МИНИСТЕРСТВО ТРАНСПОРТА И КОММУНИКАЦИЙ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Системы передачи информации»

Е. С. БЕЛОУСОВА, П. М. БУЙ

ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебно-методическое пособие для практических работ по дисциплинам «Информационная безопасность систем автоматики и телемеханики», «Защита информации в телекоммуникационных системах» и «Защита программного обеспечения и баз данных»

Гомель 2016

МИНИСТЕРСТВО ТРАНСПОРТА И КОММУНИКАЦИЙ
РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Системы передачи информации»

Е. С. БЕЛОУСОВА, П. М. БУЙ

ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Одобрено методической комиссией электротехнического факультета в качестве учебно-методического пособия для практических работ по дисциплинам «Информационная безопасность систем автоматики и телемеханики», «Защита информации в телекоммуникационных системах» и «Защита программного обеспечения и баз данных» для студентов специальности 1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте»

Гомель 2016

УДК 004.056.53 (075.8)
ББК 32.81
Б43

Рецензент – заведующий кафедрой «Защита информации» доктор технических наук, профессор *Л. М. Лыньков* (УО «БГУИР»)

Белоусова, Е. С.

Б43 Политика безопасности информационных систем : учеб.-метод. пособие / Е. С. Белоусова, П. М. Буй ; М-во трансп. и коммуникаций Респ. Беларусь, Белорус. гос. ун-т трансп. – Гомель : БелГУТ, 2016. – 38 с.

ISBN 978-985-554-563-8

Изложены цель практических работ, краткие сведения из теории, порядок выполнения, содержание отчета и контрольные вопросы.

Предназначено для студентов специальности 1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте», а также может быть использовано при изучении других курсов, связанных с вопросами информационной безопасности.

УДК 004.056.53 (075.8)
ББК 32.81

ISBN 978-985-554-563-8

Практическая работа №1

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Цель работы. Изучить типовой алгоритм описания информационной системы. Приобрести практические навыки по его применению. Научиться идентифицировать угрозы информационной системы, их источники и методы парирования.

Краткие сведения из теории

На этапе описания информационной системы (ИС) необходимо указать цели ее создания, границы, информационные ресурсы, требования в области информационной безопасности (ИБ) и компонентов управления информационной системой и режимом ИБ.

Описание рекомендуется делать в соответствии со следующим планом:

– аппаратные средства ИС, их конфигурация;

– используемое программное обеспечение (ПО);

– интерфейсы системы, то есть внешние и внутренние связи с позиции информационной технологии;

– типы данных и информации;

– персонал, работающий в данной ИС (обязанности);

– миссия данной ИС (основные цели);

– критичные типы данных и информационные процессы;

– функциональные требования к ИС;

– категории пользователей системы и обслуживающего персонала;

– формальные требования в области ИБ, применимые к данной ИС (законодательство, ведомственные стандарты и т. д.);

– архитектура подсистемы ИБ;

– топология локальной сети;

– программно-технические средства обеспечения ИБ;

– входные и выходные потоки данных;

– система управления в данной ИС (должностные инструкции, система планирования в сфере обеспечения ИБ);

– существующая система управления в области ИБ (резервное копирование, процедуры реагирования на нештатные ситуации, инструкции по ИБ, контроль поддержания режима ИБ и т. д.);

– организация физической безопасности;

– управление и контроль внешней по отношению к ИС средой (климатическими параметрами, электропитанием, защитой от затоплений, агрессивной среды и т. д.).

Активы организации – все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении. К активам организации могут относиться:

– информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т. д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);

– выпускаемая продукция и/или оказываемые услуги;

– аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, маршрутизаторы;

– программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы;

– данные: обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, передаваемые по коммуникационным линиям;

– пользователи, обслуживающий персонал;

– документация: по программам, по аппаратуре, системная, по административным процедурам;

– расходные материалы: бумага, формы, красящая лента, магнитные носители.

Для системы, находящейся в стадии проектирования, и для уже существующей системы характер описания и степень подробности ответов будут разными. В первом случае (стадия проектирования) достаточно указать общие требования в области ИБ.

Анализ угроз информационной безопасности. Под угрозой информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу. Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Уязвимость объекта – это присущие объекту причины, приводящие к нарушению безопасности информации на объекте.

А т а к а – это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости. Атака – это всегда пара «источник – уязвимость», реализующая угрозу и приводящая к ущербу.

К настоящему времени известно большое количество угроз информационной безопасности. Рассмотрим их к л а с с и ф и к а ц и ю по различным классификационным признакам.

По виду:

– физической и логической целостности (уничтожение или искажение информации). Угроза целостности – несанкционированное изменение, искажение, уничтожение информации;

– конфиденциальности (несанкционированное получение). Угроза конфиденциальности – нарушение свойства информации быть известной только определенным субъектам;

– доступности. Угроза доступности (отказ в обслуживании) – нарушение работоспособности объекта, доступ к которому получил злоумышленник;

– права собственности.

По характеру:

– случайные (отказы, сбои, ошибки, стихийные явления). Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются, как правило, в теории надежности, программировании, инженерной психологии;

– преднамеренные (злоумышленные действия людей). Преднамеренные угрозы связаны с действиями людей (работники спецслужб либо самого объекта, хакеры). Для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться штатными каналами доступа, если по отношению к ним не предприняты никакие меры защиты, либо нештатными каналами доступа, к которым принято относить:

- побочное электромагнитное излучение информации с аппаратуры системы;
- побочные наводки информации по сети электропитания и заземления;
- побочные наводки информации на вспомогательных коммуникациях;
- подключение к внешним каналам связи.

По источникам:

– человек;

– технические устройства;

– программное обеспечение;

– внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

Угроза, как следует из определения, – это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

Угрозами безопасности информации являются нарушения при обеспечении:

– конфиденциальности;

– доступности;

– целостности.

Конфиденциальность информации – это свойство информации быть известной только аутентифицированным законным ее владельцам или пользователям. Нарушения при обеспечении конфиденциальности:

– хищение (копирование) информации и средств ее обработки;

– утрата (неумышленная потеря, утечка) информации и средств ее обработки.

Доступность информации – это свойство информации быть доступной для аутентифицированных законных ее владельцев или пользователей. Нарушения при обеспечении доступности:

– блокирование информации;

– уничтожение информации и средств ее обработки.

Целостность информации – это свойство информации быть неизменной в семантическом смысле при воздействии на нее случайных или преднамеренных искажений или разрушающих воздействий. Нарушения при обеспечении целостности:

– модификация (искажение) информации;

– отрицание подлинности информации;

– навязывание ложной информации.

Все **методы защиты информации** по характеру проводимых действий можно разделить:

– на законодательные (правовые);

– организационные;

– технические;

– комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых, прежде всего, государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по

защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т. е. комплексно.

Порядок выполнения работы

1 Описать информационную систему Белорусской железной дороги, выбранный из таблицы 1 в соответствии с предпоследней цифрой шифра.

Таблица 1 – **Варианты информационных объектов Белорусской железной дороги**

Цифра шифра	Информационный объект	Цифра шифра	Информационный объект
0	Испытательный центр объектов железнодорожного транспорта	5	Отдел управления сети связи
1	Транспортно-логистический центр	6	Служба сигнализации и связи
2	Служба организации труда и заработной платы	7	Главный расчетный информационный центр
3	Служба информационных технологий	8	Служба безопасности движения поездов
4	Служба бухгалтерского учета	9	Финансово-экономическая служба

2 Конкретизировать род деятельности ИО, определить ее штат, структуру административного управления.

3 Категорировать информацию, с которой работают в данном ИО исходя из его рода деятельности.

4 Составить список необходимого оборудования для нормальной работы компании, включая, при необходимости, и бытовую технику.

5 Оценить свойства и стоимость информационных активов ИО. Работу выполнять в виде таблицы 2. Стоимость актива определять в зависимости от его свойств по таблице 3.

