Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерного проектирования

Кафедра инженерной психологии и эргономики

А. М. Прудник

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Рекомендовано УМО по образованию
в области информатики и радиоэлектроники
в качестве пособия для специальностей
1-59 80 01 «Охрана труда и эргономика»,
1-59 81 01 «Управление безопасностью производственных процессов»

Минск БГУИР 2019

УДК 004.056(076)
ББК 32.972.5я73
П85

Р е ц е н з е н т ы:

кафедра инфокоммуникационных технологий учреждения образования «Белорусская государственная академия связи» (протокол №60 от 20.12.2018);

заведующий отделом интеллектуальных информационных систем государственного научного учреждения «Объединенный институт проблем информатики Национальной академии наук Беларуси» кандидат технических наук А. М. Белоцерковский

Прудник, А. М.

П85 Безопасность информационных систем : пособие / А. М. Прудник. – Минск : БГУИР, 2019. – 64 с. : ил.

ISBN 978-985-543-492-5.

Содержит материалы для проведения практических занятий, включающие теоретическую часть, методические указания и задания для самостоятельной работы.

УДК 004.056(076)
ББК 32.972.5я73

ISBN 978-985-543-492-5

СОДЕРЖАНИЕ

1 НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 5
1.1 Теоретические сведения 5
1.2 Задание для самостоятельной работы 5

2 ОПРЕДЕЛЕНИЕ ПРИЧИН И ФАКТОРОВ РИСКА 6
2.1 Общие сведения об информационной системе «CRM» 6
2.2 Теоретические сведения 8
2.3 Задание для самостоятельной работы 8

3 ИДЕНТИФИКАЦИЯ И ОЦЕНКА ЦЕННОСТИ ПЕРВИЧНЫХ И ВТОРИЧНЫХ ИНФОРМАЦИОННЫХ АКТИВОВ 9
3.1 Теоретические сведения 9
3.2 Задание для самостоятельной работы 11

4 ИДЕНТИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ОПИСАНИЕ 13
4.1 Теоретические сведения 13
4.2 Задание для самостоятельной работы 14

5 ИДЕНТИФИКАЦИЯ МЕР ЗАЩИТЫ 16
5.1 Теоретические сведения 16
5.2 Задание для самостоятельной работы 16

6 ИДЕНТИФИКАЦИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ 17
6.1 Теоретические сведения 17
6.2 Задание для самостоятельной работы 18

7 ОПИСАНИЕ СЦЕНАРИЕВ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ 19
7.1 Теоретические сведения 19
7.2 Задание для самостоятельной работы 21

8 АНАЛИЗ И ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ 22
8.1 Теоретические сведения 22
8.2 Задание для самостоятельной работы 24

9 АНАЛИЗ ЗАТРАТ И ВЫГОД ОБРАБОТКИ РИСКОВ 26
9.1 Теоретические сведения 26
9.2 Задача 1 29
9.3 Задача 2 30
9.4 Задача 3 31

10 ОБРАБОТКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 34
10.1 Теоретические сведения 34
10.2 Задание для самостоятельной работы 34

11 ПРОВЕДЕНИЕ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ В СООТВЕТСТВИИ С СТБ 34.101.70–2016 37
11.1 Теоретические сведения 37
11.1.1 Этап идентификации риска 37
11.1.2 Этап анализа риска 46
11.1.3 Этап оценки рисков 54
11.1.4 Этап документирования результатов 57
11.2 Задание для самостоятельной работы 58

ПРИЛОЖЕНИЕ А Базовая форма записи об идентификации, оценке и обработке риска 59

ПРИЛОЖЕНИЕ Б Форма идентификации и устранения несоответствия с элементами оценки риска 61

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 63

1 НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Теоретические сведения

Управление рисками – процесс выявления рисков, обусловленных имеющимися уязвимостями, для информационных активов и инфраструктуры организации и принятия мер по снижению этих рисков до приемлемых уровней. Конфиденциальность, целостность и доступность являются неотъемлемыми характеристиками каждой организации, дающими возможность поддерживать конкурентоспособность в долгосрочной перспективе. Когда жизнеспособность организации зависит от информационных систем (ИС), информационная безопасность вообще и управление рисками в частности должны стать приоритетными соображениями для принятия решений по управлению бизнесом. Эти решения основаны на компромиссах между затратами на применение средств управления информационными системами и выгодами, полученными от их защищенности.

Управление рисками включает в себя три основных мероприятия: выявление рисков, оценка рисков и управление рисками. Идентификация риска – это проверка и документирование состояния безопасности информационных технологий организации и рисков, с которыми она сталкивается. Оценка риска – это определение степени, в которой информационные активы организации подвергаются риску. Управление рисками – это применение средств управления для снижения рисков, связанных с информационными системами организации.

1.2 Задание для самостоятельной работы

Произвести анализ [1, 2] с целью ознакомления с терминологией и приобретения навыков и разобраться в обеспечении в области риск-менеджмента.

Изучить термины, относящиеся к риску, менеджменту риска, процессу менеджмента риска, контексту, оценке риска, анализу риска, идентификации риска, обмену информацией и консультированию, оцениванию риска, обработке риска.

2 ОПРЕДЕЛЕНИЕ ПРИЧИН И ФАКТОРОВ РИСКА

2.1 Общие сведения об информационной системе «CRM»

Для выполнения практических заданий, связанных с оценкой риска информационной безопасности, предлагается компания, осуществляющая деятельность в сфере мелкооптовой и розничной торговли.

Для предоставления покупателям возможности формирования заказов с использованием сети Интернет в компании эксплуатируется информационная система «CRM».

Информационная система «CRM» представляет собой комплекс программно-технических средств компании, предназначенный для осуществления следующих функций:

– представления в сети Интернет товаров (услуг) покупателю (описание, характеристики, стоимость);

– формирования заказов на продажу и (или) доставку товаров (услуг);

– хранения информации о покупателях (клиентах), истории посещений, сформированных, доставленных и оплаченных заказах.

В состав ИС «CRM» входят следующие функциональные компоненты:

– модуль обработки данных (сервер приложений);

– модуль хранения данных (сервер базы данных);

– модуль взаимодействия с пользователями (веб-сервер).

В состав ИС «CRM» входят следующие программно-технические средства:

– серверное оборудование;

– оборудование сети передачи данных.

ИС «CRM» не взаимодействует с внешними информационными системами.

Субъектами ИС «CRM» являются:

– пользователи – покупатели (клиенты) товаров компании, осуществляющие заказ товаров компании с использованием личного кабинета;

– системный администратор – обеспечивает настройку операционных систем и программного обеспечения функциональных модулей ИС, а также автоматизированных рабочих мест (АРМ) сотрудников компании, являющихся пользователями ИС;

– администратор сети передачи данных (СПД) – обеспечивает настройку оборудования, обеспечивающего функционирование ИС;

– менеджеры по продажам – используют ИС для просмотра информации о покупателях (клиентах), истории посещений, сформированных, доставленных и оплаченных заказах с целью передачи заказов в дальнейшую обработку службой реализации и доставки.

В компании утверждено «Положение о коммерческой тайне», устанавливающее требования по защите сведений, составляющих коммерческую тайну

компании, утвержден «Перечень сведений, составляющих коммерческую тайну», назначены ответственные за организацию режима коммерческой тайны.

В компании реализованы следующие программно-технические меры по защите информации:

– для удаленного доступа покупателей к ресурсам ИС «CRM» используется защищенное соединение HTTPS (SSL);

– для антивирусной защиты АРМ сотрудников компании используются встроенные в операционную систему средства антивирусной защиты;

– для идентификации и аутентификации администратора СПД используются функции безопасности, встроенные в системное и прикладное программное обеспечение;

– для управления входящими/исходящими потоками информации используются списки управления доступом (ACL), настроенные на граничном маршрутизаторе.

В ходе проведения аудита информационной безопасности в компании было выявлено следующее:

– не организовано доведение локальных нормативных правовых актов, регламентирующих вопросы обеспечения информационной безопасности;

– отсутствуют процедуры, гарантирующие возврат ресурсов при увольнении;

– не организован контроль физического доступа в здание и помещения;

– работа внешнего персонала (а также сотрудников компании, работающих в нерабочее время) осуществляется без надзора;

– комплекс программно-технических средств (ПТС) ИС «CRM» размещен в офисном помещении компании.

При проведении обследования безопасности ИС «CRM» было выявлено:

– наличие известных уязвимостей в механизмах защиты ИС;

– отсутствие резервирования технических средств, сетевого оборудования ИС;

– отсутствие обновления ПО, используемого для защиты от вредоносного кода;

– отсутствие механизмов мониторинга комплекса ПТС, обеспечивающего функционирование ИС;

– использование в ИС легкоугадываемых паролей (смена паролей осуществляется один раз в 6 месяцев).

Также в ходе аудита было выявлено несоответствие в реализации комплекса мероприятий по защите персональных данных, обрабатываемых комплексом, требованиям «Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам» [3].

2.2 Теоретические сведения

Факторы риска – условия, способствующие проявлению причин риска, определяющие возникновение причин и воздействие различных видов риска.

Причина – источник возникновения риска. Конкретные незапланированные события, которые потенциально могут осуществиться и привести к отклонению от намеченного результата.

2.3 Задание для самостоятельной работы

Определить причины и факторы риска. Результаты представить в виде таблицы 1.

Таблица 1 – Причины и факторы риска

Номер риска	Описание риска	Факторы	Причины
Р-1	Потеря доступа к информации, вследствие реализации внешним злоумышленником атаки, направленной на отказ в обслуживании		
Р-2	Кража или повреждение компьютерного оборудования и носителей информации ИС		
Р-3	Остановка деятельности по оказанию услуг вследствие несоответствия требованиям действующего законодательства		
Р-4	Нарушение целостности и доступности данных информационной системы вследствие внедрения в систему вредоносного кода/вредоносных программ		

3 ИДЕНТИФИКАЦИЯ И ОЦЕНКА ЦЕННОСТИ ПЕРВИЧНЫХ И ВТОРИЧНЫХ ИНФОРМАЦИОННЫХ АКТИВОВ

3.1 Теоретические сведения

Выделяются следующие виды активов:

– первичные (информационные) активы – информация, имеющая ценность для компании, находящаяся в ее распоряжении и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме;

– вторичные активы – ресурсы, используемые компанией для достижения своих целей, на которых размещены или с помощью которых обрабатываются, хранятся первичные (информационные) активы.

Формирование перечня первичных информационных активов должно осуществляться в соответствии с [4], техническими нормативными правовыми актами, а также с учетом оценки критичности актива с точки зрения реализации бизнес-процесса.

Ценность первичного актива определяется исходя из предположения об ущербе, который может быть нанесен бизнесу компании в случае реализации угроз нарушения информационной безопасности в отношении первичного актива.

Шкала ценности актива опирается на три основных свойства: целостность, конфиденциальность и доступность.

Ценность первичных активов определяется в соответствии с критериями, приведенными в таблице 2.

