Содержание:

Введение

В данном реферате я попытаюсь раскрыть тему “Виды защищаемой информации”. Данная тема актуальна связи с тем что личной информацией могут воспользоваться в корыстных целях большое значение приобрела проблема распространения государственной или организационной конфиденциальной информации.

Задачи данного реферата входит ознакомление с видами защитной информацией: Государственная тайна, государственные и муниципальные информационные системы, персональные данные/ General Data Protection Regulation, коммерческая тайна, автоматизированные системы управления технологическими процессами, информация для служебного пользования, открытые информационные ресурсы.

Государственная тайна

Государственная тайна – защищаемые государством сведения в области его военной, экономической, разведывательной, внешнеполитической, контрразведывательной и оперативно-розыскной деятельности, распространение который может нанести ущерб безопасности РФ.

Защит от несанкционированного распространения подлежит информация, относящаяся к следующим сферам:

1. Вооруженные силы государства.
2. Сведения о внешнеполитической деятельности государства.
3. Информация о научно-исследовательских и опытно-конструкторских разработках, данные об экономических показателях по отдельным направлениям.
4. Сведения, относящиеся к деятельности органов национальной безопасности, внешней разведки и оперативно-розыскных мероприятий, проводимых

правоохранительными структурами.

В первую очередь признаком государственной тайны является степень конфиденциальности информаций, отнесенных к ней.

Государственную тайну составляют:

1. Сведения в области экономики, науки и техники
2. Сведения в военной области
3. Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности
4. Сведения в области внешней политики и экономике

Для сохранения государственной тайны законодательством страны вводится особый административно-правовой порядок в данной сфере – порядка конфиденциальности. Для его выполнения разрабатывается комплекс действий по защите таких информаций от разглашения и противодействия шпионажу и разведке иностранных государств. С этой целью вводится уголовная ответственность за передачу конфиденциальной информации третьим лицам или незаконного ее распространения. Важность информаций, относящихся к государственной тайне различна, часть из них является стратегическим, оперативным или локальным характером. Соответственно этому и вводится понятие о степени конфиденциальности для каждого из перечисленных уровней. В каждой из стран устанавливается своя система обозначений в указанной области, которая закрепляется законом или иными нормативно-правовыми актами. Любая информация, в том числе и относящаяся к конфиденциальной, существует на носителях разных видов. Это могут быть и материальные объекты: бумага и цифровые - компьютерные файлы на жестких и лазерных дисках, картах памяти и т.п. Носителем информации признается и человек, обладающий конфиденциальными сведениями. Доступ к государственной тайне производится на основании допуска, который оформляется компетентными органами после проверок.

Государственные и муниципальные информационные системы

Государственные и муниципальные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена

информацией между этими органами, а также в иных установленных федеральными законами целях.

Информационные системы ежедневно встречаются в нашей жизни – дома, на работе, на улице, в транспорте. И сегодня только представить жизнь без таких систем довольно сложно. Ведь информационные системы – это наши, так называемые, помощники. Любая организация уже не может полноценно заниматься какой-либо деятельностью без информационно-аналитических систем. Один из самых простых примеров повседневной информационной системы можно назвать телефонный справочник, где указаны номера, а также фамилия, имя, отчество абонентов. На предприятиях активно используются информационные системы управления. С помощью таких систем жизнь человечества существенно облегчается, это огромная и неоценимая помощь, ведь один или несколько человек не могут держать в голове или же на бумажных носителях данные, которые в компьютере занимают терабайты оперативной памяти. Просто хранить такую информацию – это мало, ее нужно систематизировать и адаптировать для удобного использования. Все информационные системы можно представить в виде информационного справочника и информационной базы данных. Каждая из этих систем может подразделяться на другие с более конкретной направленностью, например, по тематикам – медицина, география и др. Таким образом, для каждой сферы деятельности имеется своя информационная система управления. Главную функцию, которую преследует абсолютно каждая такая система – это сбор, хранение и поиск информации. Большое количество информации нередко затрудняет поиск, для этого требуется много времени и усилий. Информационные системы управления – это главный помощник в поиске нужной информации. Это очень быстро, довольно удобно и весьма практично. К тому же, информация в электронном виде в ближайшем будущем заменит бумажные документы, поскольку обращаться с электронными документами – это куда проще, быстрее и экономичнее.

Персональные данные/GDPR

Защита персональных данных – комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту информаций, относящихся к определенному или определяемому на основании такой информации физическому лицу.

Защита персональных данных включена в раздел охраны труда на предприятии, является самостоятельным элементом. Государство гарантирует работникам защиту их персональных данных, а также их права на труд, с учетом использования их персональных.

