Содержание

Введение

Актуальность темы дипломной работы определяется постоянным уровнем проблем связанных с информационной безопасностью. Вопрос информационной безопасности – один из основных для любой организации. Для ее реализации требуется совокупность мероприятий, направленных на обеспечение конфиденциальности, доступности и целостности обрабатываемой информации. Таким образом, информационную безопасность следует понимать как комплекс организационных, программных, технических и физических мер, гарантирующих достижение целостности, конфиденциальности и доступности. Многие угрозы связанные с безопасностью возникают вследствие зависимости организаций от информационных систем и услуг. Взаимодействие сетей общего и частного пользования, а также совместное использование информационных ресурсов затрудняет управление доступом к информации. Вопрос эффективности централизованного контроля возникает в связи с тенденцией использования распределенной системой обработки данных. При проектировании и построении многих информационных систем, довольно часто, вопросы информационной безопасности попросту не учитываются. Уровень безопасности, который достигается только техническими средствами, имеет ряд ограничений и недостатков и, следовательно, должен сопровождаться надлежащими организационными мерами. Для достижения необходимого уровня информационной безопасности требуется реализация комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения. Информация – это актив организации, который имеет ценность и, следовательно, должен иметь необходимый уровень защиты. Цель информационной безопасности заключается в защите информации от широкого диапазона угроз и обеспечение непрерывности бизнеса, минимизации ущерба и получение максимальной

прибыли. В настоящее время все большее количество организаций уделяет внимание вопросам информационной безопасности. Особенно это касается компаний, занимающихся розничной торговлей, таких как ООО «Диамаксис», так как конфиденциальность, целостность и доступность информации являются важными характеристиками непрерывности бизнеса. Комплекс мер направленный на обеспечение информационной безопасности может существенно повлиять на конкурентоспособность, соответствие законодательству, ликвидность и доходность организации. Цель дипломной работы состоит в разработке и внедрении комплекса мероприятий по обеспечению информационной безопасности компьютера и предприятия ООО «Диамаксис» Достижения цели дипломной работы потребовало решения следующих задач: Анализ существующих стандартов и подходов в области обеспечения информационной безопасности. Определение информационной структуры и анализ информационных рисков в ООО «Диамаксис». Разработка комплекса мероприятий по обеспечению информационной безопасности компьютерной системы и предприятия ООО «Диамаксис»

1.1 Краткая характеристика предприятия

ООО «Диамаксис», адрес: Краснодарский край, город Новороссийск, проспект Дзержинского, дом. 199 А, организация зарегистрирована 26.11.2015. Организации присвоены ИНН 2315986327, ОГРН 1152315005798, КПП 231501001. Связи с другими компаниями отсутствуют. Количество совладельцев: 3, директор – Назаренко Ирина Николаевна. Размер уставного капитала 10 000₽. Компания ООО «Диамаксис» принимала участие в 4 тендерах. В отношении компании нет исполнительных производств. ООО «Диамаксис» участвовало в 2 арбитражных делах: в 2 в качестве ответчика. На рисунке 1.1 изображено место нахождения предприятия ООО «Диамаксис» на карте.