Таблица 2 – Критерии оценки ценности первичных активов

Характеристика актива	Описание с точки зрения бизнеса компании в целом
Критичный (5)	Потеря свойства конфиденциальности, целостности или доступности может привести к невосполнимым финансовым и (или) репутационным потерям для компании: – нанесение прямого вреда компании в размере, не позволяющем осуществление дальнейшей деятельности; – публикация в СМИ развернутых статей негативного содержания по отношению к компании, распространение информации популярными печатными и (или) электронными СМИ; – уменьшение дохода компании ниже уровня условно постоянных расходов; – готовность клиентов полностью отказаться от взаимодействия с компанией; – полная остановка одного из основных процессов ком-

Характеристика актива	Описание с точки зрения бизнеса компании в целом
	пании на срок более 1 месяца; – невозможность решения критически важных задач компании
Высокий (4)	Потеря свойства конфиденциальности, целостности или доступности может привести к высоким финансовым и (или) репутационным потерям для компании: – нанесение прямого вреда компании в размере, осложняющем осуществление дальнейшей деятельности; – распространение негативных отзывов в печатных или электронных СМИ в виде отдельных небольших статей, бесед; – уменьшение дохода компании ниже уровня условно постоянных расходов; – предъявление клиентами или их представителями официальных претензий к компании, открытое распространение негативных отзывов; – значительное ухудшение работы одного из основных процессов компании
Средний (3)	Потеря свойства конфиденциальности, целостности или доступности может привести к средним финансовым и (или) репутационным потерям для компании: – необходимость проведения инициирующих встреч для согласования нарушенных договорных обязательств; – нанесение прямого вреда компании в размере, незначительно осложняющем осуществление дальнейшей деятельности; – распространение в некоторых СМИ небольших заметок негативного содержания; – уменьшение дохода компании до уровня, не позволяющего выделять средства на развитие компании; – предъявление клиентами или их представителями устных претензий своему руководству; – ухудшение работы процессов, не являющихся основными в компании
Низкий (2)	Потеря свойства конфиденциальности, целостности или доступности может привести к низким финансовым и (или) репутационным потерям для компании: – отсутствие необходимости проведения инициирующих встреч для согласования нарушенных договорных обязательств; – отсутствие прямого вреда для компании;

Характеристика актива	Описание с точки зрения бизнеса компании в целом
	– единичное появление в СМИ небольших заметок негативного содержания; – незначительное ухудшение работы процессов, не являющихся основными в компании
Незначительный (1)	Потеря свойства конфиденциальности, целостности или доступности не имеет последствий для компании

Выделяют следующие типы вторичных информационных активов:
– программное обеспечение;
– оборудование (серверное оборудование, АРМ, сетевое оборудование);
– информационные системы;
– бумажные носители информации.

Ценность вторичных активов определяется исходя из правила наследования максимальной ценности первичного актива, обрабатываемого с помощью данного вторичного актива (таблица 3).

Таблица 3 – Пример определения ценности для вторичного актива

Первичный актив	Наименование вторичного актива	К	Ц	Д
ПА-1	ИС «CRM»	3	3	1
ПА-2	ИС «CRM»	3	3	3
ПА-3	ИС «CRM»	5	2	2
Максимальный ущерб		5	3	3

Примечание – Здесь и далее К – конфиденциальность, Ц – целостность, Д – доступность.

3.2 Задание для самостоятельной работы

Провести идентификацию и оценку ценности первичных и вторичных информационных активов. Результаты представить в виде таблиц 4 и 5.

Таблица 4 – Перечень первичных информационных активов

Номер первичного актива	Наименование первичного актива	Владелец актива	Ущерб		
			К	Ц	Д
ПА-1					
ПА-2					
ПА-3					
ПА-4					
ПА-5					

Таблица 5 – Перечень вторичных информационных активов

Номер вторичного актива	Наименование типа вторичного актива	Описание
ВА-1		
ВА-2		
ВА-3		
ВА-4		
ВА-5		

4 ИДЕНТИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ОПИСАНИЕ

4.1 Теоретические сведения

Идентификация возможных источников угроз информационной безопасности (ИБ) в отношении актива характеризуется наличием источника угрозы. Угрозы ИБ могут возникать в результате природных явлений, техногенных событий или случайных/умышленных действий людей.

На этапе идентификации угроз необходимо использовать «Перечень типовых угроз информационной безопасности», приведенный в приложении В стандарта СТБ 34.101.70–2016 [5], выдержки из которого приведены ниже.

Угрозы, связанные с физическим доступом к информационным системам:

– кража или повреждение компьютерного оборудования и носителей информации внутренними нарушителями (инсайдерами);

– кража или повреждение компьютерного оборудования и носителей информации внешними нарушителями;

– кража бумажных документов внутренними нарушителями (инсайдерами);

– кража бумажных документов внешними нарушителями.

Угрозы несанкционированного доступа (НСД):

– присвоение идентификатора пользователя, использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации;

– использование внутренними и внешними нарушителями уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации.

Угрозы недоступности информационных технологий сервисов и разрушения (утраты) информационных активов:

– сбой технических средств (компьютерного оборудования);

– сбой системы кондиционирования воздуха;

– сбой сетевого оборудования;

– флуктуации в сети электропитания.

Угрозы нарушения целостности и несанкционированной модификации данных:

– нарушение целостности систем и данных, баз данных, отчетов и подобного в результате ошибок технического персонала;

– изменение конфигурации активного сетевого оборудования;

– умышленное нарушение целостности систем или данных, несанкционированное изменение системной конфигурации, файлов данных, баз данных, отчетов и подобного со стороны внутренних нарушителей (инсайдеров);

– нарушение целостности систем и данных в результате внедрения в систему и запуска вредоносных программ.

Угрозы антропогенных и природных катастроф:

– антропогенные катастрофы (взрыв, терроризм, вандализм, другие способы умышленного причинения ущерба);

– бомбардировка;

– забастовка;

– природные катастрофы (затопление, пожар, ураган, молния, землетрясение и т. п.).

Юридические угрозы:

– нарушение прав интеллектуальной собственности;

– нелегальное использование ПО;

– несанкционированное использование информационных материалов, являющихся интеллектуальной собственностью;

– нарушение патентного права;

– нарушение (несоответствие требованиям) законодательства и нормативной базы;

– нелегальный импорт/экспорт ПО;

– невыполнение контрактных обязательств.

4.2 Задание для самостоятельной работы

Провести идентификацию актуальных угроз информационной безопасности, которым могут быть подвергнуты активы, определить для каждого вида угрозы показатель «Возможность возникновения угрозы». Результаты представить в виде таблицы 6.

Таблица 6 – Перечень классов, основных источников угроз информационной безопасности и их описание

Источник угрозы информационной безопасности	Описание	Идентификатор угрозы	Возможность возникновения угрозы
Угрозы, связанные с физическим доступом к информационным системам			
Внешний нарушитель/внутренний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации	Уг-1-1	
		Уг-1-2	
		Уг-1-3	
		Уг-1-4	
		Уг-1-5	
Угрозы НСД			
		Уг-2-1	
		Уг-2-2	

Источник угрозы информационной безопасности	Описание	Идентификатор угрозы	Возможность возникновения угрозы
		Уг-2-3	
		Уг-2-4	
		Уг-2-5	
Угрозы недоступности ИТ-сервисов и разрушения (утраты) информационных активов			
		Уг-3-1	
		Уг-3-2	
		Уг-3-3	
		Уг-3-4	
		Уг-3-5	
Угрозы нарушения целостности и несанкционированной модификации данных			
		Уг-4-1	
		Уг-4-2	
		Уг-4-3	
		Уг-4-4	
		Уг-4-5	
Юридические угрозы			
		Уг-5-1	
		Уг-5-2	
		Уг-5-3	
		Уг-5-4	
		Уг-5-5	
Угрозы антропогенных и природных катастроф			
		Уг-6-1	
		Уг-6-2	
		Уг-6-3	
		Уг-6-4	
		Уг-6-5	

5 ИДЕНТИФИКАЦИЯ МЕР ЗАЩИТЫ

5.1 Теоретические сведения

Идентификация мер защиты должна проводиться с учетом уже реализованных или планируемых мер защиты.

Эксперт, выполняющий оценку рисков, определяет, реализуются ли требования безопасности, оговоренные для ИС и определенные на этапе идентификации активов, существующими или планируемыми мерами защиты.

В процессе идентификации уже действующих мер защиты необходимо проверить, правильно ли они функционируют. Если предполагается, что какое-либо средство защиты информации функционирует правильно, однако это не подтверждается в процессе осуществления деловых операций, то его функционирование может стать источником возможной уязвимости.

Результаты идентификации мер защиты документируются в соответствии с таблицами 7 и 8 с указанием статуса их реализации и использования.

5.2 Задание для самостоятельной работы

Провести идентификацию защитных мер. Результаты представить в виде таблицы 7 «Реализованные технические защитные меры» и таблицы 8 «Реализованные организационные защитные меры».

Таблица 7 – Реализованные технические защитные меры

Наименование средства защиты или базового встроенного механизма защиты	Назначение
HTTPS (SSL) для защищенного удаленного доступа клиентов к сервисам	Идентификация и аутентификация клиентов, защита информации от нарушения конфиденциальности и целостности при передаче через сети общего доступа
Встроенные в операционную систему средства антивирусной защиты	Антивирусная защита АРМ сотрудников компании
Механизмы защиты, встроенные в ПО	Идентификация и аутентификация
Использование ACL на маршрутизаторе	Управление потоками информации

Таблица 8 – Реализованные организационные защитные меры

Наименование документа	Процесс, который регламентируется
Положение о коммерческой тайне	Защита сведений, составляющих коммерческую тайну компании. Перечень сведений. Ответственные за организацию режима коммерческой тайны

6 ИДЕНТИФИКАЦИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

6.1 Теоретические сведения

Идентификация уязвимостей предполагает выявление окружающей среды, организации – владельца ИС, процедур, персонала, менеджмента, администрации, аппаратных средств, ПО или средств связи, которые могли бы быть использованы источником угроз для нанесения ущерба ИС. Само по себе наличие уязвимостей не наносит ущерба, поскольку для этого необходимо наличие соответствующей угрозы. Наличие уязвимости при отсутствии такой угрозы не требует применения мер защиты, но уязвимость должна быть зафиксирована и в дальнейшем проверена на случай изменения ситуации.

Понятие «уязвимость» можно отнести к свойствам или атрибутам актива. Исходные данные идентификации уязвимостей следует получать от владельцев или пользователей активов, специалистов по разработке оборудования и информационных технологий (ИТ), а также лиц, отвечающих за реализацию мер защиты в ИС.

В качестве вспомогательной информации для идентификации уязвимостей необходимо использовать «Перечень типовых уязвимостей информационных систем», который приведен в приложении Г СТБ 34.101.70–2016 [5], выдержки из которого приведены ниже.

Безопасность кадровых ресурсов:

– неосведомленность в вопросах безопасности;

– отсутствие процедур, гарантирующих возврат ресурсов при увольнении.

Физическая безопасность:

– неадекватное или небрежное использование механизмов контроля физического доступа в здание, комнаты и офисы;

– безнадзорная работа внешнего персонала или персонала, работающего в нерабочее время;

– подверженность оборудования влиянию температуры;

– подверженность оборудования колебаниям напряжения;

– нестабильное электропитание.

Приобретение, разработка и сопровождение ИС:

– наличие известных уязвимостей в механизмах защиты;

– отсутствие резервирования технических средств, сетевого оборудования.

Управление коммуникационными и информационными процессами:

– отсутствие обновления ПО, используемого для защиты от вредоносного кода;

– отсутствие механизмов мониторинга;

– отсутствие аттестованной системы защиты информации ИС.