Таблица 2 – **Перечень активов информационного объекта**

Тип актива	Свойства информационного актива			Стоимость актива
	целостность	доступность	конфиденциальность	

Таблица 3 – **Определение стоимости актива в зависимости от его свойств**

Стоимость актива, у. е.	Свойства актива		
	целостность	доступность	конфиденциальность
500	–	–	–
3 000	–	–	+
2 000	–	+	–
4 000	–	+	+
2 500	+	–	–
5 000	+	–	+
5 500	+	+	–
20 000	+	+	+

6 Определить не менее пяти угроз для выбранных активов, их источников и методов борьбы с ними, которые могут быть реализованы по отношению к информации, создаваемой, хранящейся и обрабатываемой на информационном объекте. Работу выполнять в виде таблицы 4.

Таблица 4 – **Определение угроз, их источников и методов борьбы с данными угрозами**

Уязвимость	Наименование угрозы	Источник угрозы	Возможный результат при реализации угрозы, какие активы могут быть повреждены

Содержание отчета

1 Цель работы.

2 Результаты выполнения задания.

3 Описание информационного объекта.

4 Таблица перечня информационного объекта

5 Таблица угроз, их источников и методов борьбы с данными угрозами для информационного объекта.

6 Вывод по работе.

Контрольные вопросы

1 Чем информационная система отличается от информационного объекта?

2 Что принято называть угрозой информационной безопасности?

3 Какова классификация методов защиты информации, в том числе по характеру проводимых мероприятий?

4 Какова классификация угроз информационной безопасности?

5 Что понимается под термином «информационный объект»?

6 Что представляет собой угроза права собственности?

Практическая работа №2

МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы. Изучить методику построения модели нарушителя информационной безопасности. Произвести классификацию определенного нарушителя и построить его модель.

Краткие сведения из теории

Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, технических и материальных средствах и т. д.

Правильно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности. Опираясь на построенную модель, уже можно строить адекватную систему информационной защиты.

Чаще всего строится неформальная модель нарушителя, отражающая причины и мотивы действий, его возможности, 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. Для достижения поставленных целей нарушитель должен приложить определенные усилия и затратить некоторые ресурсы. Например, модель нарушителя может быть представлена в форме таблицы, которая описывает характеристики некоторого нарушителя (таблица 1).

Таблица 1 – **Форма представления модели нарушителя информационной безопасности**

Характеристика	Нарушитель
Вычислительная мощность технических средств	
Доступ к интернету, тип каналов доступа	
Финансовые возможности	
Уровень знаний в области IT	
Используемые технологии	
Знания о построении системы защиты объекта	
Преследуемые цели	
Характер действий	
Глубина проникновения	

Определив основные причины нарушений, представляется возможным оказать на них влияние или необходимым образом скорректировать требования к системе защиты от данного типа угроз. При анализе нарушений защиты необходимо уделять внимание субъекту (личности) нарушителя. Устранение причин или мотивов, побудивших к нарушению, в дальнейшем может помочь избежать повторения подобного случая.

Модель может быть не одна, целесообразно построить несколько отличающихся моделей разных типов нарушителей информационной безопасности объекта защиты.

Для построения модели нарушителя используется информация, полученная от служб безопасности и аналитических групп, данные о существующих средствах доступа к информации и ее обработки, о возможных способах перехвата данных на стадиях их передачи, обработки и хранении, об обстановке в коллективе и на объекте защиты, сведения о конкурентах и ситуации на рынке, об имевших место свершившихся случаях нарушения информационной безопасности и т. п.

Кроме этого оцениваются реальные оперативные технические возможности злоумышленника для воздействия на систему защиты или на защищаемый объект. Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать нарушитель в процессе совершения действий, направленных против системы информационной защиты.

В последнее время модель нарушителя информационной безопасности перестает быть простой формальностью и начинает оказывать большое влияние на перечень актуальных угроз для информационной системы. В перечне угроз для информационной системы для каждой угрозы задан тип и потенциал нарушителя, который может ее реализовать. За счет этого устанавливается взаимосвязь между перечнями угроз и нарушителями информационной безопасности.

Потенциал нарушителя может быть высоким, средним или низким. Для каждого из вариантов задан свой набор возможностей.

Так, нарушители с низким потенциалом могут для реализации атак использовать информацию только из общедоступных источников. К нарушителям с низким потенциалом можно отнести любых внешних лиц, а также внутренний персонал и пользователей информационной системы.

Внешние нарушители, к которым могут относиться и бывшие сотрудники, имеют возможность самостоятельно создавать способы атак, проводить их подготовку и реализацию только за пределами контролируемой зоны. Внутренний персонал имеет возможность проводить атаки в пределах контролируемой зоны с возможным физическим доступом к аппаратным средствам, на которых реализована ИС, в зависимости от величины штатных полномочий.

Нарушители со средним потенциалом имеют возможность проводить анализ кода прикладного программного обеспечения, самостоятельно находить в нем уязвимости и использовать их. К таким нарушителям можно относить террористические и криминальные группы, конкурирующие организации, администраторов системы и разработчиков ПО. Эти нарушители имеют возможность привлекать специалистов с опытом разработки и анали-

за систем комплексной защиты информации (СКЗИ) (включая специалистов в области использования для реализации атак анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок, а также недокументированных возможностей прикладного программного обеспечения).

Нарушители с высоким потенциалом имеют возможность вносить закладки в программно-техническое обеспечение системы, проводить специальные исследования и применять специальные средства проникновения и добывания информации. К таким нарушителям следует относить только иностранные и отечественные спецслужбы. Они имеют возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования ИС).

Классификация нарушителей информационной безопасности. Нарушители бывают внутренними и внешними.

Среди внутренних нарушителей в первую очередь можно выделить:

– непосредственных пользователей и операторов информационной системы, в том числе руководителей различных уровней;

– администраторов вычислительных сетей и информационной безопасности;

– прикладных и системных программистов;

– сотрудников службы безопасности;

– технический персонал по обслуживанию зданий и вычислительной техники, от уборщицы до сервисного инженера;

– вспомогательный персонал и временных работников.

Среди причин, побуждающих сотрудников к неправомерным действиям, можно указать:

– безответственность;

– ошибки пользователей и администраторов;

– демонстрацию своего превосходства (самоутверждение);

– «борьбу с системой»;

– корыстные интересы пользователей системы;

– недостатки используемых информационных технологий.

Группу внешних нарушителей могут составлять:

– клиенты;

– приглашенные посетители;

– представители конкурирующих организаций;

– сотрудники органов ведомственного надзора и управления;

– нарушители пропускного режима;

– наблюдатели за пределами охраняемой территории.

Помимо этого классификацию можно проводить по следующим параметрам.

Используемые методы и средства:

– сбор информации и данных;

– пассивные средства перехвата;

– использование средств, входящих в информационную систему или систему ее защиты, и их недостатков;

– активное отслеживание модификаций существующих средств обработки информации, подключение новых средств, использование специализированных утилит, внедрение программных закладок и «черных ходов» в систему, подключение к каналам передачи данных.

Уровень знаний нарушителя относительно организации информационной структуры:

– типовые знания о методах построения вычислительных систем, сетевых протоколов, использование стандартного набора программ;

– высокий уровень знаний сетевых технологий, опыт работы со специализированными программными продуктами и утилитами;

– высокие знания в области программирования, системного проектирования и эксплуатации вычислительных систем;

– обладание сведениями о средствах и механизмах защиты атакуемой системы;

– нарушитель являлся разработчиком или принимал участие в реализации системы обеспечения информационной безопасности.

Время информационного воздействия:

– в момент обработки информации;

– в момент передачи данных;

– в процессе хранения данных (учитывая рабочее и нерабочее состояния системы).

По месту осуществления воздействия:

– удаленно с использованием перехвата информации, передающейся по каналам передачи данных, или без ее использования;

– доступ на охраняемую территорию;

– непосредственный физический контакт с вычислительной техникой, при этом можно выделить: доступ к рабочим станциям, серверам предприятия, системам администрирования, контроля и управления информационной системой, программам управления системы обеспечения информационной безопасности.