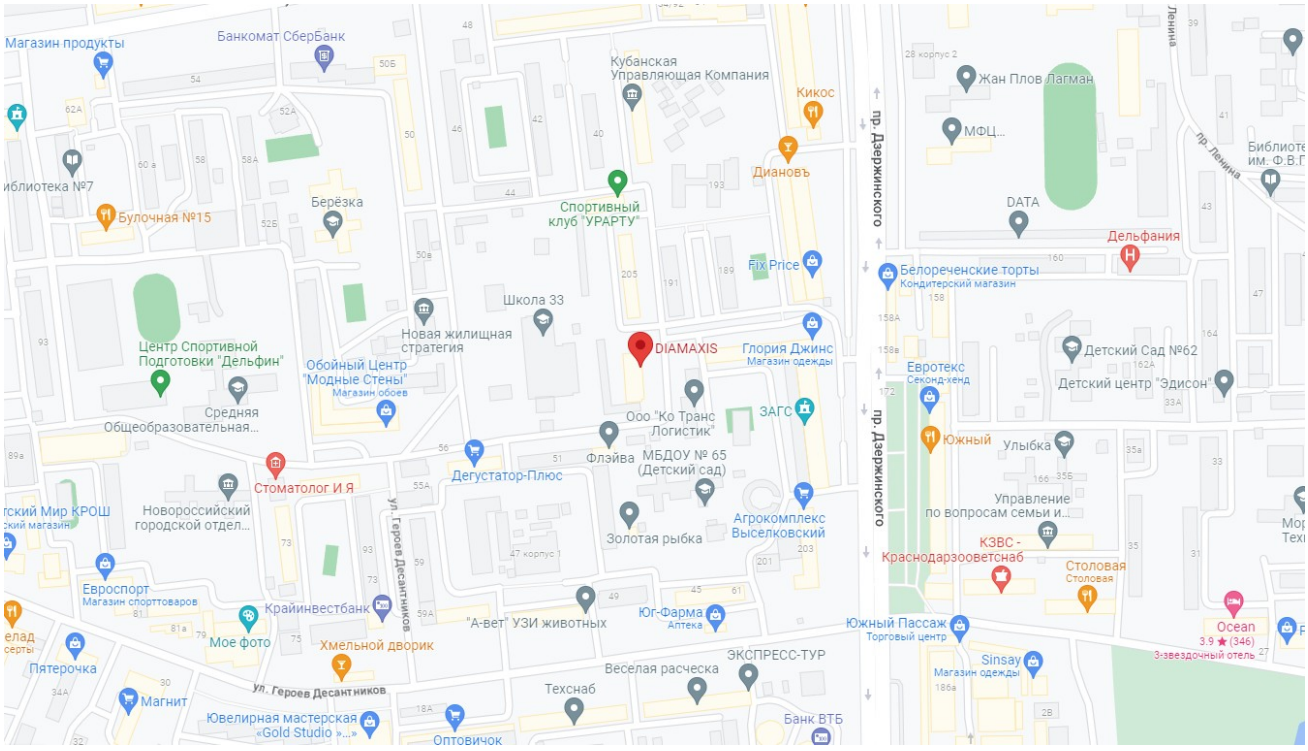

Рисунок 1.1 – Место нахождения предприятия ООО «Диамаксис» на карте

История ООО «Диамаксис» начинается в 1998 году, когда компания Anglo–Swiss Company открыла первый европейский офис в городе Шам, Швейцария. Основатель компании, сам иммигрант из Германии, с самого начала сыграл важную роль в направлении своей компании к международной

экспансии. Компания обязана основателю не только своим именем, а также логотипом и нашим первым продуктом. Он воплощал в себе многие из ключевых взглядов и ценностей, которые составляют неотъемлемую часть корпоративной культуры организации: прагматизм, гибкость, готовность учиться, непредубежденность и уважение к другим людям и культурам.

Основным видом деятельности компании ООО "ДИАМАКСИС" является "Разработка компьютерного программного обеспечения". Компания также зарегистрирована в таких категориях ОКВЭД как "Копирование записанных носителей информации", "Деятельность по письменному и устному переводу", "Ремонт коммуникационного оборудования", "Торговля розничная непродовольственными товарами, не включенными в другие группировки, в специализированных магазинах", "Торговля розничная фотоаппаратурой, оптическими приборами и средствами измерений, кроме очков, в специализированных магазинах" и других.

ОРГАНИЗАЦИОННАЯ СЧТРУКТУРА ПРЕДПРИЯТИЯ!

В организации работают с перечнем документов который нужен для защиты прав организации и её сотрудников. К примеру такими документами являются:

- отчеты о проделанной работе и ее результатах, составленный каждым разработчиком по окончании процесса разработки КП;
- заключения созданные в организации комиссии о пригодности КП в целом к использованию и соответствие ее техническому заданию;
- акты о приеме-передаче нематериальных активов по установленной форме.

ВИД ХРАНИМОЙ ИНФОРМАЦИИ!!!

Для обеспечения эффективной защиты конфиденциальной информации, предприятие ООО «Диамаксис» использует систему управления информационной безопасностью. Это должно быть частью общей системы управления качеством (СУК) организации и должно включать в себя планирование, реализацию, контроль и улучшение процессов управления информационной безопасностью.

Процесс управления информационной безопасностью включает следующие шаги:

- определение области применения и контекста системы управления информационной безопасностью;
- выработка политики информационной безопасности и ее утверждение руководством организации;
- оценка рисков и разработка мер по снижению рисков;
- разработка процедур и инструкций по обеспечению защиты конфиденциальной информации;
- обучение персонала по вопросам информационной безопасности;
- разработка и внедрение системы мониторинга и контроля за соблюдением политики информационной безопасности;
- проведение регулярных аудитов системы управления информационной безопасностью и ее постоянное улучшение.