Контроль доступа:

– плохое управление паролями (легкоугадываемые пароли, хранение паролей, недостаточно частая смена паролей).

6.2 Задание для самостоятельной работы

Провести идентификацию уязвимостей. Результаты представить в виде таблицы 9.

Таблица 9 – Перечень уязвимостей информационной системы

Номер уязвимости	Описание уязвимости	Угроза, использующая уязвимость
У-1	Отсутствие процедур, гарантирующих возврат ресурсов при увольнении	Уг-1-1
У-2	Безнадзорная работа внешнего персонала или персонала, работающего в нерабочее время	Уг-1-1
У-3	Неадекватное или небрежное использование механизмов контроля физического доступа в здание, комнаты и офисы	Уг-1-1
У-4		
У-5		
У-6		
У-7		
У-8		
У-9		
У-10		

7 ОПИСАНИЕ СЦЕНАРИЕВ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

7.1 Теоретические сведения

Наличие тех или иных возможных сценариев реализации угроз ИБ в отношении защищаемых активов определяется путем идентификации:

– возможных источников угроз ИБ;

– возможных уязвимостей, посредством которых может быть реализована угроза;

– возможных угроз ИБ, которым могут быть подвергнуты активы.

В рамках идентификации источников угроз определяются случайные и преднамеренные источники угроз ИБ.

Идентификация возможных уязвимостей

При определении перечня угроз ИБ должна быть произведена идентификация уязвимостей окружающей среды компании, процедур, аппаратных средств, программного обеспечения, которые могли бы быть использованы источником угроз для нанесения ущерба активам и оказать влияние на процессы в компании, осуществляемые с их использованием. Идентификация уязвимостей производится на основании «Перечня типовых уязвимостей информационных систем» [5].

Идентификация возможных угроз ИБ, которым могут быть подвергнуты активы

В рамках оценки рисков нарушения ИБ необходимо идентифицировать угрозы ИБ, которым могут быть подвергнуты активы. Угрозы ИБ определяются прежде всего в отношении информационных систем, предназначенных для обработки первичных активов, в состав которых в том числе входят вторичные активы, в отношении которых также могут быть реализованы угрозы ИБ.

На этапе идентификации угроз, которым могут быть подвергнуты активы, выделяются актуальные для информационных систем угрозы ИБ, в зависимости от идентифицированных возможных источников угроз и уязвимостей, а также типов вторичных активов. Выбор актуальных угроз по отношению к типам вторичных активов производится на основании сведений об используемых типах вторичных активов, полученных на этапе идентификации активов.

Идентификация угроз ИБ, которым могут быть подвергнуты активы, производится с учетом перечня применимых по отношению к компании угроз, представленных в «Перечне типовых угроз информационной безопасности» [5].

Идентификация актуальных угроз ИБ по отношению к источникам угроз производится на основании экспертного мнения, исходя из следующих критериев:

– анализ применимости (возможности) данного вида источника угрозы к рассматриваемому контексту оценки рисков нарушения ИБ;

– степень доверия пользователям (например, работники, осуществляющие администрирование оборудования, являются наиболее доверенными, чем обычные пользователи);

– возможность возникновения такого рода угроз ИБ в зависимости от территориального (географического) расположения объектов, в которых происходит обработка первичных (информационных) активов.

Выбор актуальных угроз производится либо посредством полного исключения угрозы, либо путем проставления показателя «Возможность возникновения угрозы» (ВВУ).

Определение возможности возникновения угрозы ИБ

Показатель «Возможность возникновения угрозы» характеризует вероятность, с которой та или иная угроза возможна с точки зрения адекватности и/или частоты возникновения для данного вида рассматриваемого объекта, вида местности и т. д.

Определение значения показателя «Возможность возникновения угрозы» осуществляется после идентификации возможных угроз, которым могут быть подвергнуты активы, при этом учитываются следующие факторы:

– частота возникновения угрозы;

– мотивация, возможности и ресурсы, необходимые потенциальному нарушителю и, возможно, имеющиеся в его распоряжении;

– географические и иные факторы (наличие поблизости химических или нефтеперерабатывающих предприятий, возможность возникновения экстремальных погодных условий, факторы, которые могут вызвать ошибки у персонала, техногенные факторы (выход из строя оборудования и т. п.).

Показатель «Возможность возникновения угрозы» может принимать одно из трех возможных значений: «низкая», «средняя» или «высокая». «Возможность возникновения угрозы» в отношении актива определяется на основании оценки частоты реализации угрозы (в свою очередь, частота реализации угрозы определяется на основании свидетельств, полученных в результате анализа инцидентов ИБ от владельцев активов, пользователей информационных систем компании, партнеров компании, а также из других источников), либо экспертным методом в соответствии с критериями, представленными в таблице 10.

Таблица 10 – Критерии определения показателя «Возможность возникновения угрозы»

Возможность возникновения угрозы	Описание
Высокая	– Угроза наиболее характерна для данного вида нарушителя; – случаи подобных угроз случались в недавнем прошлом; – угрозы подобного рода часто происходят в других компаниях; – для данного вида местности (района) угроза наиболее характерна (землетрясение, подтопление, ограбление);

Возможность возникновения угрозы	Описание
	– частота возникновения угрозы может достигать нескольких раз в месяц
Средняя	– Угроза может произойти, однако не так характерна для данного вида нарушителя и вида местности (района); – частота возникновения подобной угрозы может происходить в среднем несколько раз в год
Низкая	– Угроза наименее характерна для данного вида местности (района) и нарушителя; – угрозы подобного рода не реализовывались либо реализовывались довольно редко – не более одного раза в несколько лет

7.2 Задание для самостоятельной работы

Произвести описание сценариев информационной безопасности. Результаты представить в виде таблицы 11.

Таблица 11 – Форма описания сценариев в соответствии с типами вторичных активов, уязвимостями и нарушаемыми свойствами информации

Номер сценария	Описание сценария реализации угрозы	Номера типов вторичных активов	Номер уязвимости	Возможность возникновения угрозы	Нарушаемые свойства информации		
					К	Ц	Д
С-1	Кража или повреждение компьютерного оборудования и носителей информации	ВА-1, ВА-2, ВА-3, ВА-4, ВА-5, ВА-6	У-1, У-2, У-3	Высокая	+	+	+

8 АНАЛИЗ И ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

8.1 Теоретические сведения

На первом этапе на основании показателя «Возможность возникновения угрозы» оценивается вероятность реализации сценариев в отношении активов. Оценка вероятности реализации сценария заключается в анализе возможных сценариев реализации угроз и определении вероятности реализации уязвимости.

На этом этапе для каждой информационной системы, участвующей в оценке рисков, определяются имеющиеся защитные меры, которые могут закрывать имеющиеся уязвимости и тем самым снижать значение показателя «Вероятность использования уязвимостей». Перечень защитных мер фиксируется в «Отчете по результатам оценки рисков нарушения ИБ».

Затем с учетом определенных защитных мер, реализованных в компании, определяется значение показателя «Вероятность эксплуатации уязвимости», характеризующего вероятность, с которой угроза может быть реализована с учетом возможных уязвимостей. Показатель «Вероятность эксплуатации уязвимости» (ВЭУ) может принимать одно из пяти возможных значений: «очень низкая», «низкая», «средняя», «высокая» или «очень высокая». Критерии, исходя из которых определяется показатель «Вероятность эксплуатации уязвимости», представлены в таблице 12.

Таблица 12 – Критерии определения показателя «Вероятность эксплуатации уязвимости»

Уровень вероятности эксплуатации уязвимости	Описание уровня (качественная оценка)
Очень высокий	Защитные меры не реализованы (технические средства защиты не внедрены, регламентация процесса отсутствует)
Высокий	Защитные меры реализованы частично (имеются не все необходимые регламенты), выполняются не полностью, отсутствуют мероприятия по оценке эффективности принятых мер
Средний	Защитные меры реализованы (имеются необходимые регламенты), но выполняются не полностью, отсутствуют мероприятия по оценке эффективности принятых мер

Уровень вероятности эксплуатации уязвимости	Описание уровня (качественная оценка)
Низкий	Защитные меры полностью реализованы и выполняются все необходимые действия по поддержанию высокого уровня защиты, основная часть работ регламентирована, однако отсутствуют отдельные организационно-распорядительные документы по процессам. Не выполняются работы по периодическому тестированию и проверке эффективности применяемых защитных мер
Очень низкий	Защитные меры полностью реализованы и выполняются все необходимые действия по поддержанию максимального уровня защиты (внедрены технические решения, разработаны все необходимые регламенты, выполняется периодическое тестирование и проверка эффективности применяемых защитных мер)

Затем определяется показатель «Вероятность реализации сценария угрозы» (ВРС), который характеризует вероятность реализации угрозы с учетом принятых защитных мер, а также с учетом возможности возникновения угрозы и вычисляется исходя из значений показателей «Возможность возникновения угрозы» и «Вероятность использования уязвимости» согласно матрице, представленной в таблице 13. Показатель «Вероятность реализации сценария угрозы» может принимать одно из пяти возможных значений: «очень низкая», «низкая», «средняя», «высокая» или «очень высокая».

Таблица 13 – Матрица определения показателя «Вероятность реализации сценария угрозы»

		Возможность возникновения угрозы		
		Низкая	Средняя	Высокая
Вероятность использования уязвимости	Очень низкая	Очень низкая	Очень низкая	Низкая
	Низкая	Очень низкая	Низкая	Средняя
	Средняя	Низкая	Средняя	Высокая
	Высокая	Средняя	Высокая	Очень высокая
	Очень высокая	Высокая	Очень высокая	Очень высокая

Далее определяется показатель «Уровень риска нарушения ИБ», который характеризует величину, учитывающую вероятность реализации сценария и величину потерь (возможного ущерба) от реализации данного сценария, и определяется в соответствии с матрицей, представленной в таблице 14.

Таблица 14 – Матрица определения показателя «Уровень риска нарушения ИБ»

	Вероятность реализации сценария				
	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Величина потерь (возможного ущерба)	Н	Н	Н	Н	Н
	Н	Н	Н	С	С
	Н	Н	С	С	В
	Н	Н	С	В	В
	Н	С	В	В	В

Примечание – В матрице используются значения, определяющие уровень риска: Н – низкий уровень риска; С – средний уровень риска; В – высокий уровень риска.

Для каждого из свойств первичного актива (К, Ц, Д) определяется уровень риска (уровень риска нарушения конфиденциальности (РК), уровень риска нарушения целостности (РЦ), уровень риска нарушения доступности (РД)), причем необходимо учитывать, на какие свойства информации направлен тот или иной сценарий. Для этого необходимо руководствоваться «Перечнем типовых угроз информационной безопасности» и «Перечнем типовых уязвимостей информационных систем» [5].

В «Каталоге источников, угроз и уязвимостей» представлен столбец «Нарушаемые свойства информации» (К, Ц, Д), где указаны знаком «+» те свойства, на которые направлен каждый сценарий. При определении значения уровня рисков ИБ для каждого свойства при условии, что сценарий направлен только на одно или на два свойства информации, следует рассчитывать итоговый уровень по данным значениям. Оценку по свойству, на которое сценарий не направлен, не следует учитывать при определении итогового уровня.

Итоговый уровень риска ИБ определяется максимальным значением из РК, РЦ, РД.

Результаты определения значений уровней рисков ИБ вносятся в «Отчет по результатам оценки рисков ИБ».

