МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Кафедра теоретической экономики

Доклад
по дисциплине «Информационная безопасность»
на тему «Формирование требований к системе защиты информации на примере рекламы на транспорте»

Работу выполнил _____ 30.11.18 _____ Ванян Б.К.
(подпись, дата)

Факультет экономический

Направление 38.04.05 – Бизнес-информатика

Научный руководитель

д.э.н., проф. _____ 30.11.2018 Сидоров В.А.
(подпись, дата)

Краснодар 2018

При изготовлении рекламы для размещения на транспорте используются самоклеящиеся виниловые пленки с повышенным сроком службы. Для надежности дополнительно отпечатанную пленку ламинируют перед поклейкой на заранее подготовленную поверхность транспорта.

Оборудование:

− широкоформатные плоттеры Seiko H2-74S;

− широкоформатные плоттеры Seiko M-64S;

− режущий плоттер Fotoba XLD 170 N2137;

− режущий плоттер Roland GX-500 ZBA4940;

− ламинаторы Cala Mistral;

− виниловые пленки;

− ПК и ПО.

Далее рассмотрим требования к защите информации на предприятии по изготовлению рекламы для размещения на транспорте.

1. При обработке общедоступной информации никаких специальных мер защиты от несанкционированного доступа не требуется

2. Требования к защите конфиденциальной информации определяет пользователь, устанавливающий статус конфиденциальности.

3. При обработке служебной информации к ней должен быть обеспечен свободный доступ пользователям учреждения-владельца этой информации (по общему списку); доступ же пользователей, не включенных в общий список, должен осуществляться по разовым санкциям, выдаваемым пользователями, включенными в список.

4. При обработке секретной информации в зависимости от ее объема и характера может быть предъявлен один из следующих вариантов требований:

а) персональное разграничение − для каждого элемента информации составляется список пользователей, имеющих к нему право доступа;

б) коллективное разграничение − структура баз защищаемых данных организуется в соответствии со структурой подразделений, участвующих в обработке защищаемой информации; пользователи каждого подразделения имеют право доступа только к «своим» данным.

5. При обработке информации, размещенной только в ОЗУ, должны обеспечиваться требуемые уровень защиты и надежность в центральном вычислителе и на коммуникациях ввода-вывода данных. При обработке информации, размещенной на одном внешнем носителе, дополнительно предыдущему должна обеспечиваться защита в соответствующем устройстве ВЗУ и коммуникациях, связывающих это устройство с процессором.

6. При обработке информации, размещенной на нескольких внешних носителях, дополнительно к предыдущему должна обеспечиваться необходимая изоляция друг от друга данных, размещенных на различных носителях при одновременной их обработке.

7. Информация временного хранения дополнительно к предыдущему подлежит защите в течение объявленного времени хранения, после чего должна быть уничтожена во всех устройствах АСОД и на всех носителях, используемых для ее хранения. Продолжительность хранения задается или длиной промежутка времени, или числом сеансов решения соответствующих функциональных задач.

8. Информация длительного хранения подлежит постоянной защите, уничтожение ее должно осуществляться по специальным командам.

9. Информация должна защищаться во всех структурных элементах АСОД, причем специфические требования к защите информации в структурных элементах различного типа сводятся к следующему.

В терминалах пользователей:

а) защищаемая информация может находиться только во время сеанса решения задач, после чего подлежит уничтожению;

б) устройства отображения и фиксации информации должны располагаться так, чтобы исключить возможность просмотра отображаемой (выдаваемой) информации со стороны;

в) информация, имеющая ограничительный гриф, должна выдаваться (отображаться) совместно с этим грифом.

10. В простых УГВВ и в сложных с малым объемом ЗУ защищаемая информация может находиться только во время решения задач, после че го подлежит уничтожению; в сложных с большим объемом ЗУ информа ция может храниться в ВЗУ, однако продолжительность хранения должна быть ограниченной.