На предприятии ООО «Диамаксис» высокий уровень безопасности благодаря:

- Использованию локальной сети и полного отказа от Wi–Fi из–за ненадежности защиты от взлома, локальную сеть невозможно взломать, можно только подключиться благодаря чему можно сказать, что предприятие хорошо себя обезопасило;
- Шумогенератору который обычно не работает из–за лишнего шума, но на случай важного совещания или прочей передачи важной устной информации,

его включают для генераций вибраций на окнах, это помогает защититься от прослушивания лазером.

Для безопасности бумажных документов используют специальные метки безопасности, которые помогают предотвратить лишнее распространение информации. При оформлении документов на предприятии ООО «Диамаксис», отметка конфиденциальности является обязательным элементом, если документ содержит информацию, которая должна быть защищена от доступа третьих лиц. Это могут быть документы, содержащие персональные данные или коммерческую тайну.

Отметка конфиденциальности позволяет определить степень ограничения доступа к документу, а также установить ответственность за его раскрытие. Для того чтобы обеспечить максимальную защиту конфиденциальной информации, принято соблюдать требования к хранению и использованию таких документов. Например, хранить их в запираемых шкафах или сейфах, а также использовать пароли для доступа к электронным версиям документов.

Одной из особенностей документирования конфиденциальной информации является регламентирование состава создаваемых конфиденциальных документов. Конфиденциальная документированная информация должна создаваться только при действительной необходимости в письменном удостоверении наличия и содержания управленческих, коммерческих, производственных и иных действий, передаче информации, хранении и использовании ее в течение конкретного времени и в определенном количестве экземпляров. При этом решение задач конфиденциальной деятельности должно обеспечиваться минимальным количеством конфиденциальных документов при сохранении полноты требуемой информации.

На предприятии ООО «Диамаксис», должностные лица имеют право снимать отметку конфиденциальности информации с документов и изданий, подготовленных в данном структурном подразделении, руководствуясь при этом

Перечнем конфиденциальной документированной информации структурного подразделения организации.

После снятия отметки конфиденциальности документ передается в Службу делопроизводства. Об изменении или снятии конфиденциальности делается отметка на самом документе, удостоверяемая визой руководителя, подписавшего этот документ. О внесении в документ такой отметки сообщается заинтересованным лицам, учреждениям, предприятиям и организациям.

При составлении Перечня на предприятии ООО «Диамаксис», необходимо исходить из трех основных принципов: законности, обоснованности и своевременности придания документированной информации конфиденциальности, отнесения конфиденциальной информации к какой–либо тайне (коммерческой, профессиональной, служебной и персональным данным), за исключением государственной тайны.

Принцип законности заключается в соблюдении мер по охране конфиденциальности информации и запрету относить информацию к какой–либо тайне в соответствии с законодательством Российской Федерации и нормативными правовыми документами.

1.2 Организация работы с документами, содержащими конфиденциальные сведения в ООО «Диамаксис»

КОНКРЕТНО ГДЕ

Работники предприятия, допущенные к конфиденциальным сведениям и документам, прежде чем получить доступ к ним, должны пройти инструктаж и ознакомиться с памяткой о сохранении коммерческой тайны предприятия.

Ведение делопроизводства, обеспечивающего учет и сохранность документов, содержащих конфиденциальные сведения, предусматривает выполнение ряда рекомендаций.

Приказом руководителя назначается должностное лицо, ответственное за учет, хранение и использование документов, содержащих конфиденциальные сведения, либо эту работу может выполнять секретарь–референт. Эти лица несут персональную ответственность за утерю документов или утечку информации из них.

В тексте документа так же может быть оговорена конфиденциальность сведений, права предприятия на них, порядок их использования.

Печатание документов содержащих конфиденциальные сведения производится централизованно, в специально отведенном помещении, исключающем доступ посторонних лиц. Отпечатанные и подписанные документы передаются для регистрации должностному лицу, ответственному за их учет. Черновики, файлы документа, уничтожаются, и об этом делается запись на копии документа: «Черновик уничтожен. Подпись. Дата.»

Все документы, содержащие конфиденциальную информацию, должны регистрироваться отдельно от остальной документации в «Журнале регистрации документов содержащих конфиденциальные сведения».