Далее на этапе оценки рисков принимается решение о принятии рисков. Риски с уровнем «высокий» подлежат обязательной обработке. Риски с уровнями «средний» и «низкий» могут быть приняты.

На данном этапе полученные значения рисков ИБ сравниваются с уровнем допустимого риска и разрабатываются предложения по обработке неприемлемых рисков.

8.2 Задание для самостоятельной работы

Провести анализ и оценку рисков безопасности информационной системы. Результаты представить в виде таблиц 15 и 16.

Таблица 15 – Анализ рисков безопасности информационной системы

Обрабатываемые первичные активы	Реализованные защитные меры	Ущерб		
ПА-1, ПА-2, ПА-3	HTTPS (SSL) для защищенного удаленного доступа клиентов к сервисам Встроенные в операционную систему средства антивирусной защиты Механизмы защиты, встроенные в ПО Использование ACL на маршрутизаторе Положение о коммерческой тайне Инструкция. Порядок приема, перевода и увольнения сотрудников	4	3	2
Высокий риск		Средний риск		Низкий риск	

Примечание – В ячейки, расположенные рядом с ячейками «Высокий риск», «Средний риск», «Низкий риск», записывают численные значения рисков.

Таблица 16 – Оценка рисков безопасности информационной системы

Идентификатор риска	Идентификатор угрозы	Наименование сценария реализации угрозы	ВВУ	Уязвимость	ВЭУ	ВРС	Уровень риска по свойствам			Общий уровень риска	Владелец риска
Р-1	Уг-1-1	Кража или повреждение компьютерного оборудования и носителей информации	Высокая	У-1, У-2, У-3	Высокий	Очень высокая	В	В	С	В	ИТ-директор

9 АНАЛИЗ ЗАТРАТ И ВЫГОД ОБРАБОТКИ РИСКОВ

9.1 Теоретические сведения

Организации должны рассматривать экономическую целесообразность внедрения мер безопасности и мер защиты информации. Несмотря на то что всегда существует несколько вариантов решения проблем информационной безопасности, они не могут иметь одинаковую экономическую целесообразность. Большинство организаций могут потратить только определенное количество времени и средств на обеспечение информационной безопасности, и определение целесообразного количества отличается от организации к организации и даже от руководителя к руководителю. Организациям настоятельно рекомендуется начать анализ затрат и выгод с оценки стоимости информационных активов, подлежащих защите, и потери их стоимости, если эти информационные активы будут скомпрометированы в результате использования конкретных уязвимостей. Формальный процесс принятия решений называется анализом затрат и выгод или экономическим обоснованием.

Точно так же, как сложно определить ценность информации, сложно определить и стоимость защитных мер. Некоторые из элементов, влияющих на стоимость средств управления или защиты, включают следующее:

– стоимость разработки или приобретения оборудования, программного обеспечения и услуг;

– стоимость обучения персонала;

– стоимость внедрения (установки, настройки и тестирования оборудования, программного обеспечения и услуг);

– расходы на обслуживание (плата поставщика за техническое обслуживание и модернизацию);

– стоимость обслуживания (трудозатраты на проверку и постоянное тестирование, обслуживание и обновление).

Выгода – это ценность, которую организация получает, используя средства управления для предотвращения потерь, связанных с конкретной уязвимостью. Сумма выгоды обычно определяется путем оценки информационного актива или активов, подверженных уязвимости, а затем определения того, какая из этих величин подвержена риску и какой риск существует для актива. Выгода может быть выражена как уменьшение ожидаемой годовой убыточности, которая будет определена далее в этом разделе.

Оценка активов – это процесс присвоения финансовой ценности или стоимости каждому информационному активу. Считается, что невозможно абсолютно точно определить ценность информации и информационных активов. Ценность информации различается в организациях и между организациями как по характеристикам информации, так и по воспринимаемой ценности этой информации. Большая часть работы по присвоению стоимости активам может

опираться на инвентаризацию и оценку информационных активов, которые были подготовлены для процесса идентификации рисков.

Оценка активов включает оценку реальных и предполагаемых затрат, связанных с проектированием, разработкой, установкой, обслуживанием, защитой, восстановлением, защитой от потерь и судебными разбирательствами. Эти оценки рассчитываются для каждого набора информационных систем или информационных активов. Затраты на некоторые компоненты легко определить, например, стоимость замены сетевого коммутатора или аппаратного обеспечения, необходимого для определенного класса серверов. Прочие затраты почти невозможно точно определить, например, стоимость потери доли рынка, если информация о предложениях новых продуктов публикуется преждевременно и компания теряет свое конкурентное преимущество. Еще одной проблемой является ценность, приобретаемая некоторыми информационными активами с течением времени. Она может превысить внутреннюю стоимость актива. Более высокая приобретенная стоимость является более подходящей величиной стоимости для оценки в большинстве случаев.

После того как организация оценила стоимость различных активов, необходимо изучить потенциальные потери, которые могут возникнуть в результате эксплуатации уязвимости или возникновения угрозы. Этот процесс приводит к оценке потенциальных потерь на риск. Вопросы, которые в этом случае необходимо рассмотреть, следующие:

– Какой ущерб может быть нанесен и какое финансовое влияние это окажет?

– Сколько будет стоить восстановление после атаки, помимо финансового ущерба?

– Какова ожидаемая единичная потеря для каждого риска?

Ожидаемая единичная потеря (*SLE*) – это расчет значения, связанного с наиболее вероятной потерей в результате атаки. Это величина, рассчитываемая как произведение стоимости актива на фактор подверженности (*EF*), представляющий собой ожидаемый процент потерь, которые могут возникнуть в результате конкретной атаки:

SLE = стоимость актива × фактор подверженности (*EF*),

где *EF* равен проценту потерь, которые могут возникнуть в результате использования данной уязвимости.

Например, если веб-сайт имеет оценочную стоимость в 1 млн дол. США (стоимость определяется с помощью оценки активов), а сценарий преднамеренного саботажа или вандализма указывает на то, что 10 % веб-сайта будут повреждены или уничтожены после такой атаки, тогда *SLE* для этого веб-сайта будет 1 млн дол. США × 0,10 = 100 тыс. дол. США. Затем эта оценка будет использована для расчета значения ожидаемого годового убытка.

Как бы ни было сложно оценить ценность информации, оценить вероятность возникновения угрозы или атаки еще сложнее. Не всегда есть таблицы, книги или записи, которые указывают частоту или вероятность любой данной атаки. Для некоторых пар «актив – угроза» существуют доступные данные в

открытых источниках. Например, вероятность того, что стихийное бедствие разрушит жилой дом в определенном населенном пункте страны, доступна страховым агентам. Однако в большинстве случаев организация может полагаться только на свою внутреннюю информацию для расчета безопасности своих информационных активов. Даже если системные администраторы и специалисты по информационной безопасности активно и точно отслеживают эти события, информация организации не является достаточно полной. В большинстве случаев вероятность возникновения угрозы обычно представляет собой таблицу, в которой указана вероятность атаки для каждого типа угрозы в течение заданного периода времени, например один раз в 10 лет. Эта величина обычно упоминается как годовая частота возникновения (*ARO*). *ARO* – это частота ожидаемой атаки определенного типа. Однако многие атаки происходят гораздо чаще чем один или два раза в год. Например, успешный преднамеренный акт саботажа или вандализма может происходить примерно один раз в два года, и в этом случае *ARO* будет составлять 50 % (0,5), тогда как некоторые виды сетевых атак могут происходить несколько раз в секунду. Для унификации исходных данных необходимо конвертировать ставку в значение в годовом исчислении. Это выражается как вероятность возникновения угрозы.

Как только ценность каждого актива известна, следующим шагом является выяснение того, сколько потерь может быть от одной ожидаемой атаки и как часто эти атаки происходят. После того как эти значения установлены, уравнение может быть завершено для определения общей суммы потерь. Обычно это определяется с помощью ожидаемой годовой суммы потерь (*ALE*), которая рассчитывается на основе *ARO* и *SLE*:

$$ALE = SLE \cdot ARO.$$

Используя пример веб-сайта, который может пострадать от преднамеренного саботажа или вандализма и у которого *SLE* = 100 тыс. дол. США и *ARO* = 0,5, *ALE* будет рассчитываться следующим образом:

ALE = 100 тыс. дол. США × 0,5 = 50 тыс. дол. США.

Это указывает на то, что, если организация не повысит уровень безопасности своего веб-сайта, она может ожидать потери 50 тыс. дол. США ежегодно. Взяв эти данные, подразделение информационной безопасности организации может обосновать расходы на приобретение средств управления в соответствии с запланированным бюджетом. Необходимо обратить внимание, что иногда в процессе экономического обоснования обработки рисков учитываются и неэкономические факторы, поэтому в некоторых случаях, даже если суммы *ALE* невелики, большие или средние бюджеты на приобретение средств управления могут быть оправданы.

В своем простейшем определении анализ затрат и выгод (*CBA*) определяет, стоит ли конкретное средство управления (затраты на него) своей стоимости (получаемых от него выгод). Анализ затрат и выгод (экономическое обоснование) может быть проведен до того, как будет внедрено средство управления, чтобы определить, стоит ли его применять. Анализ затрат и выгод также может

быть проведен после функционирования средств управления в течение некоторого времени, что повышает точность оценки средства управления и дает возможность определить, функционирует ли оно должным образом. Хотя существует много методов анализа затрат и выгод, *CBA* легче всего рассчитать, используя *ALE (до)*, т. е. до внедрения рассматриваемого средства управления, вычитая из него *ALE (после)*, т. е. оцененного после внедрения средства управления и вычитая из полученной разности годовую стоимость защиты (*ACS*):

$$CBA = ALE(до) - ALE(после) - ACS.$$

После того как все средства управления будут внедрены, важно продолжать изучать их преимущества, чтобы определить, когда они должны быть обновлены, дополнены или заменены.

9.2 Задача 1

У организации имеется три информационных актива (сетевой коммутатор, сервер и консоль управления), которые необходимо оценить с точки зрения управления рисками (таблица 17). Какая уязвимость должна рассматриваться для внедрения дополнительных средств управления в первую очередь? Объяснить, какая из них должна рассматриваться в последнюю очередь?

Исходные данные:

1) Сетевой коммутатор соединяет сеть с Интернетом. Он имеет две уязвимости: подвержен аппаратным сбоям с вероятностью возникновения 0,2 и подвержен атаке переполнения буфера SNMP с вероятностью возникновения 0,1. Этот сетевой коммутатор имеет ценность актива (рейтинг воздействия) 90 и не имеет средства управления. Коэффициент определенности, т. е. уверенность в предположениях и имеющихся данных, равен 75%.

2) Веб-сайт компании размещается на сервере и выполняет транзакции электронной торговли. Текущую версию сервера можно атаковать, отправив ей недопустимые значения Unicode. Вероятность этой уязвимости оценивается в 0,1. Серверу была присвоена ценность актива 100, и внедрен элемент управления, который снижает влияние уязвимости на 75 %. Коэффициент определенности равен 80 %.

3) Оператор использует консоль управления для мониторинга операций в серверной комнате, для доступа к которой не используются пароли и она не подвержена угрозе неправильного использования со стороны оператора. Оценка показала, что вероятность возникновения уязвимости составляет 0,1. Этот актив не имеет средства управления, и его ценность равна 5. Коэффициент определенности равен 90 %.