Говоря о частных лицах, под “персональными данными” понимается вся возможная информация, которая либо прямо, либо косвенно относится к определенному физическому лицу (согласно терминологии закона – субъекту персональных данных). Согласие на получение и последующую обработку персональных данных частное лицо может предоставить только самостоятельно, выразив это в письменной форме. При этом разрешение на любое использование личных данных может быть оформлено и как отдельным документом, так и быть пунктом договора (например, кредитного или депозитного). Обратите внимание – любая онлайн-заявка на кредит будет недействительна при отсутствии вашего согласия (обычно требуется поставить галочку возле соответствующего пункта). Получение либо использование любой персональной информации о частном лице без наличия на то письменного или иного согласия является незаконным. Также неправомерными считаются и случаи обработки персональных информаций после получения от частного лица заявления на отзыв согласия на такую обработку. Тем не менее существуют исключения. Например, персональные данные могут быть получены без согласия человека для работы государственных органов, а для соблюдения обязательств по действующим договорам обработка персональной информации может быть продолжена и после отзыва согласия на ее использование.

Что такое GDPR?

Общий регламент по защите данных (General Data Protection Regulation). Документ предоставляет резидентам Евросоюза (ЕС) возможность управлять персональными данными: спрашивать про цели обработки, место их хранения, а в случае необходимости удалить. Он вступает в силу с 25 мая 2018 года. Какие данные защищает General Data Protection Regulation? Персональные данные — любая информация о человеке, по которой он идентифицируется: пол, возраст, место жительства, умственная, культурная, экономическая, социальная идентичность.

Принципы General Data Protection Regulation:

Прозрачность и законность. Компании должны понятно объяснить, для чего они собирают данные и как планируют использовать их в дальнейшем.

Ограничение цели. Если цели сбора данных изменились, но они и дальше продолжают использоваться – это нарушение.

Минимум информации. Данные нужны только в объеме, необходимом для достижения конкретных целей, нельзя запрашивать лишнее.

Управление данными. Пользователь может запросить копию всей личной информации, которая у вас есть по нему — будьте готовы предоставить ее в течение 30 дней. Также пользователь может потребовать удалить данные о нем без права восстановления.

Ограничение хранения. Срок хранения данных должен пересекаться со сроком достижения целей. Как только цель достигнута — данные удаляются.

Безопасность хранения. Нельзя передавать данные третьим лицам. В случае утечки сообщать об этом в течение трех дней.

Подотчетность – ответственность за обработку персональных данных и выполнение всех остальных принципов General Data Protection Regulation включая записи конфиденциальности.

General Data Protection Regulation имеет экстерриториальное действие. Новые правила распространятся на всех, кто работает с данными резидентов ЕС. Неважно, есть ли у вас филиалы в Европе, где зарегистрирована компания и где она обрабатывает данные. Главное условие — работа с данными европейцев, полученными на территории Евросоюза (в том числе через интернет). География покрытия документа — 28 стран. Игнорировать General Data Protection Regulation будет сложно всем. Даже самая маленькая российская компания не может быть на 100% уверена в том, что у одного из подписчиков не может быть 2 гражданства. И одно из них может оказаться европейским. Поэтому будет разумно еще раз проверить свои клиентские базы. За несоблюдение принципов накладывается штраф в размере от 10 до 20 миллионов евро или от 2 до 4% от годового оборота компании. Практика исполнения решений ЕС в РФ развита не очень хорошо, поэтому даже если Комиссия ЕС наложит штраф на российскую компанию, существует очень маленькая вероятность реального исполнения такого решения. Но на территории ЕС работа будет затруднена. Подобное решение может стать основанием для проведения в отношении компании проверки уже российскими органами.

Регламент General Data Protection Regulation заменил директиву Data Protection Directive от 1995 года. Постановление было принято 27 апреля 2016 года, вступило в силу 25 мая 2018 года после двух летнего переходного периода и, в разнице от директивы, не требует от правительств стран-участниц ЕС никаких изменений в локальных законодательствах и, таким образом, является непосредственно обязательным к исполнению. Это применимо не только к странам участница ЕС, но еще к любому юридическому лицу, обрабатывающему персональные данные лиц ЕС.

В законе расширено понятие персональных данных, введены понятия «трансграничной передачи данных», «псевдонимизации», установлено «право на забвение», определена роль должностного лица по защите данных.

Коммерческая тайна

Коммерческая тайна – порядок конфиденциальной информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Под порядком конфиденциальной информации понимается введение и поддержание особых мер по защите информации.

Также под коммерческой тайной могут подразумевать саму информацию, которая составляет коммерческую тайну, то есть, научно-техническую, технологическую, производственную, финансово-экономическую или иную информацию, в том числе составляющую конфиденциальные производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен порядка коммерческой тайны. Обладатель информации имеет право отнести ее к коммерческой тайне, если эта информация отвечает вышеуказанным критериям и не входит в перечень информации, которая не может составлять коммерческую тайну. Чтобы информация получила статус коммерческой тайны, ее обладатель должен исполнить установленные процедуры (составление перечня, нанесение грифа и некоторые другие). После получения статуса коммерческой тайны информация начинает охраняться законом. Разглашение информации, составляющей коммерческую тайну – действие или бездействие, в результате которых

информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору. За разглашение (умышленное или неосторожное), а также за незаконное использование информации, составляющей коммерческую тайну, предусмотрена ответственность – дисциплинарная, гражданско-правовая, административная, уголовная и материальная. Материальная ответственность наступает независимо от других форм ответственности.

Автоматизированные системы управления технологическими процессами (АСУ ТП)

Автоматизированная система управления технологическим процессом – группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях. Может иметь связь с более общей автоматизированной системой управления предприятием автоматизированные системы управления технологическими процессами Под автоматизированные системы управления технологическими процессами обычно понимается целостное решение, обеспечивающее автоматизацию основных операций технологического процесса на производстве в целом или каком-то его участке, выпускающем относительно завершенное изделие.

Понятие «автоматизированный», в разнице от понятия «автоматический», подчеркивает необходимость участия человека в отдельных операциях, как в целях сохранения контроля над процессом, так и в связи со сложностью или нецелесообразностью автоматизации отдельных операций. Составными частями автоматизированные системы управления технологическими процессами могут быть отдельные системы автоматического управления (САУ) и автоматизированные устройства, связанные в единый комплекс. Такие как системы диспетчерского управления и сбора данных (SCADA), распределенные системы управления (DCS), и другие более мелкие системы управления (например, системы на программируемых логических контроллерах (PLC)). Как правило, автоматизированные системы управления технологическими процессами имеет единую систему операторского управления технологическим процессом в виде одного или нескольких пультов управления, средства обработки и архивирования информации о ходе процесса, типовые элементы автоматики: датчики, устройства управления, исполнительные устройства. Для информационной связи всех подсистем используются промышленные сети.

Информация для служебного пользования

Документы с грифом «Для служебного пользования» - документы, содержащие служебную информацию ограниченного распространения, относящуюся к не конфиденциальной информации, касающуюся деятельности организации, ограничение на распространение которой диктуется служебной необходимостью. Общепринятым сокращением для обозначения документов, содержащих информацию ограниченного делопроизводства, является аббревиатура – ДСП. При учете документов с грифом «Для служебного пользования» необходимо фиксировать не только данные о самом документе, включая количество его экземпляров и листов, поскольку утрата экземпляра или отдельных листов при без учетном их хранении зачастую приводит и к утечке информации, но и любое движение и местонахождение документа, что позволяет, помимо расширения справочно-поисковых данных о документе, обеспечивать персональную ответственность за его сохранность и качественно проводить проверки наличия документов с целью своевременного обнаружения их возможных утрат.

Открытые информационные ресурсы

Информационные ресурсы – документы и массивы документов в информационных системах.

Современная информационная система представляет собой совокупность неоднородных элементов и реализует широкий диапазон сетевых функций и услуг. Наиболее полной моделью информационной системой является модель сетевого взаимодействия открытых систем. Такая информационная система представляет универсальную распределенную среду с широкими вычислительными возможностями, ориентированную на большой круг пользователей. Однако при этом она становится мишенью для возможных угроз, попыток несанкционированного доступа, что делает актуальной проблему защиты таких информационных систем. Потребность обеспечения надежности вычислительных услуг, целостности, конфиденциальности и доступности информации приводит к целесообразности включения функции защиты в число обязательных функций информационных систем.

Вывод

Проделанная работа позволяет нам понять, что в наше время защита информации не идеальна. Каждой организации или странам приходится свою защиту придумывать или придерживаться к стандарту.

Список литературы

1. http://www.yarsec.ru/informatsionnaya-bezopasnost/vidy-zi/
2. http://информационная-безопасность.гафнер.рф/chitat-posobie/glava-2/2-2-zashchita-gosudarstvennoy-tayny/
3. https://ru.wikipedia.org/wiki/Защита_персональных_данных
4. https://ru.wikipedia.org/wiki/Общий_регламент_по_защите_данных
5. http://www.consultant.ru/document/cons_doc_LAW_61798/6b46c7cef112b2df9fc3d7f737c7
6. https://ru.wikipedia.org/wiki/Информационные_ресурсы