиденциальной информации, обрабатываемой на средствах ПВЭМ.

6.1. Доступ к работе на персональныхэлектронно-вычислительных машинах (компьютерах), когда они не используются, необходимо закрыть с помощью пароля.

6.2. Пользователи должны знать правила доступа к программным ресурсам, действующим в агентстве. Пользователи информационных систем обязаны регистрировать отклонения в работе программы и сообщать об этом сетевому администратору.

7. Ответственность за разглашение конфиденциальных сведений, утрату документов, содержащих таких сведения, и нарушение порядка работы с ними.

7.1. Ответственность за разглашение конфиденциальных сведений несет персонально каждый работник, имеющий доступ к этим сведениям и допустившим их утечку.

7.2. О факте разглашения конфиденциальных сведений руководитель подразделения немедленно ставит в известность Отдел по защите информации и создает комиссию для служебного расследования.

7.3. Комиссия, проводящая служебное расследование, устанавливает:

- обстоятельства разглашения конфиденциальных сведений;

- виновных в разглашении конфиденциальных сведений;

- причины и условия, способствующие разглашению конфиденциальных сведений.

7.4. Служебное расследование проводится в минимально короткий срок, но не более одного месяца со дня обнаружения факта разглашения конфиденциальных сведений.

Одновременно с работой комиссии принимаются меры по локализации нежелательных последствий из-за разглашения конфиденциальных сведений.

7.5. Руководство агентства принимает решениео применении дисциплинарного взыскания к виновным лицам не позднее одного месяца после обнаружения факта разглашения конфиденциальных сведений.

7.6. Разглашение конфиденциальных сведений влечет за собой ответственность, предусмотренную действующим законодательством и трудовым договором (контрактом) между администрацией и работником.

7.7. При наличии в действиях лица, разгласившего конфиденциальные сведения, признаков уголовного преступления руководство группы предприятий имеет право обращенияв правоохранительные органы для привлечения его к ответственностив соответствии с действующими нормативными правовыми актами.

7.8. При причинении работником, разгласившим конфиденциальные сведения, убытков, нанесении ущерба деловой репутации и при отказе

добровольно возместить причиненный вред руководство группы предприятий имеет право обратиться в суд за защитой своих прави интересов.

7.9. При выявлении нарушения требований порядка обращения с конфиденциальными сведениями к лицу, допустившему нарушение, применяются меры дисциплинарного взыскания.

Утверждено Приказом

Приложение 3

УТВЕРЖДАЮ

Генеральный директор

модельного агентства «_____»

И. Фамилия

« » _____ 20__ г.

ПЕРЕЧЕНЬ

конфиденциальных сведений

1. Сведения о структуре производства, производственных, коммерческих мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции.

2. Сведения о подготовке, принятии и исполнении отдельных решений руководства агентствапо коммерческим, организационным, производственным, научно-техническим и иным вопросам.

3. Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях.

4. Те же сведения о планах инвестиций, закупок, демонстраций, продаж.

5. Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления агентства.

6. Сведения о балансах агентства.

7. Сведения о кругообороте средств агентства.

8. Сведения о финансовых операциях агентства.

9. Сведения о состоянии банковских счетов агентства и производимых операциях.

10. Сведения об уровне доходов агентства.

11. Сведения о долговых обязательствах агентства.

12. Сведения о состоянии кредита агентства (пассивы и активы).

13. Сведения о результатах изучения рынка, содержащие оценку состояния и перспектив развития рыночной конъюнктуры.

14. Сведения о рыночной стратегии агентства.

15. Сведения о применяемых агентством оригинальных методах осуществления продаж.

16. Сведения об эффективности коммерческой деятельности агентства.

17. Систематизированные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах деловых отношений агентства, а также о его конкурентах, которые не содержатся в открытых источниках (справочниках, каталогах и др.).

18. Сведения, условия конфиденциальности которых установлены в дот-ворах, контрактах, соглашениях и других обязательствах агентства.

19. Сведения о методах расчета, структуре, уровне цен на продукцию и размерах скидок.

20. Сведения о подготовке к торгам или аукциону и их результатах.

21. Сведения о целях, задачах, программах перспективных научных исследований.

22. Ключевые идеи проводимых научно-исследовательских (НИР) работ.

23. Точные значения конструкционных характеристик создаваемых изделий (образцов) и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, рецептура, температура, давление, время и т.п.).

24. Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи.

25. Данные об условиях экспериментов и оборудования, на котором они проводились.

26. Сведения о материалах, из которых изготовлены отдельные детали.

27. Сведения об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект.

28. Сведения о методах защиты от подделки товарных знаков.

29. Сведения о состоянии программного и компьютерного обеспечения.

30. Сведения о порядке и состоянии организации защиты конфиденциальной информации.

31. Сведения об организации охраны, пропускном режиме, системе сигнализации, о наличии технических средств контроля и управления доступом.

Начальник отдела информационной безопасности

И.Фамилия

« » _____ 20__ г.