Фактор риска рассчитывается следующим образом:

$$R = I_r \cdot P_v - R_c + U_{ad},$$

где I_r – ценность актива (рейтинг воздействия); P_v – вероятность возникновения уязвимости; R_c – процент снижения риска, обеспеченный имеющимися средствами управления; U_{ad} – неопределенность существующих знаний об уязвимости.

Процент снижения риска, обеспеченный имеющимися средствами управления R_c, рассчитывается по формуле

$$R_c = I_r \cdot P_v \cdot \left(L_p / 100\right),$$

где L_p – процент потери актива, %.

Неопределенность существующих знаний об уязвимости U_{ad} рассчитывается по формуле

$$U_{ad} = I_r \cdot P_v \cdot \left((100 - C_{ad})/100\right),$$

где C_{ad} – коэффициент определенности, %.

Таблица 17 – Исходные данные для оценки информационных активов

Актив	Уязвимость	Ценность актива (рейтинг воздействия)	Вероятность возникновения уязвимости	Процент потери актива L_p	Коэффициент определенности, C_{ad}, %
Сетевой коммутатор	Аппаратный сбой	90	0,2	0	75
	Атака переполнения буфера SNMP	90	0,1	0	75
Сервер	Прием и обработка недопустимых значений Unicode	100	0,1	75	80
Консоль управления	Эксплуатация без паролей допускает злонамеренное использование операторами без паролей	5	0,1	0	0,1

9.3 Задача 2

Рассчитать количество инцидентов в год (*ARO*) и ожидаемый годовой убыток (*ALE*) для каждой категории угроз, с которыми сталкивается компания во время работы над проектом разработки приложения с прогнозируемой прибылью в размере 1 млн 200 тыс. дол. США. Исходные данные представлены в таблице 18.

Ожидаемый годовой убыток рассчитывается как произведение ожидаемой единичной потери (*SLE*) на количество инцидентов в год (*ARO*), т. е.

$$ALE = SLE \cdot ARO.$$

Таблица 18 – Исходные данные для расчета ожидаемых убытков, *ALE*

Категория угрозы	Ожидаемая единичная потеря, *SLE*, дол. США	Частота инцидентов
Ошибки программиста	5000	Один раз в неделю
Потеря интеллектуальной собственности	75 000	Один раз в год
Использование пиратского программного обеспечения	500	Один раз в неделю
Кража информации (хакер)	2500	Один раз в квартал
Кража информации (сотрудник)	5000	Один раз в 6 месяцев
Разрушение веб-сайтов	500	Один раз в месяц
Кража оборудования	5000	Один раз в год
Вирусы, черви, трояны	1500	Один раз в неделю
Атаки типа «отказ в обслуживании»	2500	Один раз в квартал
Землетрясение	250 000	Один раз в 20 лет
Потоп	250 000	Один раз в 10 лет
Пожар	500 000	Один раз в 10 лет

Как компания может получить значения, содержащиеся в таблице 18? Для каждой категории угроз описывайте процесс определения потерь от инцидента и частоты инцидентов.

9.4 Задача 3

Предположим, что прошел один год и компания улучшила безопасность, применив/внедрив несколько элементов управления для каждой категории угроз. Используя информацию из задачи 2 и таблицы 19, вычислить *ARO* и *ALE (после)* с учетом применения/внедрения элементов управления.

Почему изменились значения в некоторых ячейках столбцов «Потери от инцидента» и «Частота инцидентов»? Как элемент управления мог повлиять на один из показателей, но не повлиять на другой?

Предположим, что значения в столбце «Стоимость средства управления», представленные в таблице, – это те затраты, которые непосредственно связаны с защитой от этой угрозы. Другими словами, перекрывающиеся затраты между элементами управления не нужно принимать во внимание.

Необходимо рассчитать *CBA* для запланированного подхода по управлению рисками для каждой категории угроз. Для каждой категории угрозы определить, стоит ли предлагаемый элемент управления затраченных на него средств.

CBA определяет, стоит ли оценивать альтернативу, затрачиваемую на средство управления уязвимостью. *CBA* рассчитывается с использованием *ALE* до и после применения средства управления:

$$CBA = ALE(до) - ALE(после) - ACS,$$

где *ALE (до)* представляет собой годовой ожидаемый риск до внедрения средства управления; *ALE (после)* оценивается как годовой ожидаемый риск после внедрения средства управления; *ACS* – годовая стоимость средства управления.

Таблица 19 – Годовой ожидаемый риск

Категория угрозы	Ожидаемая единичная потеря, *SLE*, дол. США	Частота инцидентов	Стоимость средства управления, дол. США	Тип средства управления
Ошибки программиста	5000	Один раз в месяц	20 000	Обучение сотрудников
Потеря интеллектуальной собственности	75 000	Один раз в 2 года	15 000	Брандмауэр / система обнаружения вторжения
Использование пиратского программного обеспечения	500	Один раз в месяц	30 000	Брандмауэр / система обнаружения вторжения
Кража информации (хакер)	2500	Один раз в 6 месяцев	15 000	Брандмауэр / система обнаружения вторжения
Кража информации (сотрудник)	5000	Один раз в год	15 000	Физическая безопасность
Разрушение вебсайтов	500	Один раз в квартал	10 000	Брандмауэр
Кража оборудования	5000	Один раз в 2 года	15 000	Физическая безопасность
Вирусы, черви, трояны	1500	Один раз в месяц	15 000	Антивирус
Атаки типа «отказ в обслуживании»	2500	Один раз в 6 месяцев	10 000	Брандмауэр
Землетрясение	250 000	Один раз в 20 лет	5000	Страхование / резервное копирование
Потоп	50 000	Один раз в 10 лет	10 000	Страхование / резервное копирование

Категория угрозы	Ожидаемая единичная потеря, *SLE*, дол. США	Частота инцидентов	Стоимость средства управления, дол. США	Тип средства управления
Пожар	100 000	Один раз в 10 лет	10 000	Страхование / резервное копирование

10 ОБРАБОТКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1 Теоретические сведения

На этапе обработки рисков информационной безопасности разрабатываются предложения по обработке неприемлемых рисков.

По результатам оценки рисков должно формироваться обоснование применимости мер обеспечения ИБ.

Реализованные меры обеспечения ИБ должны быть отражены в «Положении о применимости средств управления ИБ».

Остаточный уровень риска определяется экспертным путем на основе прогноза эффективности реализации запланированной меры.

10.2 Задание для самостоятельной работы

Разработать план обработки рисков информационной безопасности, оценить остаточный уровень риска, заполнить «Положение о применимости средств управления ИБ». Результаты представить в виде таблиц 20–22.

Таблица 20 – План обработки рисков информационной безопасности (предлагаемые действия по обработке рисков)

Идентификатор риска	Текущий уровень риска	Предлагаемые действия	Ответственный	Срок	Остаточный уровень риска	Решение по обработке остаточного риска
Р-1	Высокий	Реализовать меры по контролю и управлению доступом в здание и помещения компании	ИТ-директор		Низкий	Принять
		Реализовать процедуры, гарантирующие возврат ресурсов при увольнении	Начальник кадровой службы			
		Реализовать процедуры контроля за работой внешнего персонала или персонала, работающего в нерабочее время	ИТ-директор			

Таблица 21 – План обработки рисков информационной безопасности (сценарии реализации угроз)

Идентификатор риска	Идентификатор угрозы	Наименование сценария реализации угрозы	ВВУ	Уязвимость	ВЭУ	ВРС	Уровень риска по свойствам			Общий уровень риска	Владелец риска
							К	Ц	Д		
Р-1	Уг-1-1	Кража или повреждение компьютерного оборудования и носителей информации	Высокая	–	Очень низкий	Низкая	Н	Н	Н	Н	ИТ-директор

Таблица 22 – Положение о применимости средств управления ИБ

Меры [6]			Существующие меры	Обоснования для исключения меры	Выбранные меры и обоснование выбора					Примечания
Наименование домена	Номер раздела/ подраздела	Наименование раздела/ подраздела			ЗТ	ДО	ТС	ЛП	ОР	
А.8 Управление активами	А.8.1 Ответственность за активы	А.8.1.4 Возврат активов							+	План обработки риска (Р-1)
А.11 Физическая безопасность и защита от окружающей среды	А.11.1 Зоны безопасности	А.11.1.1 Периметр физической безопасности							+	План обработки риска (Р-1)
		А.11.1.2 Средства управления физическим доступом							+	План обработки риска (Р-1)
		А.11.1.3 Безопасность офисов, помещений и оборудования							+	План обработки риска (Р-1)
		А.11.1.5 Работа в зонах безопасности							+	План обработки риска (Р-1)

Примечание – ЗТ – законодательные требования; ДО – договорные обязательства; ТС – требования заинтересованных сторон; ЛП – лучшие практики в области ИБ; ОР – результаты оценки рисков.

11 ПРОВЕДЕНИЕ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ В СООТВЕТСТВИИ С СТБ 34.101.70–2016

11.1 Теоретические сведения

Оценка рисков ИБ ИС проводится в несколько этапов:
1. Этап идентификации рисков, а именно:
– активов;
– угроз;
– уязвимостей;
– мер защиты.
2. Этап анализа рисков:
– оценка вероятности реализации угроз;
– оценка возможных последствий (ущерба).
3. Этап оценки рисков.
Алгоритм проведения оценки рисков ИБ в ИС представлен на рисунке 1.

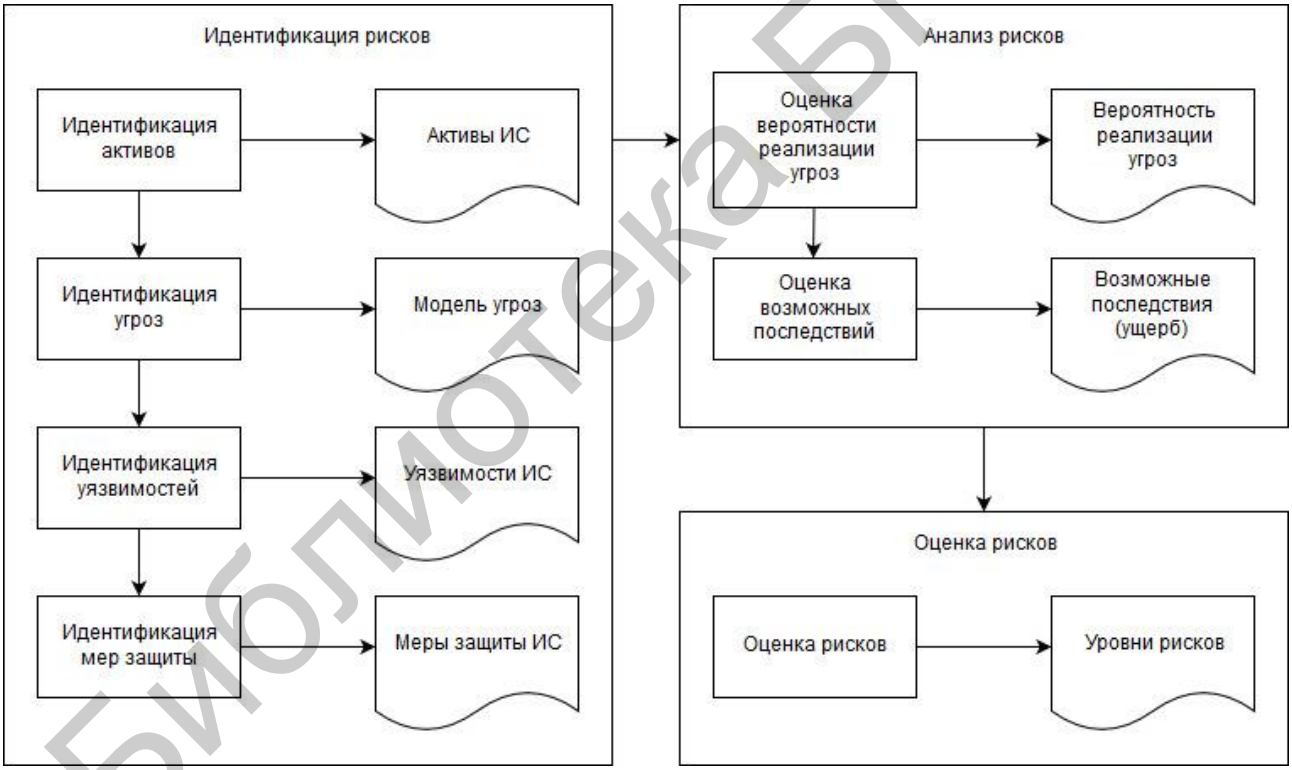

Рисунок 1 – Алгоритм оценки рисков информационной безопасности

11.1.1 Этап идентификации риска

11.1.1.1 Идентификация активов

Все активы ИС должны быть идентифицированы. Для каждого актива должен быть идентифицирован владелец, чтобы обеспечить ответственность и подотчетность для актива.