11. в УГВВ с возможностями универсального процессора при каждом обращении к защищаемой информации должны осуществляться процедуры:

− установления подлинности (опознавания) вступающих в работу терминалов и пользователей;

− проверки законности каждого запроса на соответствие предо ставленным пользователю полномочиям;

− проверки адреса выдачи информации, имеющей ограничитель ный гриф, и наличия этого грифа;

− контроля обработки защищаемой информации;

− регистрации запросов и всех нарушений правил защиты.

12. В аппаратуре и линиях связи:

а) линии связи, по которым защищаемая информация передается в явном виде, должны находиться под непрерывным контролем во все время передачи информации;

б) перед началом каждого сеанса передачи защищаемой информации должна осуществляться проверка адреса выдачи данных;

г) при передаче большого объема защищаемой информации проверка адреса передачи должна также периодически производиться в процессе передачи (через заданный промежуток времени или после передачи заданного числа знаков сообщения).

13. В центральном вычислителе:

а) защищаемая информация в ОЗУ может находиться только во время сеансов решения соответствующих задач, в ВЗУ - минимальное время, определяемое технологией решения соответствующей прикладной задачи в АСОД;

б) при обработке защищаемой информации должно осуществляться установление подлинности всех участвующих в обработке устройств и пользователей, и ведение протоколов их работы;

в) всякое обращение к защищаемой информации должно проверяться на санкционированность.

14. В ВЗУ:

а) сменные носители информации должны находиться на устройствах управления в течение минимального времени, определяемого технологией автоматизированной обработки информации;

б) устройства управления ВЗУ, на которых установлены носители с защищаемой информацией, должны иметь замки, предупреждающие не санкционированное изъятие или замену носителя;

в) должны быть предусмотрены возможности автономного аварийного уничтожения информации на носителях, находящихся на устройствах ВЗУ.

15. В хранилище носителей:

а) все носители, содержащие защищаемую информацию, должны иметь четкую и однозначную маркировку, которая, однако, не должна раскрывать содержания записанной на них информации;

б) носители, содержащие защищаемую информацию, должны храниться таким образом, чтобы исключались возможности несанкционированного доступа к ним;

в) при выдаче и приемке носителей должна осуществляться проверка личности получающего (сдающего) и его санкции на получение (сдачу) этих носителей.

16. В слабораспределенных АСОД (размещенных в нескольких помещениях, но на одной и той же территории) дополнительно к предыдущему

должна быть обеспечена требуемая защита информации в линиях связи, с помощью которых сопрягаются элементы АСОД, расположенные в различных помещениях, для чего должны быть или постоянный контроль за этими линиями связи, или исключена передача по ним защищаемой информации в явном виде.

17. К защите документальной информации предъявляются следую щие требования:

а) должна обеспечиваться защита как оригиналов документов, так и сведений о них, накапливаемых и обрабатываемых в АСОД;

б) применяемые средства и методы защиты должны выбираться с учетом необходимости обеспечения доступа пользователям различных категорий.

18. При обработке фактографической быстроменяющейся информации должны учитываться требования:

а) применяемые средства и методы защиты не должны существенно влиять на оперативность обработки информации;

б) применяемые средства и методы защиты должны выбираться с учетом обеспечения доступа к защищаемой информации строго ограниченного круга лиц.

19. К защите фактографической исходной информации предъявляются требования:

а) каждому пользователю должны быть обеспечены возможности формирования требований к защите создаваемых им массивов данных в пределах предусмотренных в АСОД возможностей защиты;

б) в системе защиты должны быть предусмотрены средства, выбираемые и используемые пользователями для защиты своих массивов по своему усмотрению.

20. К защите фактографической регламентной информации предъявляются требования:

а) применяемые средства и методы защиты должны быть рассчитаны на длительную и надежную защиту информации;

б) должен обеспечиваться доступ (в пределах полномочий) широкого круга пользователей;

в) повышенное значение приобретают процедуры идентификации, опознавания, проверки полномочий, регистрации обращений и контроля выдачи.

21. Специфические требования к защите для различных уровней автоматизации обработки информации состоят в следующем:

а) при автономном решении отдельных задач или их комплексов основными макропроцессами автоматизированной обработки, в ходе которых должен обеспечиваться необходимый уровень защиты, являются:

1) сбор, подготовка и ввод исходных данных, необходимых для решения задач;

2) машинное решение задач в автономном режиме;

3) выдача результатов решения;

б) в случае полусистемной обработки дополнительно к предыдущему на участках комплексной автоматизации должна быть обеспечена защита в ходе осуществления следующих макропроцессов:

1) автоматизированного сбора информации от датчиков и источников информации;

2) диалогового режима работы пользователей ЭВМ;

в) в случае системной обработки дополнительно к предыдущему должна быть обеспечена защита в ходе таких макропроцессов:

1) прием потока запросов и входной информации;

2) формирование пакетов и очередей запросов;

3) диспетчирование в ходе выполнения запросов;

4) регулирование входного потока информации.

22. В зависимости от способа взаимодействия пользователей с комплексом средств автоматизации предъявляются следующие специфические требования:

а) при автоматизированном вводе информации должны быть обеспечены условия, исключающие несанкционированное попадание информации одного пользователя (абонента) в массив другого, причем должны быть обеспечены возможности фиксирования и документального закрепления момента передачи информации пользователя банку данных АСОД и содержания этой информации;

б) при неавтоматизированном вводе должна быть обеспечена защита на неавтоматизированных коммуникациях «Пользователь – АСОД», на участках подготовки данных и при вводе с местных УГВВ;

в) при пакетном выполнении запросов пользователей должно исключаться размещение в одном и том же пакете запросов на обработку информации различных ограничительных грифов;

г) при обработке запросов пользователей в реальном масштабе времени данные, поступившие от пользователей, и данные, подготовленные для выдачи пользователям, в ЗУ АСОД должны группироваться с ограничительным грифом, при этом в каждой группе должен быть обеспечен уровень защиты, соответствующий ограничительному грифу данных группы.

23. В зависимости от режимов функционирования комплексов средств автоматизации предъявляют следующие специфические требования:

а) в однопрограммном режиме работы в процессе выполнения про граммы должны предупреждаться:

1) несанкционированное обращение к программе;

2) несанкционированный ввод данных для решаемой задачи;

3) несанкционированное прерывание выполняемой программы;

4) несанкционированная выдача результатов решения;

б) в мультипрограммном режиме сформулированные выше требования относятся к каждой из выполняемых программ и дополнительно должно быть исключено несанкционированное использование данных одной программы другой;

в) в мультипроцессорном режиме сформулированные выше требования должны обеспечиваться одновременно во всех участвующих в решении задачи процессорах, кроме того, должно быть исключено несанкционированное вклинивание в вычислительный процесс при распараллеливании и при диспетчеризации мультипроцессорного выполнения программ.

24. Требования, обуславливаемые этапом жизненного цикла АСОД, формулируются так:

а) на этапе создания АСОД должно быть обеспечено соответствие возможностей системы защиты требованиям к защите информации, сформулированным в задании на проектирование, кроме того, должно быть исключено несанкционированное включение элементов (блоков) в компоненты АСОД (особенно системы защиты);

б) на этапе функционирования АСОД в пассивном ее состоянии должна быть обеспечена надежная защита хранящейся информации и исключены возможности несанкционированных изменений компонентов системы;

в) на этапе функционирования АСОД в активном ее состоянии дополнительно к сформулированным выше требованиям должна быть обеспечена надежная защита информации во всех режимах автоматизированной ее обработки.

На основании перечня требований на основе защиты информации в данной работе было получено техническое задание, обусловленное спецификой работы предприятия по производству рекламы для размещения на транспорте.