Документы, содержащие конфиденциальные сведения, формируются в отдельное дело (или дела). На внутренней стороне обложки дела пишется список

сотрудников, имеющих право пользования этим делом. Все листы дела нумеруются простым карандашом в правом верхнем углу.

В начале дела подшивается внутренняя опись документов, а в конце дела подшивается заверительный лист.

Хранятся такие дела в сейфе, который опечатывается должностным лицом, ответственным за их сохранность.

Движение документов, содержащих конфиденциальные сведения, должно отражаться в журнале учета выдачи документов, содержащих конфиденциальные сведения, пустой вариант такого журнала изображён на рисунке 1.2.

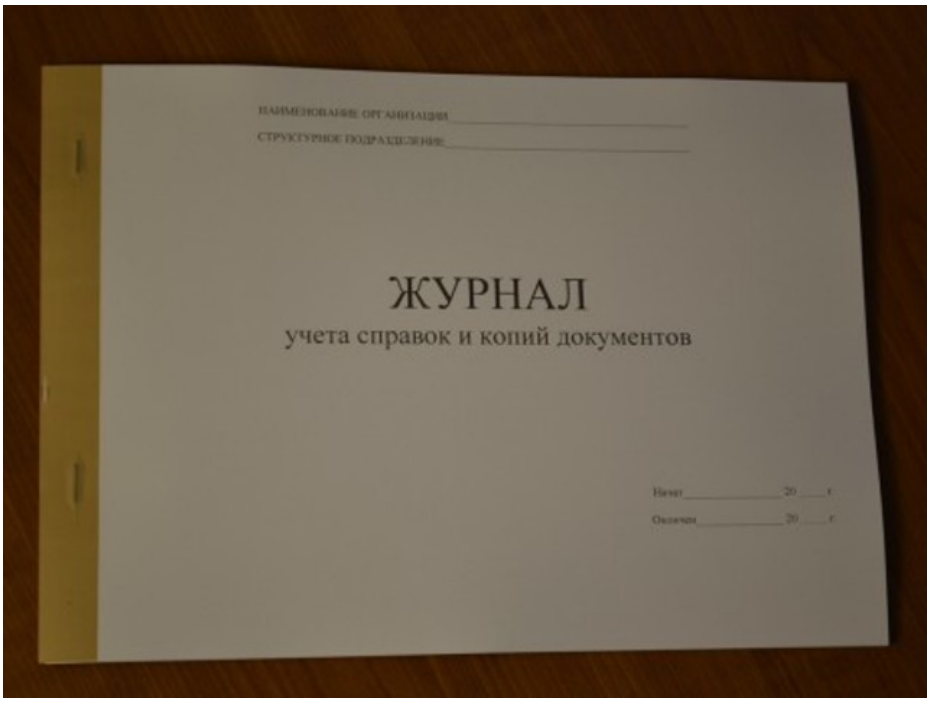

Рисунок 1.2 – Журнал учёта выдачи документов

При выдаче документа секретарем работник, получивший документ, должен сверить номер полученного документа с номером в журнале, проверить количество листов и поставить в журнале свою подпись. Выданные для работы

документы подлежат возврату секретарю–референту в тот же день (если решением руководства не предусмотрено иное).

При возврате документа секретарь–референт сверяет номер документа по журналу, проверяет количество его листов и в присутствии работника ставит в графе «Отметка о возврате» свою подпись и дату возврата документа.

Документы содержащие конфиденциальные сведения должны копироваться с разрешения руководства в специально выделенном помещении. Все копии конфиденциальных документов берутся на учет в специальном журнале или «Журнале регистрации документов содержащих конфиденциальные сведения». Размножение документов следует производить в присутствии должностного лица, ответственного за документ.

Все дела содержащие конфиденциальные сведения, журналы их учета в обязательном порядке вносятся в номенклатуру дел предприятия.

По окончании года специально созданная комиссия предприятия выполняет следующие работы: проверяет наличие всех документов содержащих конфиденциальные сведения; отбирает их для архивного хранения или для уничтожения.

В случае установления факта утраты документов содержащих конфиденциальные сведения немедленно ставится в известность руководитель предприятия, служба безопасности и принимаются все меры к розыску документа. Для расследования факта утраты руководителем предприятия назначается комиссия.

На утерянные документы после того, как розыск их не принес положительных результатов, составляется акт. В «Журнал регистрации документов содержащих конфиденциальные сведения вносятся соответствующие отметки об утрате».

При увольнении сотрудника, ответственного за документы, содержащие конфиденциальную информацию, производится проверка числящихся за ним

документов и их передача вновь назначенному лицу. Акт приема–передачи этих документов утверждается руководителем предприятия или его заместителем.

При прекращении трудовых отношений с предприятием, на котором сотрудник был допущен к конфиденциальной информации, обязательства о не разглашении конфиденциальных сведений действуют в течении 2 лет, если иной срок не установлен трудовым контрактом.

При передаче дел в архив на документы содержащих конфиденциальные сведения составляется отдельная опись.

Архивное хранение таких документов производится в опечатанных коробках, в помещениях, исключающих не санкционированный доступ.

На документы, содержащие конфиденциальные сведения, отобранные к уничтожению, составляется акт, утверждаемый руководителем предприятия. Уничтожаются документы в присутствии комиссии с помощью специальной машины или иным способом, исключающим возможность восстановления имеющейся в них информации.

Регламентация доступа персонала организации к конфиденциальным сведениям, документам и базам данных является одной из главных составных частей технологии защиты информации. важно четко и однозначно определить, кто, кого, к каким сведениям, когда и как допускает.

При разработке разрешительной системы доступа к конфиденциальной информации в полной мере учитываются характер направлений деятельности и структура организации, сложившаяся система управления, производственные связи внутри организации, распределение обязанностей между заместителями первого руководителя организации и другие факторы. Чрезмерные ограничения в выдаче разрешений к защищаемой информации приводят к снижению оперативности в решении производственных вопросов, а излишняя либерализация создаеь условия для утраты конфиденциальной информации.

Количество сотрудников организации, допускаемых к конфиденциальным сведениям, должно быть строго ограничено кругом лиц, которым указанные

сведения действительно необходимы для выполнения возложенных на них служебных обязанностей.

Разрешительная система допуска к конфиденциальной информации обычно разрабатывается службой безопасности организации, а в некрупных фирмах – первыми руководителями.

При этом под допуском понимается процедура оформления права сотрудника организации или иного лица на допуск к сведениям (информации) ограниченного распространения и одновременно правовой акт согласия (разрешения) собственника (владельца) информации на передачу ее для работы конкретному лицу.

Оформление допуска, т.е. согласия лица на определенные ограничения в использовании информации, всегда носит добровольный характер. Наличие допуска предоставляет сотруднику формальное право работать со строго определенным кругом конфиденциальных документов, баз данных и отдельных сведений.

К ценной конфиденциальной информации допускаются, как правило, люди, проработавшие в организации определенное время и зарекомендовавшие себя с положительной стороны.

В предпринимательских структурах разрешение на допуск обычно дает первый руководитель организации. Разрешение оформляется соответствующим пунктом в контракте (трудовом договоре). Допуск может также оформляться приказом первого руководителя с указанием типового состава сведений, с которыми разрешается работать данному сотруднику или группе сотрудников.

Оформление допуска обязательно сопровождается подписанием работником обязательств о неразглашении доверяемых ему конфиденциальных сведений – при поступлении на работу и при увольнении с работы.

Допуск может носить временный характер на период выполнения определенной работы и пересматриваться при изменении профиля работы сотрудника.

Доступ – практическая реализация каждым сотрудником предоставленного ему допуском права на ознакомление и работу с определенным составом конфиденциальных сведений, документов и баз данных.

Разрешение на доступ к конфиденциальным сведениям является всегда персонифицированным – индивидуальным как с точки зрения того, кто дает разрешение, так и с точки зрения того, кому дается такое разрешение. Руководители, имеющие право давать разрешение на доступ, несут персональную ответственность за принятое решение. неправильное решение трактуется как разглашение конфиденциальных сведений.

Сотрудники, работающие с конфиденциальными документами, несут персональную ответственность за сохранение в тайне содержания документов, сохранность носителя и соблюдение установленных правил работы с документами. сотрудники могут получать разрешение на доступ к конфиденциальным сведениям только в пределах своих должностных (функциональных) обязанностей и в объемах, действительно необходимых для выполнения служебных обязанностей.

Разрешение (санкция) на доступ к конкретной информации может быть дано при соблюдении следующих условий:

- наличии подписанного приказа первого руководителя о приеме на работу (переводе, временном замещении, изменении должностных обязанностей и т.п.) или назначении на должность, в состав функциональных обязанносте которой входит работа с данной конкретной информацией;

- наличии подписанного сторонами трудового договора (контракта), имеющего пункт о сохранении тайны организации, и подписанного обязательства о неразглашении ставших известными лицу конфиденциальных сведений и соблюдения правил их защиты;

- прямом отношении функциональных обязанностей сотрудника передаваемым ему документам и информации;

- знании сотрудником требований нормативно–методических документов по защите информации и сохранению тайны;

- наличии необходимых условий в офисе для работы с конфиденциальными документами и базами данных.

Структура процедуры разграничения доступа должна быть многоуровневой, иерархической. Иерархическая последовательность доступа к информации реализуется по принципу «чем выше уровень доступа, тем уже круг допущенных лиц», «чем выше ценность сведений, тем меньшее число сотрудников могут их знать».

В соответствии с иерархической последовательностью доступа определяется структура рубежей защиты информации, которая предусматривает постепенное ужесточение защитных мер по иерархической вертикали возрастания уровня конфиденциальных сведений. Этим обеспечивается недоступность этих сведений для случайных людей, злоумышленников и определяется уровень защищенности информации. Достигается также минимизация привилегий по доступу персонала к информации.

При составлении конфиденциального документа следует учитывать, что его содержание не только определяет функциональное назначение документа, но и лежит в основе разрешительной процедуры доступа персонала к данному документу. Поэтому документ необходимо посвящать только одной тематической группе вопросов, предназначенной по возможности одному конкретному сотруднику или подразделению. Документ, следовательно, должен быть по возможности простым и посвящен одному вопросу.

Для эффективных контрдействий в случае утери информации следует соблюдать правило, по которому в обязательном порядке регистрируются все лица, которые имели или имеют доступ к определенным документам, коммерческим или иным секретам.

Организуя доступ сотрудников организации к конфиденциальным массивам электронных документов, базам данных необходимо помнить о его

многоступенчатом характере. Можно выделить следующие главные составные части доступа этого вида:

- доступ к персональному компьютеру, серверу или рабочей станции;
- доступ к машинным носителям информации, хранящимся вне ЭВМ;
- непосредственный доступ к базам данных и файлам;
- В свою очередь доступ к персональному компьютеру, серверу или рабочей станции, которые используются для обработки конфиденциальной информации, предусматривает:
- определение и регламентацию первым руководителем организации состава сотрудников, имеющих право доступа (входа) в помещение, в котором находятся соответствующая вычислительная техника и средства связи;
- регламентацию первым руководителем временного режима нахождения этих лиц в указанных помещениях; персональное и временное протоколирование (фиксирование) руководителем подразделения или направления деятельности организации наличия разрешения и периода работы этих лиц в иное время (например, в вечерние часы, выходные дни и др.);
- организацию охраны этих помещений в рабочее и нерабочее время, определение правил вскрытия помещений и отключения охранных технических средств информирования и сигнализации; определения правил постановки помещений на охрану; регламентацию работы указанных технических средств в рабочее время;
- организацию контролируемого (в необходимых случаях пропускного) режима входа в указанные помещения и выхода из них;
- организацию действий охраны и персонала в экстремальных ситуациях или при авариях техники и оборудования помещений;
- организацию выноса из указанных помещений материальных ценностей. машинных и бумажных носителей информации; контроль вносимых в помещение и выносимых персоналом личных вещей.

Доступ к машинным носителям конфиденциальной информации, хранящимся вне ЭВМ, предполагает:

- организацию учета и выдачи сотрудникам чистых машинных носителей информации;
- организацию ежедневной фиксируемой выдачи сотрудникам и приема от сотрудников носителей с записанной информацией (основных и резервных);
- определение и регламентацию первым руководителем состава сотрудников, имеющих право оперировать конфиденциальной информацией с помощью компьютеров, установленных на их рабочих местах, и получать в службе КД учтенные машинные носители информации;
- организацию системы закрепления за сотрудниками машинных носителей информации и контроля за сохранностью и целостностью информации, учета динамики изменения состава записанной информации;
- организацию порядка уничтожения информации на носителе, порядка и условий физического уничтожения носителя;
- организацию хранения машинных носителей в службе КД в рабочее и нерабочее время, регламентацию порядка эвакуации носителе в экстремальных ситуациях;
- определение и регламентацию первым руководителем состава сотрудников, не сдающих по объективным причинам технические носители информации на хранение в службу КД в конце рабочего дня, организацию особой охраны помещений и компьютеров этих сотрудников.

Работа сотрудников службы конфиденциальной документации и персонал фирмы в целом с машинными носителями информации вне ЭВМ должна быть организована по аналогии с бумажными конфиденциальными документами.

Доступ к базам данных и файлам подразумевает:

- определение и регламентацию первым руководителем состава сотрудников, допускаемых к работу с определенными базами данных и файлами; контроль системы доступа администратором базы данных;

- наименование баз данных и фалов, фиксирование в машинной памяти имен пользователей и операторов, имеющих право доступа к ним;

- учет состава базы данных и файлов, регулярную проверку наличия, целостности и комплектности электронных документов;

- регистрацию (протоколирование) входы в базу данных или файл, автоматическую регистрацию имени пользователя и времени работы; сохранение первоначальной информации;

- регистрацию (протоколирование) попытки несанкционированного входа в базу данных или файл, регистрацию ошибочных действий пользователя, автоматическую передачу сигнала тревоги охране и автоматическое отключение компьютера;

- установление и бессистемное по сроку изменение имени пользователей, массивов и файлов (паролей, кодов, классификаторов, ключевых слов и т.д.), особенно при частой смене персонала;

- отключение ЭВМ при нарушениях в системе регулирования доступа или сбое системы защиты информации;

- механическое (ключом или иным приспособлением) блокирование отключенной, но загруженной ЭВМ при недлительных перерывах в работе пользователя.

Коды, пароли, ключевые слова, ключи, шифры, специальные программные продукты, аппаратные средства и тому подобные атрибуты системы защиты информации в ЭВМ разрабатываются, меняются специальной организацией и индивидуально доводятся до сведения каждого пользователя работником этой организации или администратором базы данных. Применение пользователями собственных кодов не допускается.

1.3 Угрозы и системы защиты конфиденциальной информации

Любой проект по разработке мобильных приложений в организации связан с определенными рисками той или иной степени. Риски могут различаться в зависимости от характера проекта, но в целом их можно разделить на 5 категорий:

- бюджет: риск превышения выделенного на проект бюджета;
- кадры: риск потери или нехватки членов проектной команды;
- знания: команда может иметь лишь узконаправленные знания, или неверно передавать между собой информацию;
- продуктивность: этот риск чаще всего угрожает долгосрочным проектам;
- время: при разработке программного обеспечения очень распространены задержки релизов продукции, что является результатом неправильного планирования, крайне сжатых сроков и неспособности разработчиков адаптироваться к меняющимся требованиям по отношению к продукту.

Даже в среде гибкой разработки от них не застрахован никто: риски возникают из-за ошибок проектной команды, неверного планирования, сбоев в рабочем процессе и неожиданных изменений в процессе работы над продуктом, тем не менее в ООО «Диамаксис» нашли способы управления такими рисками.

Проблемы с бюджетом они решают с помощью метода «набегающей волны». Команды принимают решения по продукту по мере продвижения работы, вместо того, чтобы разрабатывать подробнейший план действий на

самом старте проекта. Действенные решения, принятые на основе новых знаний о развитии продукта, снижают вероятность рисков, связанных с бюджетом, так как команде не нужно тратить время и ресурсы на повторное планирование.

Риски с кадрами и знаниями решаются с помощью разделения работников на несколько команд. Идеальная команда для разработки ПО – пара групп по несколько человек, которые совместно планируют проект, делятся друг с другом опытом, выполняют проверку кода и сообща работают над задачей от начала до конца. Разработчики должны обладать максимальным объемом знаний, что помогает решать проблемы, связанные как с персоналом, так и с риском нехватки нужных знаний.

Проблемы с продуктивностью решаются с помощью назначения спринтов, Спринты – это краткосрочные этапы разработки с целью создания демо-версии продукта в заданные сроки (1-2 недели). Они служат для обозначения правильных целей и задач для проектных команд и позволяют увидеть промежуточные результаты работы.

Решением проблемы со временем является правильная организация процесса разработки. Процесс должен быть гибким, чтобы разработчики могли быстро адаптироваться к меняющимся требованиям, имели возможность быстро предоставлять исправленный продукт заказчику, и могли точно определять количество времени, необходимое для выполнения той или иной задачи.

Информация является одним из важнейших видов продуктов и видов товара на рынке, в том числе на международном. Средства ее обработки, накопления, хранения и передачи постоянно совершенствуются. Информация как категория, имеющая действительную или потенциальную ценность, стоимость, как и любой другой вид ценности, – охраняется, защищается ее собственником или владельцем.

Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для ее собственника, ограничение распространения которой приносит ему какую–то пользу или прибыль, возможность эффективно

решать стоящие перед ним задачи. Под защищаемой информацией понимают сведения, на использование и распространение которых введены ограничения их собственником.

Под общими признаками (концепциями) защиты любого вида охраняемой информации понимают следующее:

- защиту информации организует и проводит собственник, владелец / уполномоченное на это лицо;
- защитой информации собственник охраняет свои права на владение и распространение информации, стремится оградить ее от незаконного завладения и использования в ущерб его интересам;
- защита информации осуществляется путем проведения комплекса мер по ограничению доступа к защищаемой информации и созданию условий, исключающих или существенно затрудняющий несанкционированный доступ к засекреченной информации.

Следовательно, защита информации – есть комплекс мероприятий, проводимых собственником информации по ограждению своих прав на владение и распоряжение прав на информацию, создание условий, ограничивающих и исключающих или существенно затрудняющих несанкционированный доступ к засекреченной информации и ее носителям.

Защита информации – это деятельность собственника информации или уполномоченных им лиц по: обеспечению своих прав на владение, распоряжение и управление защищаемой информацией; предотвращению утечки и утраты информации; сохранению полноты достоверности, целостности защищаемой информации, ее массивов и программ обработки, сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Сохранение сведений в тайне, владение секретами дает определенные преимущества той стороне, которая ими владеет. Защищаемая информация, как

и любая другая информация, используется человеком или по его воле различными созданными искусственно или существующими естественно системами в интересах человека. Она носит семантический, то есть смысловой, содержательный характер. Это дает возможность использовать одну и ту же информацию разными людьми, народами независимо от языка ее представления и знаков, которыми она записана, формы ее выражения и т.д. В то же время защищаемая информация имеет и отличительные признаки:

- засекречивать информацию, то есть ограничивать к ней доступ, может только ее собственник (владелец) или уполномоченные им на то лица;
- чем важнее для собственника информация, тем тщательнее он ее защищает. А для того чтобы все, кто сталкивается с этой защищаемой информацией, знали, что одну информацию необходимо оберегать более тщательно, чем другую, собственник определяет ей различную степень секретности;
- защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства.

Основной угрозой информационной безопасности является несанкционированный (незаконный, неразрешенный) доступ злоумышленника или постороннего лица к документированной информации с ограниченным доступом и, как результат, овладение информацией и незаконное, противоправное ее использование.

Разработка мер, и обеспечение защиты информации осуществляются подразделениями по защите информации (служба безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России и / или ФАПСИ на право оказания услуг в области защиты информации.

Под злоумышленником понимается лицо, действующее в интересах противника, конкурента или в личных корыстных интересах (на сегодняшний день – террористы любых мастей, промышленный и экономический шпионаж, криминальные структуры, отдельные преступные элементы, лица, сотрудничающие со злоумышленником, психически больные лица и т.п.).

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники милиции, МЧС, коммунальных служб, медицинской помощи, прохожие и др.), посетители организации, работники других организаций, включая контролирующие органы, а также работники самого предприятия, не обладающие правом доступа в определенные здания и помещения, к конкретным документам, базам данных.

Каждое из указанных лиц может быть злоумышленником или его сообщником, агентом конкурента и т.п., но может и не быть им.

Наиболее часто встречающимися угрозами (опасностями) конфиденциальных сведении в документопотоках могут быть:

- Несанкционированный доступ постороннего лица к документам, делам и базам данных за счет его любопытства или обманных, провоцирующих действий, а также случайных или умышленных ошибок персонала фирмы;
- Утрата документа или его отдельных частей (листов, приложений, схем, копий, экземпляров, фотографий и др.), носителя чернового варианта документа или рабочих записей за счет кражи, утери, уничтожения;
- Утрата информацией конфиденциальности за счет ее разглашения персоналом или утечки по техническим каналам, считывания данных в чужих массивах, использования остаточной информации на копировальной ленте, бумаге, дисках и дискетах, ошибочных действий персонала;
- Подмена документов, носителей и их отдельных частей с целью фальсификации, а также сокрытия факта утери, хищения;

- Случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов, фальсификация документов;
- Гибель документов в условиях экстремальных ситуаций.

Заключение

–

Список использованных источников

–