После того как все активы и их владельцы идентифицированы, должна быть определена ценность этих активов.

Исходные данные для оценки должны быть получены от владельцев и пользователей активов. Чтобы определить ценность активов, необходимо в первую очередь идентифицировать все активы (на соответствующем уровне детализации). Могут различаться основные активы и вспомогательные (поддерживающие).

Основные активы:

– бизнес-процессы и бизнес-деятельность;

– информация.

Вспомогательные (поддерживающие) активы, от которых зависят основные элементы области применения всех типов:

– аппаратные средства;

– программное обеспечение;

– сеть;

– персонал;

– место функционирования организации;

– организация.

Каталог вспомогательных активов ИС приведен в приложении Б СТБ 34.101.70–2016 [5], но следует учитывать, что перечень активов в данном каталоге неполный и может быть дополнен на усмотрение эксперта.

Эксперт, проводящий оценку рисков, должен составить перечень активов, при этом следует запросить содействие лиц, непосредственно являющихся владельцами и/или пользователями ИС, для получения информации по каждому из активов. Полученные данные анализируются экспертом, соотносятся с возможностью негативного воздействия на работу ИС, связанного с нарушением конфиденциальности, целостности, доступности, сохранности и подлинности. Проанализировав собранную информацию, эксперт производит оценку активов. Эксперт должен быть готов по соответствующему требованию объяснить, на основании чего были получены ценности активов ИС. Существуют два варианта для определения ценности:

1) «низкая», «средняя» или «высокая»;

2) с большей степенью детализации: «пренебрежимо малая», «низкая», «средняя», «высокая», «очень высокая».

Конечным результатом данного этапа является составление перечня активов с указанием их ценности.

Результаты идентификации активов ИС документируются в соответствии с формой, представленной в таблице 23.

Таблица 23 – Активы информационной системы

Номер актива	Наименование	Категория	Владелец	Ценность
А-1	Веб-сервер	Аппаратно-программные ресурсы	ИТ-директор	Высокая
А-2	Сервер базы данных	Аппаратно-программные ресурсы	ИТ-директор	Высокая
А-3	Сервер приложений	Аппаратно-программные ресурсы	ИТ-директор	Высокая
А-4	Коммутатор	Сетевое оборудование	ИТ-директор	Средняя
А-5	Маршрутизатор	Сетевое оборудование	ИТ-директор	Средняя
А-6	АРМ системного администратора (сотрудника компании)	Рабочая станция	Системный администратор	Средняя
А-7	АРМ пользователя (сотрудника компании)	Рабочая станция	Специалист по продажам	Средняя
А-8	Персональные данные клиентов: ФИО, телефон, адрес	Информация	Директор	Высокая
А-9	Учетные данные/записи клиентов: логин, настройки учетной записи, список сформированных заказов, сведения об сформированных и отгруженных заказах, сведения о планируемых заказах (корзина)	Информация	Менеджер по продажам	Средняя

11.1.1.2 Идентификация угроз

В основе угроз может лежать как природный, так и человеческий фактор. Они могут реализовываться случайно или преднамеренно. Выявление максимального количества угроз позволит снизить вероятность нарушения функционирования ИС.

Исходные данные для идентификации угроз следует получать от владельцев или пользователей активов, специалистов по разработке оборудования и ИТ, а также лиц, отвечающих за реализацию мер защиты в ИС. Опыт, полу-

ченный в результате инцидентов, и предыдущие оценки угроз должны быть учтены при идентификации угроз. На этапе идентификации угроз необходимо использовать «Перечень типовых угроз информационной безопасности» [5].

При использовании перечня типовых угроз или результатов ранее проводившихся оценок угроз следует иметь в виду, что угрозы постоянно меняются, особенно в случае смены задач, выполняемых ИС.

После завершения оценки угроз составляют перечень идентифицированных угроз.

Результаты идентификации угроз документируются в соответствии с формой, представленной в таблице 24.

Таблица 24 – Модель угроз

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)
Угрозы, связанные с физическим доступом к информационным системам			
Уг-1-1	Физическая угроза	Внешний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации
Уг-1-2	Физическая угроза	Внутренний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации
Угрозы НСД			
Уг-2-1	Угроза НСД	Внешний нарушитель	Использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации
Уг-2-2	Угроза НСД	Внешний нарушитель	Использование уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации
Уг-2-3	Угроза НСД	Внутренний нарушитель	Использование уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)
Угрозы недоступности ИТ-сервисов и разрушения (утраты) информационных активов			
Уг-3-1	Сбой технических средств	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов
Уг-3-2	Сбой системы кондиционирования воздуха	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов
Уг-3-3	Сбой сетевого оборудования	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов
Уг-3-4	Флуктуации в сети электропитания	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов
Угрозы нарушения целостности и несанкционированной модификации данных			
Уг-4-1	Угроза нарушения целостности	Внутренний нарушитель	Нарушение целостности систем и данных, баз данных, отчетов и подобного в результате ошибок технического персонала
Уг-4-2	Угроза нарушения целостности	Внутренний нарушитель	Умышленное нарушение целостности систем или данных, несанкционированное изменение системной конфигурации, файлов данных, баз данных, отчетов и подобного.
Уг-4-3	Несанкционированная модификация данных	Внутренний нарушитель	Изменение конфигурации активного сетевого оборудования
Уг-4-4	Несанкционированная модификация данных	Внешний нарушитель	Изменение конфигурации активного сетевого оборудования
Уг-4-5	Угроза нарушения целостности	Внутренний нарушитель	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей» и т. п.

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)
Уг-4-6	Угроза нарушения целостности	Внешний нарушитель	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей» и т. п.
Несоответствие требованиям надзорных и регулирующих органов, действующему законодательству			
Уг-5-1	Угроза несоответствия требованиям законодательства	Несоответствие действующему законодательству	Административные санкции со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц подразделения, а также остановка отдельных видов деятельности

11.1.1.3 Идентификация уязвимостей

Идентификация уязвимостей предполагает идентификацию уязвимостей окружающей среды, организации-владельца ИС, процедур, персонала, менеджмента, администрации, аппаратных средств, ПО или средств связи, которые могли бы быть использованы источником угроз для нанесения ущерба ИС. Само по себе наличие уязвимостей не наносит ущерба, поскольку для этого необходимо наличие соответствующей угрозы. Наличие уязвимости при отсутствии такой угрозы не требует применения мер защиты, но уязвимость должна быть зафиксирована и в дальнейшем проверена на случай изменения ситуации.

Понятие «уязвимость» можно отнести к свойствам или атрибутам актива. Исходные данные идентификации уязвимостей следует получать от владельцев или пользователей активов, специалистов по разработке оборудования и ИТ, а также лиц, отвечающих за реализацию мер защиты в ИС. В качестве вспомогательной информации для идентификации уязвимостей необходимо использовать «Перечень типовых уязвимостей информационных систем» [5].

Результаты идентификации уязвимостей документируются в соответствии с формой, представленной в таблице 25.

Таблица 25 – Перечень уязвимостей информационной системы

Номер уязвимости	Описание уязвимости	Вид уязвимости	Угроза, использующая уязвимость
Безопасность кадровых ресурсов			
У-1-1	Неосведомленность в вопросах безопасности	Безопасность кадровых ресурсов	Уг-4-1. Нарушение целостности систем и данных, баз данных, отчетов в результате ошибок технического персонала

Номер уязвимости	Описание уязвимости	Вид уязвимости	Угроза, использующая уязвимость
			Уг-4-2. Умышленное нарушение целостности систем или данных, несанкционированное изменение системной конфигурации, файлов данных, баз данных, отчетов
			Уг-4-3. Изменение конфигурации активного сетевого оборудования
У-1-2	Отсутствие процедур, гарантирующих возврат ресурсов при увольнении	Безопасность кадровых ресурсов	Уг-1-2. Кража или повреждение компьютерного оборудования и носителей информации
Физическая безопасность			
У-2-1	Неадекватное или небрежное использование механизмов контроля физического доступа в здание, комнаты и офисы	Физическая безопасность	Уг-1-1. Кража или повреждение компьютерного оборудования и носителей информации
			Уг-1-2. Кража или повреждение компьютерного оборудования и носителей информации
			Уг-4-3. Изменение конфигурации активного сетевого оборудования
			Уг-4-4. Изменение конфигурации активного сетевого оборудования
У-2-2	Безнадзорная работа внешнего персонала или персонала, работающего в нерабочее время	Физическая безопасность	Уг-1-1. Кража или повреждение компьютерного оборудования и носителей информации
			Уг-1-2. Кража или повреждение компьютерного оборудования и носителей информации
			Уг-4-3. Изменение конфигурации активного сетевого оборудования
			Уг-4-4. Изменение конфигурации активного сетевого оборудования

Номер уязвимости	Описание уязвимости	Вид уязвимости	Угроза, использующая уязвимость
У-2-3	Подверженность оборудования влиянию температуры	Физическая безопасность	Уг-3-2. Сбой системы кондиционирования воздуха
У-2-4	Подверженность оборудования колебаниям напряжения	Физическая безопасность	Уг-3-4. Флуктуации в сети электропитания
У-2-5	Нестабильное электропитание	Физическая безопасность	Уг-3-4. Флуктуации в сети электропитания
Приобретение, разработка и сопровождение ИС			
У-3-1	Наличие неизвестных уязвимостей в механизмах защиты	Приобретение, разработка и сопровождение ИС	Уг-2-2. Использование уязвимых мест в компонентах системы защиты
			Уг-2-3. Использование уязвимых мест в компонентах системы защиты
У-3-2	Отсутствие резервирования технических средств, сетевого оборудования	Приобретение, разработка и сопровождение ИС	Уг-3-1. Сбой технических средств
			Уг-3-3. Сбой сетевого оборудования
Управление коммуникационными и информационными процессами			
У-4-1	Отсутствие обновления ПО, используемого для защиты от вредоносного кода	Управление коммуникационными и информационными процессами	Уг-4-5. Внедрение в систему и выполнение вредоносных программ
			Уг-4-6. Внедрение в систему и выполнение вредоносных программ
У-4-2	Отсутствие механизмов мониторинга	Управление коммуникационными и информационными процессами	Уг-4-1. Нарушение целостности систем и данных, баз данных, отчетов в результате ошибок технического персонала
			Уг-4-2. Умышленное нарушение целостности систем или данных, несанкционированное изменение системной конфигурации, файлов данных, баз данных, отчетов

Номер уязвимости	Описание уязвимости	Вид уязвимости	Угроза, использующая уязвимость
			Уг-4-3. Изменение конфигурации активного сетевого оборудования
			Уг-4-4. Изменение конфигурации активного сетевого оборудования
У-4-3	Отсутствие аттестованной системы защиты информации ИС	Управление коммуникационными и информационными процессами	Уг-5-1. Угроза несоответствия требованиям законодательства
Контроль доступа			
У-5-1	Плохое управление паролями (легкоугадываемые пароли, хранение паролей, недостаточно частая смена)	Контроль доступа	Уг-2-1. Использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации

11.1.1.4 Идентификация мер защиты

Идентификация мер защиты должна проводиться с учетом уже реализованных или планируемых мер защиты.