Порядок выполнения работы

1 В соответствии с последней цифрой шифра из таблицы 2 выбрать нарушителя информационной безопасности.

2 Определить потенциал нарушитель информационной безопасности.

3 Определить, к каким классам относится нарушитель информационной безопасности в соответствии с классификацией, представленной в кратких сведениях из теории.

Таблица 2 – **Нарушители информационной безопасности**

Цифра шифра	Нарушитель информационной безопасности	Цифра шифра	Нарушитель информационной безопасности
0	Несовершеннолетний хакер	5	Опытный хакер одиночка
1	Работник предприятия, не относящийся к службе ЗИ	6	Уволенный работник
2	Группа хакеров	7	Работник службы ЗИ предприятия
3	Спецподразделение конкурирующей компании	8	Разведка своего государства
4	Разведка другого государства	9	Террористическая группировка

4 Для выбранного нарушителя информационной безопасности построить модель в соответствии с указанной выше формой представления (см. таблицу 1), используя в качестве объекта защиты информационную систему, исследованную в практической работе № 1.

Содержание отчета

1 Цель работы.
2 Классификация и потенциал нарушителя информационной безопасности.
3 Модель нарушителя информационной безопасности.
4 Вывод по работе.

Контрольные вопросы

1 Что такое модель нарушителя информационной безопасности?
2 С какой целью строится модель нарушителя информационной безопасности?
3 Какова методика построения модели нарушителя информационной безопасности?
4 Что такое потенциал нарушителя информационной безопасности?
5 По каким основным критериям производится классификация нарушителей информационной безопасности?
6 Какие классы нарушителей информационной безопасности являются наиболее опасными для определенной информационной системы?

Практическая работа №3

КОЛИЧЕСТВЕННАЯ ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы. Изучить методики оценки рисков и необходимости защиты информационной системы. Научиться рассчитывать риски, используя количественную методику.

Краткие сведения из теории

Управление информационными рисками – системный процесс идентификации, контроля и уменьшения информационных рисков

компаний в соответствии с определенными ограничениями нормативно-правовой базы (НПБ) в области защиты информации и собственной корпоративной политики безопасности.

Защита активов связана с деятельностью по предотвращению угроз, классифицируемых в зависимости от характера ущерба, который они могут нанести этим активам. Во внимание должны приниматься все угрозы, но в первую очередь те, которые связаны со случайными и преднамеренными действиями человека.

Основной нормативно-правовой базой являются международные стандарты ISO 17799 и ISO 13335. Согласно СТБ 34.101.1–2014 риск нарушения безопасности – это возможность реализации угрозы, которая нанесет ущерб владельцу. Так же под риском понимают сочетание вероятности события и его последствий.

Суть количественной оценки рисков сводится к поиску единственного оптимального решения из множества существующих. Например, необходимо ответить на следующие вопросы: «Как, оставаясь в рамках утвержденного годового (квартального) бюджета на информационную безопасность, достигнуть максимального уровня защищенности информационных активов компании?» или «Какую из альтернатив построения корпоративной защиты информации (защищенного *WWW* сайта или корпоративной *E-mail*) выбрать с учетом известных ограничений бизнес-ресурсов компании?» К количественным методикам управления рисками относятся методики *CRAMM, MethodWare* и др. Рассмотрим наиболее распространённую из них.

CRAMM. Управление рисками в методике *CRAMM* осуществляется в несколько этапов. На первом этапе инициализации – «*Initialization*» – определяются границы исследуемой информационной системы компании, состав и структура ее основных физических и информационных активов и транзакций. Первичная информация собирается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

На втором этапе идентификации и оценки ресурсов – «*Identification and Valuation of Assets*» – четко идентифицируются активы и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.

На третьем этапе оценивания угроз и уязвимостей – «*Threat and Vulnerability Assessment*» – идентифицируются и оцениваются угрозы и уязвимости информационных активов компании. Для такой оценки и идентификации в коммерческом варианте метода *CRAMM* (профиль *Standard*, в других вариантах совокупность будет иной, например, в версии, используемой в правительственных учреждениях, добавляются параметры, отражающие такие области, как национальная безопасность и международные

отношения) используется следующая совокупность критериев (последствий реализации угроз информационной безопасности): критерий 1 – ущерб репутации организации; 2 – финансовые потери, связанные с восстановлением ресурсов; 3 – дезорганизация деятельности компании; 4 – финансовые потери от разглашения и передачи информации конкурентам, а также другие критерии.

Четвертый этап анализа рисков – «*Risk Analysis*» – позволяет получить количественные оценки рисков. Эти оценки могут быть рассчитаны по формулам (1) – (4):

$$R = P_{\text{ущ}} C_{\text{ущ}}; \tag{1}$$

$$R = P_{\text{угр}} P_{\text{уяз}} C_{\text{ущ}}, \tag{2}$$

где R – величина риска в результате реализации угрозы;

$P_{\text{ущ}}$ – вероятность ущерба в результате реализации угрозы;

$P_{\text{угр}}$ – вероятность реализации угрозы;

$P_{\text{уяз}}$ – вероятность реализации уязвимости;

$C_{\text{ущ}}$ – величина ущерба в результате реализации угрозы.

Если информационный объект (ИО) подвержен нескольким (N) угрозам (критериям оценки возможного ущерба), то совокупный риск ($R_{\text{общ}}$) нанесения злоумышленниками ущерба ИО может быть представлен как

$$R_{\text{общ}} = \sum_{i=1}^{N} P_i \cdot C_i, \tag{3}$$

где C_i – цена ущерба по i-й угрозе;

P_i – вероятность ущерба i-й угрозы, выбираемый экспертами из условия

$$\sum_{i=1}^{N} P_i = 1 \cdot \tag{4}$$

На пятом этапе управления рисками – «*Risk management*» – предлагаются меры и средства уменьшения или уклонения от риска. Возможно проведение коррекции результатов или использование других методов оценки. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком. Только после этого можно переходить к заключительной стадии метода.

На заключительной стадии *CRAMM* генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры разбиваются на группы и подгруппы по следующим категориям:

- обеспечение безопасности на сетевом уровне;
- обеспечение физической безопасности;
- обеспечение безопасности поддерживающей инфраструктуры;
- меры безопасности на уровне системного администратора.

Порядок выполнения работы

1 Оценить риски информационного объекта по методике *CRAMM*.

2 Согласно идентифицируемым уязвимостям и угрозам в практической работе № 1 определить вероятности их реализации согласно таблицам 1 и 2. Результаты оформить в виде таблицы 3.

3 Осуществить расчет рисков согласно формулам (1), (2).

4 Рассчитать общий риск для всего предприятия по формуле (3).

5 По произведенным расчетам оценить уровень ущерба по таблице 4.

Таблица 1 – **Оценка вероятности осуществления угрозы**

Вероятность атаки	Описание	Значение вероятности
1 Очень низкая	Угроза практически никогда не произойдет	[0; 0,25)
2 Низкая	Маловероятно, что эта угроза осуществится, не существует инцидентов, статистики, мотивов и т.п., которые указывали бы на то, что это может произойти.	[0,25; 0,5)
3 Средняя	Вероятность проведения угрозы равновероятна	0,5
4 Высокая	Возможно, эта угроза осуществится (в прошлом происходили инциденты), или существует статистика или другая информация, указывающая на то, что такие или подобные угрозы иногда осуществлялись прежде, или существуют признаки того, что у атакующего могут быть определенные причины для реализации таких действий	(0,5; 0,75]
5 Очень высокая	Угроза, скорее всего, осуществится. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза, скорее всего, осуществится, или могут существовать серьезные причины или мотивы для атакующего, чтобы осуществить такие действия	(0,75; 1]

Таблица 2 – **Оценка вероятности осуществления угрозы через уязвимости**

Вероятность осуществления	Описание	Значение вероятности
1 Высокая	Уязвимость легко использовать, и существует слабая защита или защита вообще отсутствует	(0,75; 1]
2 Средняя	Уязвимость может быть использована, но существует определенная защита	[0,35; 0,75)
3 Низкая	Уязвимость сложно использовать, и существует хорошая защита	[0; 0,35)

Таблица 3 – **Результаты анализа рисков информационного объекта**

Наименование уязвимости	Наименование угрозы	Вероятность осуществления угрозы	Вероятность осуществления уязвимости	Риск, у.е.

Таблица 4 – **Оценка уровня ущерба**

Уровень ущерба	Описание
1 Малый (менее 1000 у.е.)	Незначительные потери материальных активов, которые быстро восстанавливаются, или незначительные последствия для репутации компании
2 Умеренный (от 1000 до 5000 у.е.)	Заметные потери материальных активов, или умеренные последствия для репутации компании
3 Средней тяжести (от 5000 до 10000 у.е.)	Существенные потери материальных активов или значительный урон репутации компании
4 Большой (от 10000 до 30000 у.е.)	Большие потери материальных активов и большой урон репутации компании
5 Критический (более 30000 у.е.)	Критические потери материальных активов, или полная потеря репутации компании на рынке, что делает невозможным ее дальнейшую деятельность

Содержание отчета

1 Цель работы.

2 Результаты оценки рисков по количественной методике, оформленные согласно таблице 3.

3 Вывод по работе.

Контрольные вопросы

1 Этапы количественной методики оценки рисков.
2 Стандарты, регламентирующие управление информационными рисками.
3 Что такое управление информационными рисками?
4 Суть этапа инициализации количественной методики оценки рисков.
5 Критерии оценивания угроз и уязвимостей.
6 Этап анализа рисков.

Практическая работа №4

КАЧЕСТВЕННАЯ ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы. Изучить методики оценки рисков и необходимости защиты информационной системы. Научиться рассчитывать риски, используя качественную методику.

Краткие сведения из теории

Защита активов связана с деятельностью по предотвращению угроз, классифицируемых в зависимости от характера ущерба, который они могут нанести этим активам. Во внимание должны приниматься все угрозы, но в первую очередь те, которые связаны со случайными и преднамеренными действиями человека. На рисунке 1 приведены концептуальные понятия безопасности и их взаимосвязь, регламентируемые СТБ 34.101.1–2014.

В защите активов заинтересованы их собственники (владельцы). Но эти активы представляют интерес и для нарушителей, которые стремятся использовать активы в своих целях, вопреки интересам владельцев. Нарушения безопасности обычно включают (но не ограничиваются только этими категориями): несанкционированное раскрытие (потерю конфиденциальности), несанкционированную модификацию (потерю целостности) или несанкционированное лишение доступа к активам (потерю доступности).

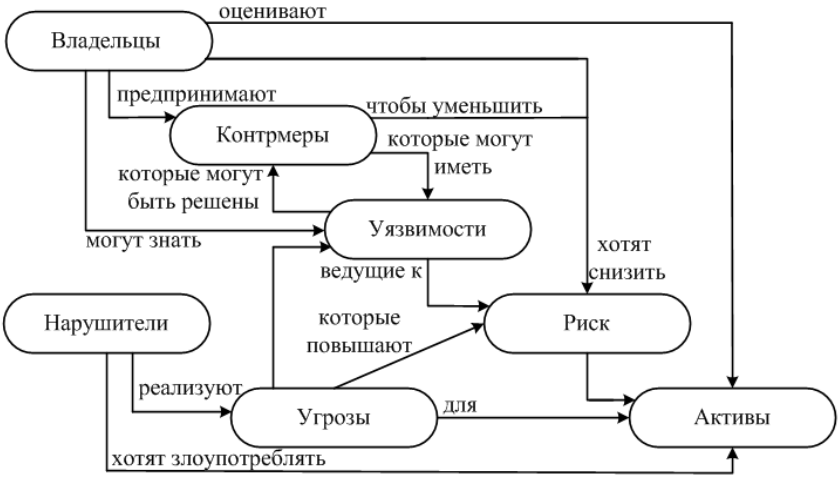

Рисунок 1 – Схема концептуальных понятий безопасности и их взаимосвязь

Владельцы активов должны проводить анализ риска, т. е. определять угрозы, уязвимые места, возможный ущерб от реализации каждой угрозы и контрмеры. Чтобы выполнялась требуемая владельцем политика безопасности активов, необходимо принять меры по уменьшению числа уязвимых мест, так как нарушители могут их использовать.

Еще до ввода в эксплуатацию системы (продукта) ИТ владелец заинтересован в оценке эффективности мер противодействия угрозам.

Результатом такой оценки является заключение о степени гарантии, с которой меры противодействия уменьшают риск для активов. Гарантией называется основание для уверенности в том, что система (продукт) ИТ отвечает задачам безопасности.

Качественная методика предназначена для проведения общей и частных оценок, позволяющих руководителю организации принять обоснованное решение о необходимости защиты конфиденциальной информации, циркулирующей внутри организации, от конкурентов с оценкой предстоящих расходов на защиту. Методика позволяет быстро и достаточно объективно провести экспресс-оценку необходимости защиты конфиденциальной информации и на ее основе оперативно принять соответствующее решение, т. е. она позволяет руководителю избежать больших коммерческих неудач и потерь прибыли из-за доступности информации конкурентам.

Решение о необходимости защиты конфиденциальной информации, циркулирующей внутри организации, должно приниматься руководством организации. Никто не заинтересован в такой мере, как руководство, в защите секретов организации, и никто так не знает всю совокупность циркулирующей в организации информации, ее степень секретности, внутреннюю и внешнюю обстановку, как ее учредитель.

Методика состоит из двух взаимосвязанных частей. Первая часть позволяет на основе обработки результатов анкетного опроса принципиально ответить на вопрос, нужно или не нужно защищать информацию, циркулирующую в организации, а вторая часть, в случае положительного решения первого вопроса, позволяет приближенно оценить затраты на предстоящую защиту информации (ЗИ).

Учитывая заинтересованность, компетентность и кругозор учредителя организации, предложена методика, которая максимально учитывает знания, опыт и мнение самого учредителя организации. В основу первой части методики положен метод анкетного опроса с последующей обработкой его результатов.

Для реализации данного метода разработан перечень анкетных вопросов для учредителя организации, охватывающий все стороны деятельности организации, связанные с циркулирующей на ней информацией.

Вопросы анкеты сформулированы таким образом, что не требуют пространных ответов, а сводятся к односложным ответам «да», «нет». Заполнение анкеты не требует специальной подготовки в области ЗИ и не вызывает трудностей и больших временных затрат. Специальные знания по ЗИ учтены при разработке анкетных вопросов и при последующей обработке результатов опроса с участием специалистов по ЗИ.

Количественная оценка о состоянии и необходимости дополнительной защиты получается путем математической обработки ответов на анкетные вопросы. С этой целью каждому вопросу анкеты поставлена в соответствие

весовая величина, численно выражающая долевой вклад содержания вопроса в общую систему защиты конфиденциальной информации. Значения весовых коэффициентов получены экспертным методом.

При обработке результатов анкетного опроса можно получить как общую оценку состояния защиты в организации, так и ряд частных оценок по направлениям защиты. Совокупность всех оценок позволяет руководителю, в конечном счете, принять решение о необходимости организации защиты путем проведения режимных, организационных и технических мер.

На основе анализа оценок каждой составляющей защиты выявляются те ее звенья, где ЗИ не обеспечена и вероятность ее перехвата конкурентом (утечка) недопустимо высока. Проведя такой анализ, руководитель организации может целенаправленно проводить работы по устранению утечки информации по выявленным направлениям.

Порядок проведения оценок и существо первой части методики заключается в следующем.

На первом этапе заинтересованная в ЗИ сторона в лице учредителя руководителя организации заполняет анкету, отвечая на ее вопросы, приведенные в приложении А. Ответы на вопросы анкеты в форме «да» или «нет» заносятся в столбец 3 таблицы 1 против соответствующих вопросов.

На втором этапе с привлечением консультанта проводится анализ результатов опроса. Если ответ на вопрос соответствует увеличению опасности утечки информации, то в столбце 4 таблицы 1 проставляется знак «+», в противном случае проставляется знак «–».

На третьем этапе производится суммирование долевых коэффициентов столбца 5, соответствующих знаку «+» по всем вопросам анкеты. Долевые коэффициенты для каждого вопроса представлены в приложении Б. Результат суммирования является общей оценкой (G) для принятия решения о необходимости защиты конфиденциальной информации в организации в целом. При этом если общая оценка G равна или больше 50 ($G > 50$), то **защиту необходимо проводить по всем направлениям.**

Если общая оценка G больше 20, но меньше 50 ($50 > G > 20$), то вероятность утечки информации достаточно велика, необходимо провести частные оценки, защита необходима по отдельным направлениям. Если общая оценка меньше 20 ($G < 20$), то **вероятность утечки информации мала и дополнительную защиту информации можно не проводить.**

На четвертом этапе проводится анализ с помощью частных оценок по всем пяти пунктам опросной анкеты. Для получения частных оценок проводят суммирование долевых коэффициентов столбца 6 таблицы 1, помеченных знаком «+» для каждого пункта отдельно. При этом получится пять частных оценок (таблица 2).

Таблица 1 – **Расчет частных и общих оценок рисков по качественной методике**

Анкеты	№ вопроса по пунктам анкеты	Ответы на вопросы анкетируемого	Результаты анализа ответов	Долевые коэффициенты оценок		Оценки	
				общей	частных	общая	частные
1	2	3	4	5	6	7	8
1	1						
	2						
	3						
2	1						
	2						
	3						
3	1						
	2						
	3						
4	1						
	2						
	…						
	11						
5	1						
	2						
	…						
	18						

Таблица 2 – **Частные оценки**

Анкеты	Частная оценка
1	Конкурентоспособность продукции (услуг) – $G1$
2	Степень конфиденциальности информации – $G2$
3	Временные характеристики конфиденциальности информации – $G3$
4	ЗИ режимными и организационными методами – $G4$
5	Возможность утечки информации через технические средства – $G5$

Если частная оценка по каждому из пунктов 1–3 равна или больше 20 ($G1 > 20$, $G2 > 20$, $G3 > 20$), то **это подтверждает необходимость проведения мер по защите информации.**

Если частная оценка по каждому из пунктов 4, 5 равна или больше 20 ($G4 > 20$, $G5 > 20$), то это указывает на необходимость проведения ЗИ режимными и организационными методами или с помощью технических средств защиты соответственно. В том случае, если частная оценка по одному из пунктов 1–3 меньше 20 ($G1 < 20$, $G2 < 20$, $G3 < 20$), то **защиту информации можно не проводить.**

Таким образом, на основе проведенных оценок руководитель организации принимает решение о необходимости проведения работ по организации ЗИ.

Вполне естественно, что перед руководителем организации встает дру-

гой очень важный вопрос о предстоящих затратах на организацию ЗИ. Этот вопрос решается с помощью второй части методики, которая предназначается для определения ориентировочной оценки ожидаемых затрат, связанных с защитой конфиденциальной информации. В общем случае затраты на ЗИ складываются из затрат на проведение организационно-режимных и технических мер. В свою очередь, затраты на техническую защиту складываются из затрат на проведение защиты речевой информации и на защиту других видов информации, в частности, дискретной, обрабатываемой на ПК, телеграфной, факсимильной и других видов, используемых в деятельности организации.

Затраты на режимные и организационные меры ЗИ определяются главным образом заработной платой работников режимных подразделений (групп), обеспечивающих организацию и контроль режимных мер, повышающих безопасность информации. Расчет этих затрат полностью находится в ведении руководителя организации и затруднений не вызывает. Затраты на техническую ЗИ складываются из затрат на проведение исследований, позволяющих выявить каналы утечки информации, определить способы ее защиты, и из ожидаемых затрат на реализацию технических решений защиты.

Порядок выполнения работы

1 Оценить риски по качественной методике.

2 Используя описание информационной системы ответить на вопросы анкеты (см. приложение А).

3 Рассчитать частные и общие оценки и сделать вывод о необходимости проведения мер по защите информации. Для выполнения работы заполнить таблицу 1.

Содержание отчета

1 Цель работы.

2 Ответы на вопросы анкеты в виде таблицы из приложения А.

2 Результаты оценки рисков по качественной методике, оформленные согласно таблице 1.

3 Вывод по работе.

Контрольные вопросы

1 Основные отличия качественной методики оценки рисков от количественной?

2 Этапы качественной методики оценки рисков.

3 Зачем необходимо рассчитывать долевые коэффициенты?

4 Особенность анкетных вопросов в качественной методике оценки рисков.

5 Описание модели безопасности согласно СТБ 34.101.1–2014.

6 Что такое нарушение безопасности.

Практическая работа №5

ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА

Цель работы. Изучить способы разграничения доступа. Научиться распределять права доступа сотрудникам предприятия в зависимости от их должностных обязанностей.

Краткие сведения из теории

Разграничение доступа к элементам защищаемой информации заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий. В этих целях разработаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, программам обработки информации, полям (областям ОЗУ, ПЗУ) и массивам (базам) данных. Само разграничение может осуществляться несколькими способами, а именно:

1) списки контроля доступа (ACL – Access Control Lists);

2) избирательное или дискреционное управление доступом (DAC – Discretionary Access Control, матрицей контроля доступа), схема которого представлена на рисунке 1;

3) полномочное (мандатное) управление доступом (MAC – Mandatory Access Control) – по уровням секретности, схема которого представлена на рисунке 2.

Разграничение доступа по *спискам контроля доступа* заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа. Наиболее полной моделью распределения полномочий является матрица доступа, в строках которой перечислены субъекты, в столбцах – объекты; в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия, текущие права других субъектов) и разрешенные виды доступа. В таблице 1 представлен пример разграничения доступа в структуре университета, права пользователь соответствуют следующим сокращениям: *X* – нет прав; *R* – чтение; *W* – запись; *C* – создание; *E* – редактирование; *D* – удаление.

Избирательное или дискреционное управление доступом (разграничение доступа по матрицам полномочий) предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистриро-

ванных пользователей, а по столбцам – идентификаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя относительно соответствующего элемента. Недостатком метода разграничения доступа на основе матрицы полномочий является то, что с увеличением масштаба данная матрица может оказаться слишком громоздкой. Преодолеть данный недостаток можно путем применения следующих рекомендаций по сжатию матрицы установления полномочий:

– пользователей, имеющих идентичные полномочия, в группы;

– объединение ресурсов, полномочия на доступ к которым совпадают.

Таблица 1 – **Пример таблицы разграничения доступа по списку контроля доступа**

Субъект	Объект			
	персональные данные	финансовые отчеты	учебно-методические комплексы	приказы
Ректорат	*R*	*R*	*R*	*R, W, C, D*
Бухгалтерия	*R*	*W, C, E*	*R*	*R*
Преподаватели	*X*	*X*	*W, R, C, E, D*	*R*
Студенты	*X*	*X*	*R*	*R*

Таблица 2 – **Пример таблицы избирательного разграничения доступа**

Субъект	Объект			
	персональные данные ассистента	финансовый отчет	методическое пособие	приказ
Ректор	*R*	*R*	*R*	*R, W, C, D*
Главный бухгалтер	*R*	*W, C, E*	*R*	*R*
Преподаватель	*X*	*X*	*W, R, C, E, D*	*R*
Студент	*X*	*X*	*R*	*R*

Рисунок 1 – Схема реализации дискреционного управления доступом

Полномочное (мандатное) управление доступом есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

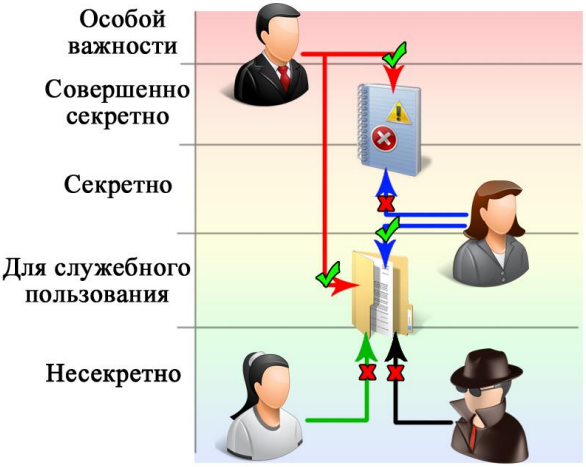

Рисунок 2 – Схема реализации мандатного управления доступом

Полномочное (мандатное) управление доступом заключается в том, что защищаемые данные распределяются по массивам (базам) таким образом, чтобы в каждом массиве (каждой базе) содержались данные одного уровня секретности (например, только с грифом «конфиденциально» или только «секретно», или только «совершенно секретно», или каким-либо другим). Каждому зарегистрированному пользователю предоставляется вполне определенный уровень допуска (например, «секретно», «совершенно секретно» и т. п.). Тогда пользователю разрешается доступ к массиву (базе) своего уровня и массивам (базам) низших уровней и запрещается доступ к массивам (базам) более высоких уровней.

В таблице 3 представлен пример дискреционного управления доступом на железнодорожной станции, причем символ «+» означает наличие разрешенного действия (строка) для субъекта (столбец). В информационной системе выделены следующие субъекты информационной системы: начальник станции, дежурный по станции, начальник участка СЦБ, старший электромеханик, электромеханик, диспетчер отделения дороги.

Таблица 3 – **Пример дискреционного управления доступом на железнодорожной станции**

Действия субъектов согласно ПРД	Субъекты информационной системы					
	начальник станции	дежурный по станции	начальник участка СЦБ	старший электромеханик	электромеханик	диспетчер отделения дороги
Получение информации о поездной обстановке на станции	+	+	+	+	+	+
Получение специальной технологической информации по станции	+	+	–	–	–	–
Получение диагностической информации о системе ПРЦ по фиксированным запросам	–	–	+	+	+	–
Управление объектами станции с обеспечением условий безопасности движения поездов	+	+	–	–	–	–
Техническое обслуживание объектов управления на станции	–	–	+	+	+	–
Обслуживание технических средств ПРЦ	–	–	+	+	+	–

Порядок выполнения работы

1 Выполнить разграничение доступа по спискам контроля доступа для всех пользователей информационной системы Белорусской железной дороги из практической работы № 1. В таблице 4 разделить всех пользователей на не менее чем 5 групп. В таблице 5 прописать разрешенные действия для групп и активов, для обозначения прав использовать следующие сокращения: *X* – нет прав; *R* – чтение; *W* – запись; *C* – создание; *E* – редактирование; *D* – удаление.

Таблица 4 – **Разделение пользователей на группы**

Группа пользователей	Состав группы пользователей			

Таблица 5 – **Разграничение прав пользователей по спискам контроля доступа**

Актив	Группы пользователей				

2 Выполнить избирательное разграничение доступа для всех пользователей предприятия (не менее семи). Задание выполнить в виде таблицы 6.

Таблица 6 – **Разграничение прав пользователь по избирательному контролю доступа**

Пользователи	Активы					

3 Выполнить полномочное управление доступом для всех пользователей предприятия. В таблицах 7 и 8 распределить метки критичности для пользователей (не менее семи) и активов (не менее семи).

Таблица 7 – **Определение меток критичности для пользователей**

Пользователи	Метка критичности				
	Особой важности	Совершенно секретно	Секретно	Для служебного пользования	Несекретно

Таблица 8 – **Определение меток критичности для активов**

Активы	Метка критичности				
	Особой важности	Совершенно секретно	Секретно	Для служебного пользования	Несекретно

Содержание отчета

1 Цель работы.
2 Результаты выполнения задания.
3 Описание информационного объекта.
4 Таблицы правил разграничения доступа.
5 Вывод по работе.

Контрольные вопросы

1 Основные отличия избирательного и полномочного управления доступом.
2 В каких сферах может использоваться мандатное управление доступом?
3 Достоинства и недостатки мандатного разграничения доступа.
4 Особенности разграничения доступа по спискам.

Практическая работа №6

ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Цель работы. Изучить структуру документа политики безопасности. Научиться составлять политику безопасности для информационного объекта.

Краткие сведения из теории

Высокая стоимость конфиденциальных сведений о деятельности конкурирующих структур показывает, что проблема ЗИ от перехвата ее техническими средствами и агентами конкурентов весьма актуальна как для государственного, так и негосударственного сектора. Особенно остро в настоящее время встает вопрос о необходимости защиты конфиденциальной информации негосударственного сектора. Это обусловлено тем, что государственный сектор давно серьезно занимался ЗИ и имеет в настоящее время солидный научно-технический потенциал, силы и технические средства для решения этих задач; негосударственный же сектор в вопросах ЗИ в стране делает первые шаги в отличие от государственного и частных фирм зарубежных стран, где этому вопросу уделяется большое внимание. Отсутствие подготовленных специалистов, научных проработок, опыта, знаний, необходимых документов и технических возможностей фирм у этого сектора в условиях конкуренции ставит их в затруднительное, неравное с предприятиями госсектора, положение.

Задача создания простых методических материалов, позволяющих руководителям грамотно организовать ЗИ на своих предприятиях, весьма актуальна.

Политика безопасности – совокупность норм, правил, рекомендаций, регламентирующих работу средств защиты ИО от фиксированного множества угроз безопасности.

Для определения области политики безопасности необходимо провести анализ угроз и рисков, классифицировать имеющиеся активы и размеры ущербов в случае их повреждения. На основе данного анализа составляют политику безопасности с целью уменьшить возможное проникновение угроз в систему.

Политика безопасности устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Она заставляет людей делать вещи, которые они не хотят делать. Однако она имеет огромное значение для организации и является наиболее важной работой отдела информационной безопасности.

Определение способов развертывания системы безопасности, надлежащих механизмов для защиты информации и систем, правильная настройка компьютерных систем и сетей в соответствии с требованиями физической безопасности – это все функции политики безопасности.

Политика устанавливает порядок осуществления служащими своих обязанностей, связанных с вопросами безопасности, определяет поведение пользователей при использовании компьютерных систем, размещенных в организации. И, самое главное, она устанавливает порядок реагирования в случае каких-либо непредвиденных обстоятельств. При нарушении без-

опасности или сбое в работе системы, политики и процедуры устанавливают порядок действий и выполнения задач, направленные на устранение последствий этого инцидента.

Исходя из положений международного стандарта ISO 17799, можно предложить следующую структуру типовой политики безопасности организации:

1 Общие положения.

1.1 Назначение документа.

1.2 Цели и задачи политики безопасности.

1.3 Нормативно-правовая база.

1.4 Основные определения.

2 Идентификация информационной системы.

2.1 Описание структурных подразделений

2.2 Идентификация активов.

2.3 Классификация информации по уровням секретности.

2.4 Идентификация уязвимостей ИС.

2.5 Идентификация угроз ИС.

2.6 Оценка рисков.

3.Меры информационной безопасности.

3.1 Средства физической безопасности и контроля территории.

3.2 Средства программно-технической защиты информации.

3.3 Средства обеспечения целостности информации.

3.4 Правила разграничения доступа сотрудников к информационным ресурсам.

3.5 Обеспечение безопасности при подключении к сети общего пользования.

4.Управление информационной безопасностью.

4.1 Аудит.

4.2 Осведомленность и обучение специалистов.

4.3 Сообщение об инцидентах информационной безопасности, реагирование и отчетность.

4.4 Должностные обязанности и ответственность.

В подразделе **«Назначение документа»** приводиться описание организации (структурного подразделения организации) и обосновывается необходимость защиты информации и составления политики безопасности.

Каждая политика и процедура имеют четко определенную цель, описывающую причины, почему создана та или иная политика или процедура, и какую выгоду от этого надеется получить организация.

Целью разработки официальной политики предприятия в области информационной безопасности является определение правильного (с точки зрения организации) способа использования вычислительных и коммуникационных ресурсов, а также разработка процедур, предотвращающих или

реагирующих на нарушения режима безопасности. Чтобы достичь данной цели, следует учесть специфику конкретной организации.

Во-первых, необходимо принять во внимание цели и основные направления деятельности организации. Например, на военной базе и в университете существенно разные требования к конфиденциальности.

Во-вторых, разрабатываемая политика должна согласовываться с существующими законами и правилами, относящимися к организации. Значит, эти законы и правила необходимо выявить и принять во внимание при разработке политики.

В-третьих, если локальная сеть организации не является изолированной, вопросы безопасности следует рассматривать в более широком контексте. Политика должна освещать проблемы, возникающие на локальном компьютере из-за действий удаленной стороны, а также удаленные проблемы, причиной которых является локальный хост или пользователь.

К общим целям защиты информации относятся предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Подраздел **«Нормативно-правовая база»** включает в себя перечень нормативных и правовых актов, используемых для написания политики безопасности и разъяснение соответствия положений политики местному и международному законодательству.

В случае если в политике безопасности встречаются нововведенные термины в подразделе **«Основные определения»** приводиться терминология.

В разделе **«Идентификация информационной системы»** классифицируются материальные и информационные ресурсы по их виду и уровню защиты. Также приводится перечень подразделений и должностей, работающих с материальными и информационными ресурсами, подлежащих защите, и отвечающих за работы в области информационной безопасности. В данном разделе представлены результаты идентификации уязвимостей, угроз и оценки рисков.

В разделе **«Меры информационной безопасности»** прописываются основные правила использования информационных и материальных активов с целью сохранения их целостности и недопущения несанкционированного допуска.

В подразделе **«Средства физической безопасности и контроля территории»** могут приводиться регламентация допуска сотрудников в помещения, регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов. Например, системы хранения и передачи данных должны находиться в специальных помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и

постоянно быть под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов. В политике безопасности рекомендуется прописывать требования к средствам идентификации и аутентификации: какие системы должны использоваться для идентификации пользователей, какие пароли должны выбирать пользователи и др.

В подразделе **«Средства программно-технической защиты информации»** должен определяться список программных продуктов для обеспечения информационной безопасности, требования к ним и места для их обязательной установки (файловые серверы, рабочие станции и серверы электронной почты).

В политике безопасности устанавливаются стандартные требования к **управлению доступом** к электронным файлам, в которых предусматриваются формы управления доступом пользователей по умолчанию, доступные для каждого файла в системе. В разделе **«Правила разграничения доступа сотрудников к информационным ресурсам»** определяются разрешения на чтение, запись и исполнение, которые даются владельцам файлов и прочим пользователям системы.

Политика безопасности также описывает правила установки сетевых соединений и используемые механизмы защиты. Для соединений устанавливают технические правила аутентификации и аутентификации для каждого типа соединения (строгий контроль над разрешенными точками доступа). В качестве устройств защиты выделенных линий используют межсетевые экраны.

Политика безопасности должна определять механизмы, используемые при осуществлении удаленного доступа сотрудниками к внутренним системам. При этом политика безопасности должна определять процедуру прохождения авторизации для такого доступа. И самое главное при осуществлении удаленного доступа, чтобы все соединения были защищены шифрованием. Необходимо четко определять условия, при которых разрешается использование беспроводных соединений (если таковые имеются), и то, каким образом будет осуществляться авторизация в такой сети (дополнительные требования, предъявляемые к аутентификации или шифрованию).

В политике безопасности необходимо описывать правила по работе с системой электронной почты. Так, содержание электронных сообщений при обмене документами с партнерами посредством электронной почты должно соответствовать корпоративным стандартам.

Аудит (auditing) – фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам.

Подсистема аудита современных ОС позволяет дифференцированно задавать перечень интересующих администратора событий с помощью удобного графического интерфейса.

Средства учета и наблюдения обеспечивают возможность обнаружить и зафиксировать важные события, связанные с безопасностью, или любые попытки создать, получить доступ или удалить системные ресурсы.

Подраздел **«Осведомленность и обучение специалистов»,** характеризующий меры безопасности, применяемые к персоналу, включает описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п. Пользователи информационной системы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации.

Ключевым элементом политики является доведение до каждого его обязанностей по поддержанию режима безопасности. Политика не может предусмотреть всего, однако она обязана гарантировать, что для каждого вида проблем существует ответственный внутри каждого подразделения, который должен своевременно и правильно среагировать на любой инцидент. Для этого в подразделе **«Сообщение об инцидентах информационной безопасности, реагирование и отчетность»** описывается порядок действия сотрудников при нарушении информационной безопасности.

В разделе **«Должностные обязанности и ответственность»** определяются лица, ответственные за соблюдение политики безопасности и доведения до сведения сотрудников их обязанностей в области информационной безопасности. Дополнения к должностным обязанностям руководителей - ответственность за обеспечение информационной безопасности внутри подразделения, включая ответственность за предоставление отчетов об инцидентах.

В информационной безопасности можно выделить несколько уровней ответственности. На первом уровне каждый пользователь компьютерного ресурса обязан заботиться об информационной защите. Пользователь, допустивший компрометацию, увеличивает вероятность компрометации других ресурсов.

Системные администраторы или руководители подразделений образуют другой уровень ответственности. Они должны обеспечивать защиту компьютерных систем. Сетевых администраторов можно отнести к еще более высокому уровню.

В данном разделе также прописываются ответственности за нарушения установленного порядка пользования ресурсами информационной системы. Любое грубое нарушение порядка и правил пользования информационными ресурсами должно расследоваться. К виновным должны применяться адекватные меры воздействия.

Порядок выполнения работы

1 На основе данных, полученных в предыдущих практических работах, составить политику безопасности информационного объекта в соответствии с рекомендациями, изложенными в кратких сведениях из теории.

Содержание отчета

1 Цель работы.
2 Текст политики безопасности.
3 Вывод по работе.

Контрольные вопросы

1 Какие мероприятия необходимо проводить для внедрения политики безопасности?
2 Какие основные разделы должна включать политика безопасности?
3 Чем отличается идентификация пользователя от аутентификации?
4 Для чего необходим аудит?
5 Классификация информации.

СПИСОК ИСПОЛЬЗОВАННОЙ И РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1 **Корниенко, А. А.** Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) : учеб. пособие для вузов / А. А. Корниенко, М. А. Еремеев, С. Е. Ададуров. – М. : Маршрут, 2006. – 252 с.

2 **Голиков, В. Ф.** Методологические основы информационной безопасности : учеб.-метод. пособие / В. Ф. Голиков, И. И. Черная, О. Б. Зельманский. – Минск : БГУИР, 2012. – 72 с.

3 **Щеглов, А. Ю.** Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2005. – 384 с.

4 **Аверченков, В. И.** Аудит информационной безопасности : учеб. пособие для вузов / В. И. Аверченков. – 2-е изд. – М. : ФЛИНТА, 2011. – 269 с.

5 Основы управления информационной безопасностью : учеб. пособие для вузов / А. П. Курило [и др.]. – 2-е изд., испр. – М. : Горячая линия-Телеком, 2014. – 244 с.

6 **Малюк, А. А.** Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов / А. А. Малюк. – М. : Горячая линия-Телеком, 2004. – 280 с.

7 **Петренко, С. А.** Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. – М. : Компания АйТи, 2006. – 400 с.

8 **Петренко, С. А.** Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М. : ДМК Пресс, 2004. – 384 с.

9 Защита информации в банковских технологиях : учеб.-метод. пособие / Л. М. Лыньков [и др.]. – Минск : БГУИР, 2009. – 198 с.

ПРИЛОЖЕНИЕ А
(*обязательное*)

Анкетные вопросы для качественной методики оценки рисков

№ п/п	Вопросы анкеты	Ответ
Уровень конкуренции		
1	1 Конкурентоспособна ли Ваша продукция на внутреннем рынке?	
	2 Конкурентоспособна ли Ваша продукция на внешнем рынке?	
	3 Монопольна ли Ваша продукция на внутреннем рынке?	
Степень конфиденциальности информации, циркулирующей на фирме		
2	1 Имеется ли информация, предназначенная только лицам верхнего звена управления, с грифом «строго конфиденциально»?	
	2 Имеется ли информация, предназначенная ограниченному кругу лиц, выполняющих конкретные операции и задания, в части, их касающаяся, с грифом «конфиденциально»?	
	3 Имеется ли информация ограниченной доступности только работникам организации?	
Время «старения» конфиденциальности информации		
3	1 Носит ли конфиденциальность долговременный характер (год и более)?	
	2 Носит ли конфиденциальность кратковременный характер (месяц и более)?	
	3 Носит ли конфиденциальность оперативный характер (до месяца)?	
Режимные и организационные мероприятия		
4	1 Учитываются ли интересы сохранения тайны организации при кадровом отборе верхнего звена управления?	
	2 То же при подборе лиц, допущенных к конфиденциальной информации?	
	3 То же при кадровом отборе штатного персонала организации в целом?	
	4 Налажен ли контроль за сохранением работниками организации коммерческой тайны?	
	5 Обеспечена ли охрана организации и конфиденциальной документации, содержащей коммерческую тайну?	
	6 Возможен ли доступ «недопущенных» лиц к средствам размножения и обработки информации, отнесенной к указанным в пункте 2 категориям конфиденциальности?	
	7 Возможно ли, по Вашему мнению, проникновение агента конкурирующей организации в верхнее звено управления?	
	8 То же в среднее звено управления?	
	9 То же в обслуживающий технику персонал?	
	10 То же в персонал, выполняющий работы, прямо не связанные с конфиденциальной информацией?	
	11 Выделено ли специальное помещение для совещаний и переговоров с деловыми партнерами?	

Окончание приложения А

№ п/п	Вопросы анкеты	Ответ
Оснащение служебных помещений техническими средствами		
5	1 Телефонными аппаратами?	
	2 Переговорными устройствами?	
	3 Датчиками пожарной и охранной сигнализации?	
	4 Электрическими и электронными часами?	
	5 Абонентскими громкоговорителями?	
	6 Телефонными аппаратами с автонабором и концентраторами, используемыми в системах связи?	
	7 Установками прямой телефонной связи?	
	8 Сетевое оборудование?	
	9 Телевизорами?	
	10 Серверами?	
	11 Диктофонами?	
	12 Установкой оперативной (директорской) связи?	
	13 Телефаксами?	
	14 Персональными ЭВМ?	
	15 Видеокамерами?	
	16 Автоматической телефонной станцией?	
	17 Радиотелефоном?	
	18 Организована ли техническая защита на фирме?	

ПРИЛОЖЕНИЕ Б
(*обязательное*)

Долевые коэффициенты для расчета риска по качественной методике

№ п/п	Вопросы анкеты	Долевые коэффициенты оценок	
		общих	частных
Уровень конкуренции			
1	1 Конкурентоспособна ли Ваша продукция на внутреннем рынке?	3,5	35
	2 Конкурентоспособна ли Ваша продукция на внешнем рынке?	5,0	50
	3 Монопольна ли Ваша продукция на внутреннем рынке?	1,5	15
Степень конфиденциальности информации, циркулирующей на фирме			
2	1 Имеется ли информация, предназначенная только лицам верхнего звена управления, с грифом «строго конфиденциально»?	11,0	55
	2 Имеется ли информация, предназначенная ограниченному кругу лиц, выполняющих конкретные операции и задания, в части, их касающаяся, с грифом «конфиденциально»?	5,0	25
	3 Имеется ли информация ограниченной доступности только работникам организации?	4,0	20
Время «старения» конфиденциальности информации			
3	1 Носит ли конфиденциальность долговременный характер (год и более)?	5,0	50
	2 Носит ли конфиденциальность кратковременный характер (месяц и более)?	4,0	40
	3 Носит ли конфиденциальность оперативный характер (до месяца)?	1,0	10
Режимные и организационные мероприятия			
4	1 Учитываются ли интересы сохранения тайны организации при кадровом отборе верхнего звена управления?	3,8	13
	2 То же при подборе лиц, допущенных к конфиденциальной информации?	2,7	9
	3 То же при кадровом отборе штатного персонала организации в целом?	1,5	5
	4 Налажен ли контроль за сохранением работниками организации коммерческой тайны?	1,8	6
	5 Обеспечена ли охрана организации и конфиденциальной документации, содержащей коммерческую тайну?	2,2	7,4

Окончание приложения Б

№ п/п	Вопросы анкеты	Долевые коэффициенты оценок	
		общих	частных
4	6 Возможен ли доступ «недопущенных» лиц к средствам размножения и обработки информации, отнесенной к указанным в пункте 2 категориям конфиденциальности?	2,3	7,6
	7 Возможно ли, по Вашему мнению, проникновение агента конкурирующей организации в верхнее звено управления?	6,0	19,7
	8 То же в среднее звено управления?	3,7	12,3
	9 То же в обслуживающий технику персонал?	2,3	7,6
	10 То же в персонал, выполняющий работы, прямо не связанные с конфиденциальной информацией?	1,5	5
	11 Выделено ли специальное помещение для совещаний и переговоров с деловыми партнерами?	2,2	7,4
Оснащение служебных помещений техническими средствами			
5	1 Телефонными аппаратами?	2,5	8,5
	2 Переговорными устройствами?	1,5	5
	3 Датчиками пожарной и охранной сигнализации?	0,6	2
	4 Электрическими и электронными часами?	0,8	2,5
	5 Абонентскими громкоговорителями?	0,9	3
	6 Телефонными аппаратами с автонабором и концентраторами, используемыми в системах связи?	1,5	5
	7 Установками прямой телефонной связи?	1,3	4,5
	8 Сетевое оборудование?	1,5	5
	9 Телевизорами?	1,5	5
	10 Серверами?	0,5	1,5
	11 Диктофонами?	0,5	1,5
	12 Установкой оперативной (директорской) связи?	1,5	5
	13 Телефаксами?	2,2	7,5
	14 Персональными ЭВМ?	3	10
	15 Видеокамерами?	0,9	3
	16 Автоматической телефонной станцией?	3	10
	17 Радиотелефоном?	1,5	5
	18 Организована ли техническая защита на фирме?	4,5	1,5

ОГЛАВЛЕНИЕ

Учебное издание

Белоусова Елена Сергеевна
Буй Павел Михайлович

ПОЛИТИКА БЕЗОПАСНОСТИ
ИНФОРМАЦИОННЫХ СИСТЕМ

Учебно-методическое пособие для практических работ

Редактор *И. И. Эвентов*
Технический редактор *В. Н. Кучерова*

Подписано в печать 26.09.2016. Формат бумаги 60x84$^{1}/_{16}$
Бумага офсетная. Гарнитура Times. Печать на ризографе.
Усл. печ. л. 2,32. Уч.-изд. л. 2,45. Тираж 200 экз.
Зак № . Изд. № 67

Издатель и полиграфическое исполнение:
Белорусский государственный университет транспорта.
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий
№ 1/361 от 13.06.2014.
№ 2/104 от 01.04.2014.
Ул. Кирова, 34, 246653, г. Гомель.