Эксперт, выполняющий оценку рисков, определяет, реализуются ли требования безопасности, оговоренные для ИС и определенные на этапе идентификации активов, существующими или планируемыми мерами защиты.

В процессе идентификации уже действующих мер защиты необходимо проверить, правильно ли они функционируют. Если предполагается, что какое-либо средство защиты информации функционирует правильно, однако это не подтверждается в процессе осуществления деловых операций, то его функционирование может стать источником возможной уязвимости.

Результаты идентификации мер защиты документируются в соответствии с формой, представленной в таблице 26, с указанием статуса их реализации и использования.

Таблица 26 – Результат идентификации мер защиты

Номер меры защиты	Наименование меры защиты	Статус реализации/использования
ТМ-1	HTTPS (SSL) для	Идентификация и аутентификация клиен-

Номер меры защиты	Наименование меры защиты	Статус реализации/использования
	защищенного удаленного доступа клиентов к сервисам	тов, защита информации от нарушения конфиденциальности и целостности при передаче через сети общего доступа
ТМ-2	Встроенные в операционную систему средства антивирусной защиты	Антивирусная защита АРМ сотрудников компании
ТМ-3	Механизмы защиты, встроенные в ПО	Идентификация и аутентификация
ТМ-4	Использование ACL на маршрутизаторе	Управление потоками информации
ТМ-5	HTTPS (SSL) для защищенного удаленного доступа клиентов к сервисам	Идентификация и аутентификация клиентов, защита информации от нарушения конфиденциальности и целостности при передаче через сети общего доступа
ТМ-6	Встроенные в операционную систему средства антивирусной защиты	Антивирусная защита АРМ сотрудников компании
ОМ-7	Положение о коммерческой тайне	Защита сведений, составляющих коммерческую тайну компании. Перечень сведений. Ответственные за организацию режима коммерческой тайны
ОМ-8	Инструкция. Порядок приема, перевода и увольнения сотрудников	Порядок приема на работу нового сотрудника. Требования к перемещению сотрудника внутри компании или изменение его задач. Порядок увольнения сотрудника

11.1.2 Этап анализа риска

11.1.2.1 Оценка вероятности реализации угроз

Оценка вероятности реализации угроз должна учитывать природу угроз и особенности, присущие различным группам угроз.

Определение вероятности реализации угроз может быть осуществлено по следующим результатам:

– анализа имеющихся статистических данных о нарушениях ИБ ИС (предыстория);

– применения аналитических или имитационных методов;

– обработки мнений экспертов.

Перечисленные подходы могут применяться как по отдельности, так и комбинированно для повышения степени достоверности получаемых результатов.

Критерии определения вероятности реализации угроз представлены в таблице 27.

Таблица 27 – Критерии определения показателя «Вероятность реализации угрозы»

Вероятность реализации	Описание
Высокая (1,0)	Угроза, скорее всего, осуществится. Существуют инциденты, статистика или другая информация, указывающие на то, что угроза, скорее всего, осуществится, или могут существовать серьезные причины или мотивы для злоумышленника, чтобы осуществить такие действия. Ожидаемая частота реализации угрозы – еженедельно или чаще
Средняя (0,5)	Возможно, эта угроза осуществится (в прошлом происходили инциденты) либо существует статистика или другая информация, указывающие на то, что такие или подобные угрозы иногда осуществлялись прежде, либо существуют признаки того, что у злоумышленника могут быть определенные причины для реализации таких действий. Ожидаемая частота реализации угрозы – примерно один раз в год
Низкая (0,1)	Маловероятно, что эта угроза осуществится, не существует инцидентов, статистики, мотивов, которые указывали бы на то, что это может произойти. Ожидаемая частота реализации угрозы не превышает одного раза в 5–10 лет

Результатом этапа является определение вероятности («высокая», «средняя», «низкая») для каждого типа угроз.

Результаты оценки вероятности реализации угроз документируются в соответствии с формой, представленной в таблице 28.

Таблица 28 – Угрозы ИБ ИС (вероятность реализации угрозы)

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Вероятность реализации угрозы
Угрозы, связанные с физическим доступом к информационным системам				

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Вероятность реализации угрозы
Уг-1-1	Физическая угроза	Внешний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации	Низкая
Уг-1-2	Физическая угроза	Внутренний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации	Средняя
Угрозы НСД				
Уг-2-1	Угроза НСД	Внешний нарушитель	Использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации	
Уг-2-2	Угроза НСД	Внешний нарушитель	Использование уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации	
Уг-2-3	Угроза НСД	Внутренний нарушитель	Использование уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации	
Угрозы недоступности ИТ-сервисов и разрушения (утраты) информационных активов				
Уг-3-1	Сбой технических средств	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Вероятность реализации угрозы
Уг-3-2	Сбой системы кондиционирования воздуха	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Уг-3-3	Сбой сетевого оборудования	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Уг-3-4	Флуктуации в сети электропитания	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Угрозы нарушения целостности и несанкционированной модификации данных				
Уг-4-1	Угроза нарушения целостности	Внутренний нарушитель	Нарушение целостности систем и данных, баз данных, отчетов и подобного в результате ошибок технического персонала	
Уг-4-2	Угроза нарушения целостности	Внутренний нарушитель	Умышленное нарушение целостности систем или данных, несанкционированное изменение системной конфигурации, файлов данных, баз данных, отчетов и т. п.	
Уг-4-3	Несанкционированная модификация данных	Внутренний нарушитель	Изменение конфигурации активного сетевого оборудования	
Уг-4-4	Несанкционированная модификация данных	Внешний нарушитель	Изменение конфигурации активного сетевого оборудования	

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Вероятность реализации угрозы
Уг-4-5	Угроза нарушения целостности	Внутренний нарушитель	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей» и т. п.	
Уг-4-6	Угроза нарушения целостности	Внешний нарушитель	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей» и т. п.	
Несоответствие требованиям надзорных и регулирующих органов, действующему законодательству				
Уг-5-1	Угроза несоответствия требованиям законодательства	Несоответствие действующему законодательству	Административные санкции со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц подразделения, а также остановка отдельных видов деятельности	

11.1.2.2 Оценка возможных последствий

При оценке последствий нарушения ИБ, вытекающих из потери конфиденциальности, целостности, доступности, сохранности и подлинности, необходимо использовать следующую информацию:

– целевое назначение ИС (с учетом, например, процессов, выполняемых ИС);

– критичность ИС и данных (например, ценность и важность ИС для организации);

– конфиденциальность ИС и данных;

– ценность активов.

Основываясь на полученных данных, эксперт производит оценку влияния угроз на активы ИС.

Влияние может ранжироваться в следующем диапазоне: «высокое», «среднее», «низкое». Описание величин влияния угроз приведено в таблице 29.

Таблица 29 – Критерии определения показателя «Последствия нарушения ИБ»

Влияние	Определение влияния
Высокое (100)	Потеря конфиденциальности, целостности, доступности, сохранности и подлинности может привести к тяжелым или катастрофичным неблагоприятным последствиям, которые отразятся на функционировании ИС, а также на ее активах. Тяжелые или катастрофичные неблагоприятные последствия означают, что потеря конфиденциальности, целостности, доступности, сохранности и подлинности может: – вызвать невосполнимую деградацию целевых показателей, в результате чего ИС будет не способна выполнять свои функции; – привести к невосполнимым повреждениям активов
Среднее (50)	Потеря конфиденциальности, целостности, доступности, сохранности и подлинности может привести к серьезным неблагоприятным последствиям, которые отразятся на функционировании ИС, а также на ее активах. Серьезные неблагоприятные последствия означают, что потеря конфиденциальности, целостности, доступности, сохранности и подлинности может: – вызвать значительную деградацию целевых показателей ИС, при этом ИС будет выполнять свои основные функции, но эффективность этих функций значительно снизится; – привести к значительным повреждениям активов
Низкое (10)	Потеря конфиденциальности, целостности, доступности, сохранности и подлинности может вызвать ограниченные неблагоприятные последствия, которые отразятся на функционировании ИС, а также на ее активах. Ограниченные неблагоприятные последствия означают, что потеря конфиденциальности, целостности, доступности, сохранности и подлинности может вызвать деградацию целевых показателей ИС, при этом ИС будет способна выполнять свои основные функции, но эффективность этих функций заметно снизится

Результатом этапа является определение влияния угроз на безопасность ИС.

Результаты оценки возможных последствий документируются в соответствии с формой, представленной в таблице 30.

Таблица 30 – Угрозы ИБ ИС (влияние)

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Влияние угрозы
Угрозы, связанные с физическим доступом к информационным системам				
Уг-1-1	Физическая угроза	Внешний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации	Среднее
Уг-1-2	Физическая угроза	Внутренний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации	Среднее
Угрозы НСД				
Уг-2-1	Угроза НСД	Внешний нарушитель	Использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации	
Уг-2-2	Угроза НСД	Внешний нарушитель	Использование уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации	
Уг-2-3	Угроза НСД	Внутренний нарушитель	Использование уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации	
Угрозы недоступности ИТ-сервисов и разрушения (утраты) информационных активов				
Уг-3-1	Сбой технических средств	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Уг-3-2	Сбой системы конди-	Форс-мажорные	Недоступность ИТ-сервисов и разрушение (утрата) информа-	

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Влияние угрозы
	ционирования воздуха	обстоятельства	ционных активов	
Уг-3-3	Сбой сетевого оборудования	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Уг-3-4	Флуктуации в сети электропитания	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Угрозы нарушения целостности и несанкционированной модификации данных				
Уг-4-1	Угроза нарушения целостности	Внутренний нарушитель	Нарушение целостности систем и данных, баз данных, отчетов и подобного в результате ошибок технического персонала	
Уг-4-2	Угроза нарушения целостности	Внутренний нарушитель	Умышленное нарушение целостности систем или данных, несанкционированное изменение системной конфигурации, файлов данных, баз данных, отчетов и т. п.	
Уг-4-3	Несанкционированная модификация данных	Внутренний нарушитель	Изменение конфигурации активного сетевого оборудования	
Уг-4-4	Несанкционированная модификация данных	Внешний нарушитель	Изменение конфигурации активного сетевого оборудования	
Уг-4-5	Угроза нарушения целостности	Внутренний нарушитель	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей» и т. п.	
Уг-4-6	Угроза нарушения целостности	Внешний нарушитель	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей» и т. п.	

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Влияние угрозы
Несоответствие требованиям надзорных и регулирующих органов, действующему законодательству				
Уг-5-1	Угроза несоответствия требованиям законодательства	Несоответствие действующему законодательству	Административные санкции со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц подразделения, а также остановка отдельных видов деятельности	

11.1.3 Этап оценки рисков

Окончательное определение рисков осуществляется путем перемножения вероятности реализации и уровня возможных последствий с использованием матрицы расчета рисков, представленной в таблице 31.

Таблица 31 – Матрица расчета уровня рисков

Вероятность угрозы	Влияние		
	Низкое (10)	Среднее (50)	Высокое (100)
Низкая (0,1)	Низкий (10·0,1=1)	Низкий (50·0,1=5)	Низкий (100·0,1=10)
Средняя (0,5)	Низкий (10·0,5=5)	Средний (50·0,5=25)	Средний (100·0,5=50)
Высокая (1,0)	Низкий (10·1,0=10)	Средний (50·1,0=50)	Высокий (100·1,0=100)

В таблице 32 приведено описание уровней риска. Здесь представлена шкала риска с рейтингом риска («высокий», «средний» и «низкий»). Данный рейтинг представляет степень или уровень риска, которому ИС, средство или процедуры могут подвергнуться, если будет реализована некоторая угроза. На этой шкале риска также предлагаются действия, которые руководство организации, собственник ИС или данных должны предпринять для данного уровня риска.

Таблица 32 – Шкала риска и необходимых действий

Уровень риска	Влияние угрозы
Высокий (от 51 до 100)	Если в результате обследования риск оценен как высокий, необходимо быстро выполнить корректирующие действия. Существующая система может продолжать функционировать, но корректирующие действия должны быть произведены незамедлительно

Уровень риска	Влияние угрозы
Средний (от 11 до 50)	Если в результате обследования риск оценен как средний, необходимы корректирующие действия, которые должны лечь в основу плана снижения риска, чтобы реализовать эти действия в разумные сроки
Низкий (от 1 до 10)	Если в результате обследования риск оценен как низкий, необходимо на уровне руководства организации определить, следует выполнять корректирующие действия или принять риск

Результатом этапа оценки рисков является оценка уровня риска («высокий», «средний», «низкий») для каждой угрозы ИС.

Результаты оценки риска документируются в соответствии с формой, представленной в таблице 33.

Таблица 33 – Угрозы ИБ ИС (уровень риска)

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Уровень риска
Угрозы, связанные с физическим доступом к информационным системам				
Уг-1-1	Физическая угроза	Внешний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации	Низкий
Уг-1-2	Физическая угроза	Внутренний нарушитель	Кража или повреждение компьютерного оборудования и носителей информации	Средний
Угрозы НСД				
Уг-2-1	Угроза НСД	Внешний нарушитель	Использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации	
Уг-2-2	Угроза НСД	Внешний нарушитель	Использование уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации	

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Уровень риска
Уг-2-3	Угроза НСД	Внутренний нарушитель	Использование уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НСД к информации	
Угрозы недоступности ИТ-сервисов и разрушения (утраты) информационных активов				
Уг-3-1	Сбой технических средств	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Уг-3-2	Сбой системы кондиционирования воздуха	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Уг-3-3	Сбой сетевого оборудования	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Уг-3-4	Флуктуации в сети электропитания	Форс-мажорные обстоятельства	Недоступность ИТ-сервисов и разрушение (утрата) информационных активов	
Угрозы нарушения целостности и несанкционированной модификации данных				
Уг-4-1	Угроза нарушения целостности	Внутренний нарушитель	Нарушение целостности систем и данных, баз данных, отчетов и подобного в результате ошибок технического персонала	
Уг-4-2	Угроза нарушения целостности	Внутренний нарушитель	Умышленное нарушение целостности систем или данных, несанкционированное изменение системной конфигурации, файлов данных, баз данных, отчетов и т. п.	

Номер угрозы	Вид угрозы	Источник угрозы	Результат реализации угрозы (сценарий)	Уровень риска
Уг-4-3	Несанкционированная модификация данных	Внутренний нарушитель	Изменение конфигурации активного сетевого оборудования	
Уг-4-4	Несанкционированная модификация данных	Внешний нарушитель	Изменение конфигурации активного сетевого оборудования	
Уг-4-5	Угроза нарушения целостности	Внутренний нарушитель	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей» и т. п.	
Уг-4-6	Угроза нарушения целостности	Внешний нарушитель	Внедрение в систему и выполнение вредоносных программ: программных закладок, «троянских коней», программных «вирусов» и «червей» и т. п.	
Несоответствие требованиям надзорных и регулирующих органов, действующему законодательству				
Уг-5-1	Угроза несоответствия требованиям законодательства	Несоответствие действующему законодательству	Административные санкции со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц подразделения, а также остановка отдельных видов деятельности	

11.1.4 Этап документирования результатов

По окончании оценки рисков необходимо документировать результаты в виде отчета. Отчет об оценке риска документально обосновывает процесс анализа рисков и должен включать в себя либо план анализа рисков, либо ссылки на него и результаты оценки опасности.

В отчете должна быть отражена следующая информация:

– цели оценки рисков;

– граница исследования ИС;

– ограничения и допущения, используемые в ходе оценки рисков;

– результаты идентификации активов (см. таблицу 23), результаты идентификации угроз (см. таблицу 24), результаты идентификации уязвимостей ИС (см. таблицу 25);

– результаты идентификации мер защиты (см. таблицу 26);

– результаты оценки вероятности реализации угроз (см. таблицу 27);

– результаты оценки влияния угроз (см. таблицу 28);

– результаты оценки риска (см. таблицу 33);

– выводы;

– используемые модели, в том числе допущения и их обоснования;

– использованные данные и их источники;

– ссылки и рекомендации.

11.2 Задание для самостоятельной работы

Провести оценку, анализ и предложить меры по обработке риска (в соответствии с предложенным вариантом задания) с использованием базовой формы записи об идентификации (приложение А), а также формы идентификации и устранения несоответствия с элементами оценки риска (приложение Б).

ПРИЛОЖЕНИЕ А

(*обязательное*)

БАЗОВАЯ ФОРМА ЗАПИСИ ОБ ИДЕНТИФИКАЦИИ, ОЦЕНКЕ И ОБРАБОТКЕ РИСКА

Дата составления _____ Рег. № ____

1. Идентификация риска

1.1. Исследуемый объект _____

_____

_____

_____

_____

1.2. Событие _____

_____

_____

_____

_____

1.3. Последствия _____

_____

_____

_____

_____

1.4. Объект, подвергающийся риску:

а) _____

_____

б) _____

_____

в) _____

1.5. Источник риска _____

_____

_____

_____

2. Оценка риска

2.1. Тяжесть последствий: незначительная/умеренная/значительная.

2.2. Вероятность возникновения: низкая/средняя/высокая.

2.3. Значимость риска: A – недопустимый (требуется немедленная обработка); B – умеренный (требуется обработка); C – допустимый (обработка не требуется).

Вероятность возникновения	Тяжесть последствий		
	Незначительная	Умеренная	Значительная
Низкая	C	B	B
Средняя	B	B	A
Высокая	B	A	A

3. Обработка риска

Действия по обработке:

– очевидные/неочевидные;

– нересурсоемкие/ресурсоемкие;

– направлены на предупреждение/устранение последствий;

– носят технический/организационный характер.

Описание действий по обработке _____

_____

_____

_____

_____

_____

Ответственный _____

_____

Срок/периодичность исполнения _____

_____

_____

_____

СОСТАВИЛИ:

_____	_____	_____
_____	_____	_____
_____	_____	_____
(Должность)	(Подпись)	(ФИО)

ПРИЛОЖЕНИЕ Б

(*обязательное*)

ФОРМА ИДЕНТИФИКАЦИИ И УСТРАНЕНИЯ НЕСООТВЕТСТВИЯ С ЭЛЕМЕНТАМИ ОЦЕНКИ РИСКА

Дата составления _____ Рег. № ____

1. Идентификация несоответствия

1.1. Объект _____

_____

_____

_____

1.2. Тип несоответствия: несоответствие/потенциальное несоответствие.

_____

_____

_____

1.3. Описание несоответствия _____

_____

_____

_____

1.4. Нормативный документ с указанием раздела и пункта, требования которого не выполнены _____

_____

_____

_____

1.5. Источник (причина) несоответствия_____

_____

_____

_____

2. Оценка риска

2.1. Степень несоответствия: незначительная/умеренная/значительная.

2.2. Вероятность повторного возникновения: маловероятная/вероятная.

2.3. Значимость риска: А – недопустимый (необходимы немедленные действия по устранению); В – умеренный (действия по устранению необходимы в течение определенного времени); С – допустимый (действия по устранению не требуются).

Вероятность повторного возникновения	Степень несоответствия		
	Незначительная	Умеренная	Значительная
Маловероятно	С	С	В
Вероятно	В	В	А

3. Устранение несоответствия

Действия по устранению:

– очевидные/неочевидные;

– нересурсоемкие/ресурсоемкие;

– направлены на предупреждение/устранение последствий;

– носят технический/организационный характер.

Описание действий по обработке _____

_____

_____

_____

_____

_____

Ответственный _____

_____

Срок/периодичность исполнения _____

_____

_____

_____

СОСТАВИЛИ:

_____	_____	_____
_____	_____	_____
_____	_____	_____
(Должность)	(Подпись)	(ФИО)

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. СТБ ISO Guide 73–2014. Менеджмент рисков. Термины и определения. – Введ. 2014–11–01. – Минск : Госстандарт Респ. Беларусь : БелГИСС, 2014. – 24 с.

2. СТБ ISO 31000–2015. Менеджмент рисков. Принципы и руководящие указания. Введ. 2015–09–01. – Минск : Госстандарт Респ. Беларусь : БелГИСС, 2015. – 28 с.

3. Положение о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 30.08.2013 №62 (в редакции приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 11.10.2017 №64) // Национальный правовой интернет-портал Республики Беларусь. – Режим доступа : pravo.by/document/?guid=12. – Дата доступа : 04.03.2019.

4. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. №455-З // Нац. реестр правовых актов Респ. Беларусь. – 2008. – №279, 2/1552.

5. СТБ 34.101.70–2016. Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах. – Введ. 2017–04–01. – Минск : Госстандарт : БелГИСС, 2016. – II, 35 с.

6. СТБ ISO/IEC 27001–2016. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Введ. 2016–10–01. – Минск : Госстандарт : БелГИСС, 2016. – 28 с.

Св. план 2019, поз. 11

Учебное издание

Прудник Александр Михайлович

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

ПОСОБИЕ

Редактор *М. А. Зайцева*
Корректор *Е. И. Костина*
Компьютерная правка, оригинал-макет *В. М. Задоля*

Подписано в печать 16.07.2019. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 3,84. Уч.-изд. л. 4,0. Тираж 50 экз. Заказ 49.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск