МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Разработка методики анализа и оценки угроз информационной безопасности для образовательной организации

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
84,03% авторского текста

Работа рекомендована к защите
«26» декабря 2022 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Молев Константин Сергеевич

Научный руководитель:
д.т.н., профессор
Белевитин В.А.

Челябинск
2023

АННОТАЦИЯ
НА МАГИСТЕРСКУЮ ДИССЕРТАЦИЮ
Молева Константина Сергеевича

Тема работы: **«Разработка методики анализа и оценки угроз информационной безопасности для образовательной организации»**

Определены ключевые угрозы, уязвимости и риски информационной безопасности для организации профессионального образования, и подходы, модели и методики анализа и оценки угроз безопасности информационной системы (ИС) профессиональной образовательной организации (ПОО), а именно конфиденциальности, целостности и доступности. На основе анализа результатов экспертной оценки критических угроз, активов и уязвимостей безопасности ИС ПОО сформулирован предварительный вывод, что комплексные оценки угроз распределены в интервале от значений 2.48 до 2,98. Вероятностный анализ 34-х угроз безопасности ИС профессиональной образовательной организации выявил наибольшую значимость события угрозы «Халатность пользователей» (3,76 %). Разработан проект методики количественной оценки угроз и уязвимостей ИС ПОО путем суммирования выставленных экспертами баллов на вопросы предложенных им тест-анкет. Несомненным достоинством предложенного проекта методики оценки угроз и уязвимостей ИС ПОО, реализующего подход наиболее популярного во всем мире метода CRAMM, является возможность учета множества косвенных факторов, причем не только технических. Основные положения и результаты выполненного педагогического исследования расширили проблемное поле современной теории общей педагогики в вопросах образования с учетом его модернизации за счет количественной оценки эффективности применения новых информационных технологий.

Магистрант _____ _____ Молев К.С.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Преобразования, происходящие во всех сферах российского общества: экономической, социальной, политической, культурной, не миновали и систему образования, определяющую интеллектуальный потенциал страны в будущем и являющуюся условием ее развития и процветания. В современном мире имеет место тенденция слияния образовательных и информационных технологий и формирование на этой основе принципиально новых интегрированных технологий обучения.

Актуальность вопросов безопасности образовательных организаций очевидна – наряду с уже существующими многочисленными угрозами современного мира постоянно появляются новые, изменяется их характер и степень опасности. В свете таких обстоятельств возникает настоятельная необходимость одновременного решения нескольких задач по безопасности используемых образовательными организациями информационных систем. При анализе комплексной безопасности информационных систем образовательных организаций необходимо ориентироваться на приемлемые уровни риска, которые, как правило, установлены федеральными законами, директивными документами, техническими регламентами и т.д. И рассматривать эти риски необходимо как максимально допустимые в реальных условиях технического, экономического и социального состояния общества.

Комплексная безопасность образовательной организации – это состояние ее защищенности от реальных и прогнозируемых угроз социального, техногенного и природного характера, обеспечивающее его безопасное функционирование. Чтобы обеспечить комплексную безопасность, необходимо иметь перечень возможных угроз для объектов образовательных организаций; далее нужно выделить из этого перечня значимые угрозы и выбрать уровень обеспечения безопасности. Определить значимость угроз –

это значит сравнить их между собой с помощью единой шкалы измерений угроз (при разработке такой шкалы следует исходить из тяжести последствий их возможной реализации). Для определения перечня возможных угроз для образовательной организации рекомендуется изучить детальное описание его структуры, связей с другими объектами и т.д.

В свете такого подхода **актуальность** работы определяется:

1) эволюционными тенденциями в системе образования, связанными с необходимостью повышения как качества подготовки кадров в организациях образования, так и, кроме эффективности создания и применения инновационных электронных научно-образовательных ресурсов информационно-коммуникационных технологий (ИКТ), еще и с обеспечением безопасности используемых образовательными организациями информационных систем (ИС);

2) возрастанием требований к безопасности используемых образовательными организациями ИКТ в составе их ИС соответственно изменениям в настроениях пользователей, характера и степени опасности угроз и уязвимостей ИС, реализующих ИКТ.

3) недостаточной разработанностью методик анализа и оценки угроз и уязвимостей ИС образовательных организаций с точки зрения предупреждения и нейтрализации негативных последствий наступления нежелательных событий соответственно изменениям в настроениях пользователей, характера и степени опасности угроз и уязвимостей ИС образовательных организаций.

На основании анализа научных изысканий, а также в результате собственного поиска автора магистерской диссертации в указанном направлении была сформулирована **проблема исследования**. Ее суть заключается в насущной необходимости разрешения **противоречия** между возросшей потребностью обеспечения эффективной безопасности (защиты) используемых об-

разовательными организациями ИС, с одной стороны, и недостаточной разработанностью методик анализа и оценки угроз и уязвимостей ИС образовательных организаций с точки зрения предупреждения и нейтрализации негативных последствий наступления нежелательных событий соответственно изменениям в настроениях пользователей, характера и степени опасности угроз и уязвимостей ИС образовательных организаций, с другой стороны. Данное исследование – попытка внести вклад в решение вышеотмеченной проблемы.

Актуальность рассматриваемой проблемы обусловила выбор темы исследования: «Разработка методики анализа и оценки угроз информационной безопасности для организации профессионального образования».

Объект исследования – управление рисками информационной безопасности в организации профессионального образования.

Предмет исследования – методики анализа и оценки угроз информационной безопасности в организации профессионального образования.

Цель исследования – разработка методики анализа и оценки угроз информационной безопасности для организации профессионального образования на основе компетентностного подхода.

Гипотеза исследования: если в системе организаций профессионального образования будут иметь место научно-обоснованные методики анализа и оценки угроз информационной безопасности реализуемых при обучении студентов в наукоемкой образовательной среде ресурсов информационно-коммуникационных технологий, то становится более реальной возможность предупреждения и нейтрализации негативных последствий наступления нежелательных событий соответственно изменениям в настроениях пользователей, характера и степени опасности угроз и уязвимостей информационной системы образовательных организаций.

В соответствии с целью, объектом, предметом и гипотезой определены следующие **задачи исследования:**

1. На основе изучения научно-методической и психолого-педагогической литературы проанализировать теоретические аспекты информационной безопасности организаций профессионального образования в части угроз и уязвимостей, их количественного анализа и вероятностной оценки.
2. Определить и количественно оценить факторы и критерии угроз и уязвимостей информационной безопасности организаций профессионального образования.
3. Разработать проект методики оценки угроз и уязвимостей информационной системы профессиональной образовательной организации.

Теоретико-методологическую основу исследования дают теории:

– *компетентностного подхода* к профессионально-педагогической подготовке (Е.А. Гнатышина, И.А.Зимняя, Н.В.Кузьмина, Г.М. Коджаспирова, И.А. Колесникова, Дж. Равен, В. Хутмахер, А.В. Хуторской и др.);

– *системного подхода в образовании* (В.Г. Буданов, В.В. Гузеев, Э.Н. Гусинский, С.А. Зайцева, Г.П. Щедровицкий и др.);

– *информационного подхода в образовании* (А.С. Архангельский, А.А. Дорофеев, Г.Н. Степанова, В.С. Степин, и др.);

– *педагогического проектирования и моделирования* (А.П. Аношкин, С.И. Архангельский, В.С. Безрукова, В.П. Беспалько, А.П. Тряпицина, и др.).

Наиболее детально на фоне разворачивающейся информационной революции в научно-технической литературе проработан подход, исследующий проблемы информационной безопасности (В.А. Васенин, Д.П. Зегжд, А.А. Малюк, Е.И. Орлов, А.В. Старовойтов, М.П. Сычев, Н.Г. Шурухнов, В.Н. Ясенев и др.) в части технических приемов и методов обеспечения защиты компьютерной информации и информационных систем. Существенен

вклад в изучение проблем развития и применения информационных технологий в информационном обществе как доминанте развития современного общества в результате широкого внедрения информационных технологий и обеспечения их информационной безопасности Ю.Ф. Абрамова, С.Н. Гриняева, Г.В. Емельянова, К.К. Колина, А.Н. Кочергина, А.В. Манойло, В.В. Мантатова, Л.В. Мантатова, Н.Н. Моисеева, А.И. Позднякова, А.И. Ракитова, С.П. Расторгуев, Г.Л. Смоляна, А.В. Тонконогова, а также Т. Байнама, Ж. Бодрийяра, М. Вебера, Д. Готтербана, У. Дайзарда, П. Друкера, С. Спинелло, Т. Фрелиха, К. Химмы и др.

Для решения поставленных задач и проверки выдвинутой гипотезы нами использованы теоретические и эмпирические методы исследования, совокупность таких подходов, как системный, синергетический и герменевтический позволивших расширить границы предметного поля информационной безопасности и рассматривать защиту безопасности как сложнофункционирующее явление. **Теоретические методы**: анализ психолого-педагогической литературы, монографических и диссертационных работ, публикаций периодической печати по теме исследования, сравнение, аналогия, моделирование. Теоретические методы в процессе организации исследования дополнялись **эмпирическими методами**: опрос, анкетирование, тестирование, наблюдение, индивидуальные и групповые беседы со студентами и преподавателями образовательных организаций. Частные эмпирические методы дополнялись педагогическим экспериментом, результаты которого обрабатывались методами статистической обработки полученной информации.

Экспериментальная база исследования: ГБПОУ "Южно-Уральский энергетический техникум"

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОЦЕНКИ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1. Угрозы, уязвимости и риски информационной безопасности: основные понятия и особенности

Угроза (threat, действие) – это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации [1–2].

Термин «угроза» редко применяют в отношении информационных систем (ИС) и очень часто употребляют применительно к информации, что, по-видимому, связано с самой распространенной таксономией угроз: угрозы конфиденциальности информации, угрозы целостности информации, угрозы доступности информации и угрозы безопасности, ИС в частности [3].

Угроза безопасности ИС – это возможность нарушения безопасности ИС, ИС образовательной организации в частности. Чаще всего угроза – это следствие наличия в защите ИС уязвимых мест, к которым есть доступ посторонних лиц к коммуникационному оборудованию или ошибки в программном обеспечении. Для каждой угрозы существует риск. Если существует угроза, значит, существует и риск ее осуществления.

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании.

Критичность реализации угрозы (Кр) – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурсов, ИС профессиональной образовательной организации, в частности. Задается Кр в процентах. Состоит из критичности реализации угрозы по

конфиденциальности (Крк), целостности (Крц) и доступности (Крд).

Вероятность реализации угрозы через уязвимость в течение календарного года (P(V)) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается P(V) в процентах.

Уязвимость (vulnerability) ИС – это недостаток, чаще ошибка в реализации, которая делает возможным непредусмотренное воздействие на систему, влекущее сбои в работе системы. Уязвимости классифицируются по множеству признаков. Один из особенно важных признаков – вред, который можно нанести системе, используя уязвимость. Чаще всего под уязвимостью понимают конкретную ошибку, допущенную при проектировании или кодировании системы. К возникновению угрозы ведет 99% случаев наличия уязвимостей. Наличие нескольких уязвимостей, используя которые можно осуществить данную угрозу, повышает риск ее осуществления.

Риск – это вероятность или возможность наступления того или иного события. Применительно к ИС образовательной организации понимают всевозможные негативные события. Рисками управляют. Задача управления рисками состоит в идентификации, оценке и минимизации рисков.

Риски необходимо контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность. Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС профессиональной образовательной организации.

Управление рисками можно подразделить на следующие этапы [1]:

– инвентаризация анализируемых объектов;

– выбор методики оценки рисков;

– идентификация активов;

– анализ угроз и их последствий, определение уязвимостей в защите;

– оценка рисков и выбор защитных мер;

– реализация и проверка выбранных мер, оценка остаточного риска.

Первым шагом в процессе оценки рисков является определение объекта оценки, то есть границ анализируемой информационной системы, а также ресурсов и информации, образующих ИС. О системе необходимо собрать следующую информацию [1]:

– архитектура ИС, используемое аппаратное и программное обеспечение;

– системные интерфейсы (внутренняя и внешняя связность);

– топология сети;

– присутствующие в системе данные и информация;

– поддерживающий персонал и пользователи;

– миссия системы (то есть процессы, выполняемые ИС);

– критичность системы и данных;

– чувствительность (т. е. требуемый уровень защищенности) системы и данных.

При этом следует использовать следующие входные данные:

– ресурсы, их критичность, угрозы, действующие на ресурсы;

– отделы, к которым относятся ресурсы;

– уязвимости, через которые реализуются угрозы;

– вероятность реализации угрозы через данную уязвимость;

– критичность реализации угрозы через данную уязвимость.

Для определения уровня безопасности ИС профессиональной образовательной организации желательно следовать следующей цепочке: источник угрозы – уязвимость (фактор) – угроза (действие) – последствия (атака, выбор и разработка мер защиты аппаратного и используемого програм-

много обеспечения, совершенствование политики информационной безопасности профессиональной образовательной организации) (рис. 1.1) [7–9].

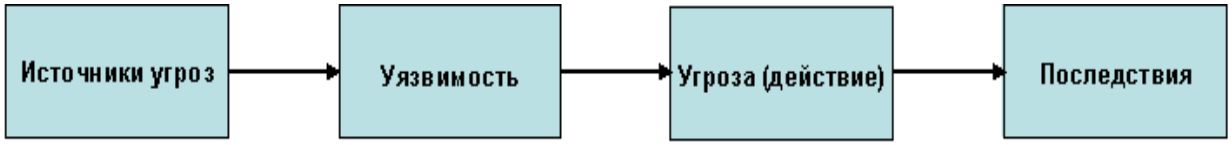

Рис. 1.1 – Логическая цепочка угроз и их проявлений

При этом возникает необходимость рассмотрения возможности создания комбинации угроз/уязвимостей с проблемами конфиденциальности, целостности и/или доступности ИС профессиональной образовательной организации. В зависимости от результатов такого рассмотрения должны быть выбраны подходящие значения ценности активов ИС профессиональной образовательной организации, т.е. значения, которые выражают последствия нарушения или конфиденциальности, или целостности, или доступности ИС профессиональной образовательной организации.

В свете такого подхода с точки зрения базовых угроз информационной безопасности профессиональной образовательной организации существует два алгоритма расчета уровня угроз одной базовой угрозы (суммарной) или трех базовые угрозы (конфиденциальности, целостности и доступности ИС профессиональной образовательной организации), по их уязвимости на основе критичности и вероятности реализации каждой конкретной угрозы.

1.2. Анализ угроз и уязвимостей конфиденциальности, целостности и доступности ИС в профессиональной образовательной организации

1.2.1. Классификация уязвимостей безопасности

Угроза информационной безопасности – это совокупность факторов и последствий, которые могут создать потенциальную или фактическую опасность состоянию защищенности личности, общества и государства.

Такими факторами может быть весь перечень основных принципов функционирования Интернета. Среди них: принципы иерархичности, демократичности, децентрализации, конвергенции и экстерриториальности [15]. В общем смысле под угрозами информационной безопасности принято понимать совокупность факторов и условий, которые создают опасность нарушения безопасности и целостности информации, в том числе копирование, распространение, изменение, блокирование, несанкционированный доступ или иные неуполномоченные действия с защищенной информацией.

Для реализации угроз информационной безопасности необходимо создание канала между носителем информации и источником угрозы, что создает благоприятную среду для нарушения безопасности информационной системы.

Существуют три основных элемента для реализации угроз информационной безопасности, это: источник информации, среда воздействия и носитель. Источником угроз информационной безопасности может выступать материальный объект, субъект или определенное физическое явление, несущее угрозу. Среда воздействия информации представляет собой тот путь распространения информации, в котором 23 определенные программы, данные или сигнал могут оказывать воздействия на доступность, целостность и конфиденциальность защищенной информации. Роль носителя информации может играть как материальный предмет или физическое лицо, так и информационное поле.

Анализ отрицательных воздействий осуществления и возникновения угроз включает в себя обязательную идентификацию возможных источников уязвимостей, угроз, а также методов их реализации. Для осуществления эффективной и комплексной идентификации и дальнейшего

устранения потенциальных угроз информационной безопасности необходимо выстроить четкую классификацию.

Общая классификация угроз информационной безопасности осуществляется:

- по источнику угроз информационной безопасности;
- по степени вероятности осуществления;
- по объекту воздействия;
- по способу реализации;
- по положению источника;
- по характеру источника;
- по последствиям.

Источником угрозы информационной безопасности можно разделить на три группы: антропогенные, технические и природные, но для более подробной классификации необходимо проанализировать каждую из них. Классификация по источнику угроз информационной безопасности представлена на рис. 1.2.

Угрозами безопасности информации ИС профессиональной образовательной организации являются [4; 7]:

– хищение (копирование) информации;

– уничтожение информации;

– модификация (искажение) информации;

– нарушение доступности (блокирование) информации;

– отрицание подлинности информации;

– навязывание ложной информации.

Хищение – совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу иму-

щества.

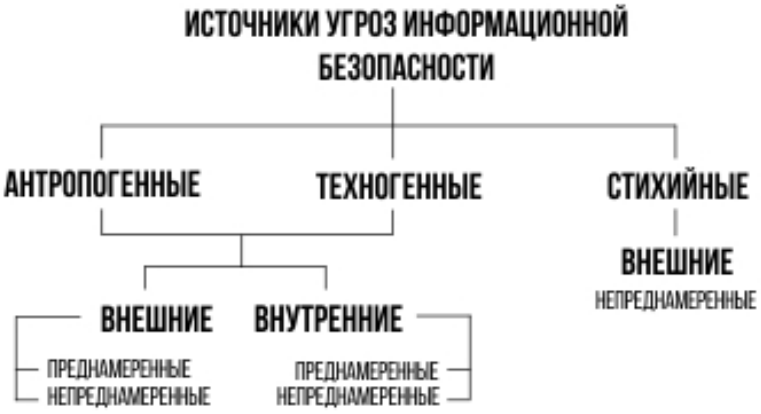

Рис. 1.2 – Классификация по источнику угроз информационной безопасности [33]

Копирование компьютерной информации – повторение и устойчивое запечатление информации на машинном или ином носителе.

Уничтожение – внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.

Уничтожение компьютерной информации – стирание ее в памяти ЭВМ.

Повреждение – это изменение свойств контента (имущества, информационных материалов), при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования.

Модификация компьютерной информации – внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.

Блокирование компьютерной информации – искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

Несанкционированное уничтожение, блокирование модификация, копирование информации – любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.

Обман (отрицание подлинности, навязывание ложной информации) – умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Носителями угроз безопасности информации являются источники (уязвимости) угроз. Все источники угроз безопасности информации можно разделить на три основные группы обусловленные: а) действиями субъекта (антропогенные источники угроз); б) техническими средствами (техногенные источники угрозы); в) стихийными источниками (рис. 1.3.) [8].

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

– криминальные структуры;

– потенциальные преступники и хакеры;

– недобросовестные партнеры;

– технический персонал поставщиков телематических услуг;

– представители надзорных организаций и аварийных служб;

– представители силовых структур.

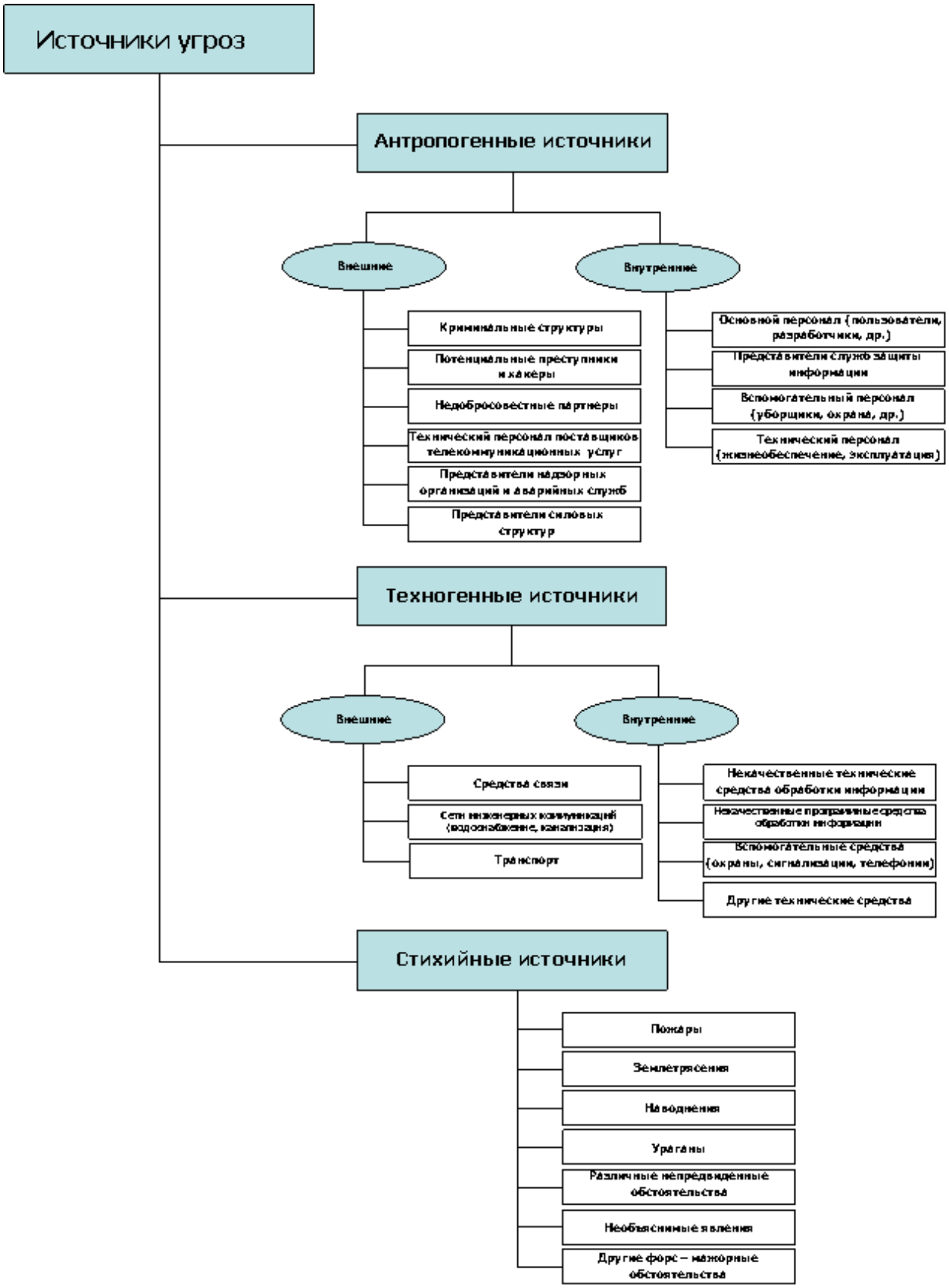

Рис. 1.3 – Классификация источников угроз

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

– основной персонал (пользователи, программисты, разработчики);

– представители службы защиты информации;

– вспомогательный персонал (уборщики, охрана);

– технический персонал (жизнеобеспечение, эксплуатация).

Менее прогнозируемыми, требующими особого внимания являются техногенные источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Эти угрозы напрямую зависят от свойств используемой техники. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Технические средства, являющиеся источниками потенциальных угроз безопасности информации также могут быть внешними:

– средства связи,

– сети инженерных коммуникации (водоснабжения, канализации),

– транспорт,

и внутренними:

– некачественные технические средства обработки информации;

– некачественные программные средства обработки информации;

– вспомогательные средства (охраны, сигнализации, телефонии);

– другие технические средства, применяемые в профессиональной образовательной организации.

Стихийными источниками потенциальных угроз информационной безопасности, как правило, являются внешними по отношению к защищаемому объекту и понимаются под ними, прежде всего, природные катаклизмы: пожары, землетрясения, наводнения, ураганы, различные непредвиденные обстоятельства, необъяснимые явления, другие форс-мажорные обстоятельства.

Среди угроз, направленных на нарушение безопасности информации, можно также выделить: угрозы, которые связаны непосредственно с аппаратной частью информационной системы;

– угрозы, которые связаны с коммуникациями информационной системы;

– угрозы, характерные для организаций профессионального образования. Наглядная схема классификации вышеперечисленных угроз более подробно представлена на рис. 1.4.

Способы воздействия угроз информационной безопасности на объект делятся на информационные, программно-математические, физические, радиоэлектронные, организационно-правовые. Конкретные методы воздействия угроз информационной безопасности на объект представлены на схеме рис. 1.5 [17].

1.2.2. Классификация уязвимостей безопасности

Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости (факторы), приводящие к нарушению безопасности инфор-

мации на конкретном объекте информатизации.

Рис. 1.4 – Классификация угроз информационной безопасности в информационных системах [27]

Рис. 1.3 – Способы воздействия угроз информационной безопасности на объект

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации. Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть объективными, субъективными и случайными.

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации. К ним относятся электромагнитные излучения (элементов технических средств, кабельных линий технических средств, излучения на частотах работы генераторов, на частотах самовозбуждения усилителей, цепей электропитания и заземления и др.), звуковые сигналы, активизируемые аппаратные закладки (устанавливаемые в телефонные линии, в сети электропитания, в технических средствах),

программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии программного обеспечения ИС), обладающие электроакустическими преобразованиями элементы (телефонные аппараты, громкоговорители и микрофоны и пр.), подверженные воздействию электромагнитного поля элементы, (магнитные носители, микросхемы, нелинейные элементы, поверженные ВЧ навязыванию), особенности местоположения защищаемого объекта и организации каналов обмена информацией (использование радиоканалов, глобальных информационных сетей, арендуемых каналов).

Субъективные уязвимости зависят от действий сотрудников профессиональной образовательной организации, которые, в основном, устраняются организационными и программно-аппаратными методами. Это: а) ошибки пользователей ИС профессиональной образовательной организации при подготовке и использовании программного обеспечения ИС (при разработке программного обеспечения и его инсталляции), при управлении сложными системами (с использованием возможностей самообучения систем, настройке сервисов систем, организации управления потоками обмена информации), при эксплуатации технических средств (вкл/выкл. технических средств, использовании технических средств охраны, средств обмена информацией); б) нарушения режима охраны и защиты (доступа на объект, к техническим средствам), режима эксплуатации технических средств, режима использования информации (обработки и обмена информацией, хранения и уничтожения носителей информации, уничтожения производственных отходов и брака), режима конфиденциальности (сотрудниками в нерабочее время, уволенными сотрудниками).

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы,

как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности, а именно: а) сбои и отказы технических средств, обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа; б) старение и размагничивание носителей информации (дискет и съемных носителей, жестких дисков, элементов микросхем, кабелей и соединительных линий); в) сбои программного обеспечения (ОС и СУБД, прикладных, сервисных и антивирусных программ); г) сбои электроснабжения (оборудования, обрабатывающего информацию, обеспечивающего и вспомогательного оборудования); д) неисправности и повреждения жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации, кондиционирования и вентиляции) и др.

1.3. Оценка угроз информационно-безопасной сохранности контента учебных достижений обучающихся профессиональных организаций

Процесс оценки угроз конфиденциальности, целостности и доступности ИС профессиональной образовательной организации и рисков можно подразделить на девять основных этапов [11]: определение характеристик ИС; идентификация уязвимостей; идентификация угроз; анализ регуляторов безопасности; определение вероятностей; анализ воздействий; определение рисков; рекомендуемые контрмеры; результирующая документация.

Идентификация уязвимостей и угроз, а также анализ регуляторов безопасности и воздействий могут выполняться относительно независимо и параллельно после того, как завершен первый этап и определены характеристики ИС. На рис. 1.4 показаны основные этапы процесса оценки рисков вместе с входной и выходной информацией для каждого из них.

Рисунок 1.4 – Основные этапы процесса оценки угроз и рисков, их входная и выходная информация

Все источники угроз конфиденциальности, целостности и доступности ИС профессиональной образовательной организации имеют разную степень опасности $(Коп)_i$, которую можно количественно оценить, проведя их ранжирование. При выборе метода ранжирования источников угроз целесообразно использование методология, изложенной в международных стандартах [5; 10], а также практического опыта российских экспертов в области информационной безопасности.

Перед ранжированием источников угроз, как правило, проводится ранжирование уязвимостей, имеющих разную степень опасности $(К_{ОП})_i$, которую можно оценить количественно. При этом в качестве критериев сравнения служат показатели: а) фатальности $(К_f)_i$, свидетельствующего о степени угрозы (для объективных уязвимостей таким показателем является информативность – способность уязвимости полностью (без искажений) передать информационный сигнал);

б) доступности $(К_Д)_i$, определяющего удобство (возможность) использования уязвимости источником угроз (массогабаритные размеры, сложность, стоимость необходимых средств, возможность использования не специализированной аппаратуры); количество $(К_К)_i$ элементов объекта, для которого характерна та или иная уязвимость. Итоговая степень опасности $(К_{оп})_i$ для отдельной *i*-той уязвимости определяется как отношение произведения вышеперечисленных показателей к максимальному значению (125):

$$(К_{ОП})_i = ((К_f)_i \cdot (К_Д)_i \cdot (К_К)_i) / 125.$$

Каждый показатель оценивается экспертно-аналитическим методом по пятибалльной системе. Причем, 1 соответствует самой минимальной степени влияния оцениваемого показателя на опасность использования уязвимости, а 5 – максимальной. Итоговая степень опасности для подгруппы уязвимостей $(К_{ОП})^{пг}$ определяется как среднее арифметическое коэффициентов

отдельных уязвимостей в подгруппе. Для удобства анализа итоговой степени опасности $(К_{ОП})^{г}$ для группы уязвимостей осуществляется нормирование относительно совокупности всех коэффициентов подгрупп, а итоговая степень опасности $(К_{ОП})^{к}$ для класса уязвимостей определяется как совокупность коэффициентов подгрупп класса нормированных относительно всей совокупности коэффициентов подгрупп. Результаты анализа с указанием коэффициентов опасности каждой уязвимости, сводятся в таблицу.

Оценка степени опасности угроз безопасности ИС образовательной организации проводится по косвенным показателям аналогично степени опасности уязвимостей. В качестве критериев сравнения могут быть использованы такие показатели как: а) возможность возникновения источника угроз, позволяющая определять степень доступности к защищаемому объекту (для антропогенных источников), удаленность от защищаемого объекта (для техногенных источников) или особенности обстановки (для случайных источников); б) готовность источника угроз, как степень квалификации и привлекательности совершения деяний со стороны источника угрозы (для антропогенных источников) или наличие необходимых условий (для техногенных и стихийных источников); в) фатальность угроз, определяющая степень неустранимости последствий реализации угрозы. Каждый показатель оценивается экспертно-аналитическим методом по 5-ти балльной системе. Причем, 1 соответствует самой min. степени влияния оцениваемого показателя на опасность использования источника, а 5 – max.

Степень доступности к защищаемому объекту (для антропогенных источников) при выявлении возможности возникновения источника угроз в процессе реализации подготовительного этапа оценки степени опасности угроз безопасности ИС профессиональной образовательной организации, позволяющая определять степень доступности к защищаемому объекту мо-

жет быть классифицирована по следующей шкале:

– высокая степень доступности – антропогенный источник угроз имеет полный доступ к техническим и программным средствам обработки защищаемой информации (характерно для внутренних антропогенных источников, наделенных максимальными правами доступа, например, представители служб безопасности информации, администраторы);

– первая средняя степень доступности – антропогенный источник угроз имеет возможность опосредованного, не определенного функциональными обязанностями, (за счет побочных каналов утечки информации, использования возможности доступа к привилегированным рабочим местам) доступа к техническим и программным средствам обработки защищаемой информации (характерно для внутренних антропогенных источников);

– вторая средняя степень доступности – антропогенный источник угроз с ограниченной возможностью доступа к программным средствам в силу введенных ограничений в использовании технических средств, функциональных обязанностей или по роду своей деятельности (характерно для внутренних антропогенных источников с обычными правами доступа, например, пользователи, или внешних антропогенных источников, имеющих право доступа к средствам обработки и передачи защищаемой информации, например, хакеры, технический персонал поставщиков телематических услуг);

– низкая степень доступности – антропогенный источник угроз имеет очень ограниченную возможность доступа к техническим средствам и программам, обрабатывающим защищаемую информацию (характерно для внешних антропогенных источников);

– отсутствие доступности – антропогенный источник угроз не имеет доступа к техническим средствам и программам, обрабатывающих защищаемую информацию.

Степень удаленности от защищаемого объекта (для техногенных источников) или особенности обстановки (для случайных источников) при выявлении возможности возникновения источника угроз в процессе подготовительного этапа оценки степени опасности угроз безопасности ИС образовательной организации, позволяющая определять степень доступности к защищаемому объекту можно характеризовать следующими параметрами:

– совпадающие объекты – объекты защиты сами содержат источники техногенных угроз и их территориальное разделение невозможно;

– близко расположенные объекты – объекты защиты в непосредственной близости от источников техногенных угроз и любое проявление таких угроз может оказать существенное влияние на защищаемый объект;

– удаленно расположенные объекты – объект защиты располагается на удалении от источника техногенных угроз, исключающем возможность его прямого воздействия.

– сильно удаленные объекты – объект защиты располагается на значительном удалении от источников техногенных угроз, полностью исключающем любые воздействия на защищаемый объект, в том числе и по вторичным проявлениям.

Особенности обстановки, характеризуются расположением объектов защиты в различных природных, климатических, сейсмологических, гидрологических и других условиях можно оценить по следующей шкале:

– очень опасные условия – объект защиты расположен в зоне действия природных катаклизмов;

– опасные условия – объект защиты расположен в зоне, где многолетние наблюдения выявляют возможность проявления природных катаклизмов;

– умеренно опасные условия – объект защиты расположен в зоне в которой по проводимым наблюдениям на протяжении долгого периода отсутст-

вуют проявления природных катаклизмов, но имеются предпосылки возникновения стихийных источников угроз на самом объекте;

– слабо опасные условия – объект защиты находится вне пределов зоны действия природных катаклизмов, однако на объекте имеются предпосылки возникновения стихийных источников угроз;

– неопасные условия – объект защиты находится вне пределов зоны действия природных катаклизмов и на объекте отсутствуют предпосылки возникновения стихийных источников угроз.

Квалификация антропогенных источников играет важную роль в определении их возможностей по совершению противоправных деяний. Принята следующая классификация уровня квалификации по возможности (уровню) взаимодействия с защищаемой сетью [6]:

– нулевой уровень – определяется отсутствием возможности какого-либо использования программ;

– первый уровень – ограничивается возможностью запуска задач/программ из фиксированного набора, предназначенного для обработки защищаемой информации (уровень неквалифицированного пользователя);

– второй уровень – учитывает возможность создания и запуска пользователем собственных программ с новыми функциями по обработке информации (уровень квалифицированного пользователя, программиста);

– третий уровень – определяется возможностью управления функционированием сетью, то есть воздействием на базовое программное обеспечение, ее состав и конфигурацию (уровень системного администратора);

– четвертый уровень – определяется всех возможностей субъектов, осуществляющих проектирование и ремонт технических средств, вплоть до включения в состав сети собственных технических средств с новыми функциями по обработке информации (уровень разработчика и администратора).

Нулевой уровень является самым низким уровнем возможностей по ведению диалога источника угроз с защищаемой сетью. При оценке возможностей антропогенных источников предполагается, что субъект, совершающий противоправные действия, либо обладает, либо может воспользоваться правами соответствующего уровня.

Привлекательность совершения деяния со стороны источника угроз устанавливается следующим образом:

– особо привлекательный уровень – защищаемые информационные ресурсы содержат информацию, которая может нанести непоправимый урон и

– привлекательный уровень – защищаемые информационные ресурсы содержат информацию, которая может быть использована для получения выгоды в пользу источника угрозы или третьих лиц;

– умеренно привлекательный уровень – защищаемые информационные ресурсы, содержат информацию, разглашение которой может нанести ущерб отдельным личностям;

– слабо привлекательный уровень – защищаемые информационные ресурсы содержат информацию, которая при ее накоплении и обобщении в течение определенного периода может причинить ущерб организации, осуществляющей защиту;

– не привлекательный уровень – информация не представляет интерес для источника угрозы.

Необходимые условия готовности источника определяются исходя из возможности реализации той или иной угрозы в конкретных условиях расположения объекта. При этом предполагается, что угроза:

– реализуема – условия благоприятны/могу быть благоприятны для реализации угрозы (например, активизация сейсмической активности);

– реализуема – условия благоприятны для реализации угрозы, но долгосрочные наблюдения не выявляют возможности ее активизации в период существования и активной деятельности объекта защиты;

– слабо реализуема – существуют объективные причины на самом объекте или в его окружении, препятствующие реализации угрозы;

– не реализуема, т.к. – отсутствуют предпосылки для реализации предполагаемого события.

Степень неустранимости последствий проявления угрозы (фатальность) определяется по следующей шкале:

– неустранимые последствия – результаты проявления угрозы могут привести к полному разрушению (уничтожению, потере) объекта защиты, как следствие к невосполнимым потерям и исключению возможности доступа к защищаемым информационным ресурсам;

– практически неустранимые последствия – результаты проявления угрозы могут привести к разрушению (уничтожению, потере) объекта и к значительным затратам (материальным, временным и пр.) на восстановление последствий, сопоставимых с затратами на создание нового объекта и существенному ограничению времени доступа к защищаемым ресурсам;

– частично устранимые последствия – результаты проявления угрозы могут привести к частичному разрушению объекта защиты и, как следствие, к значительным затратам на восстановление, ограничению времени доступа к защищаемым ресурсам;

– устранимые последствия – результаты проявления угрозы могут привести к частичному разрушению (потере) объекта защиты, не требующих больших затрат на его восстановление и, практически не влияющих на ограничение времени доступа к защищаемым информационным ресурсам;

– отсутствие последствий – результаты проявления угрозы не могут повлиять на деятельность объекта защиты.

Результаты ранжирования относительно конкретного объекта защиты сводятся в таблицу, позволяющую определить наиболее опасные для данного объекта источники угроз безопасности информации.

При выборе допустимого уровня источника угроз предполагается, что источники угроз, имеющие значение коэффициента $(К_{оп})_i$ менее (0,1–0,2) могут в дальнейшем не учитываться, как маловероятные.

Определение актуальных (наиболее опасных) угроз осуществляется на основе анализа расположения объектов защиты и структуры построения ИС, а также информационных ресурсов, подлежащих защите (рис. 1.6) [8].

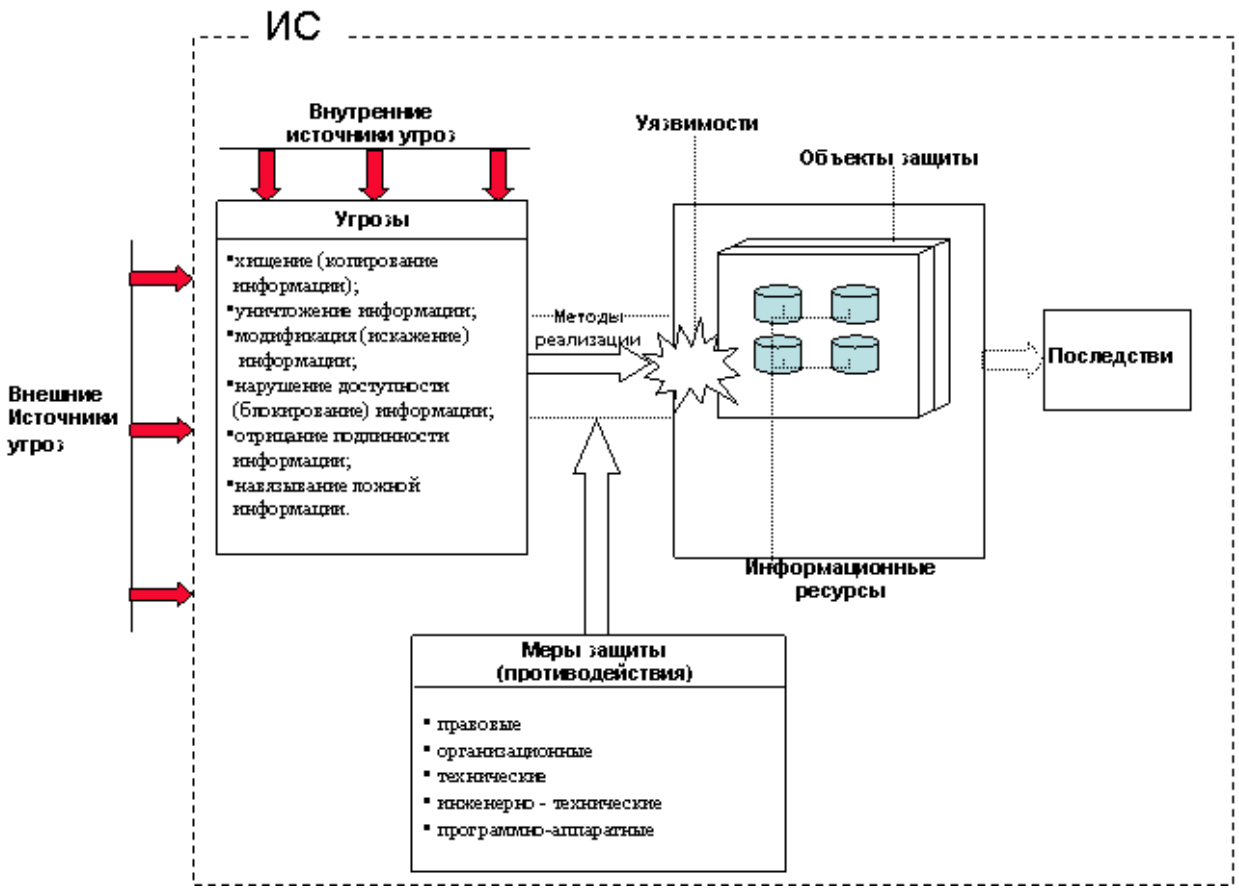

Рис. 1.6 – Модель реализации угроз информационной безопасности ИС

1.4. Модели, методики анализа и цифровая оценка угроз информационной безопасности контента профессиональных образовательных организаций

Исходные данные для цифровой оценки с анализом угроз информационной безопасности ИС по алгоритму анализа и цифровой оценки угроз информационной безопасности профессиональных образовательных организаций (рис. 1.7) позволяет установить приоритеты целей безопасности; определить актуальные источники угроз и уязвимостей с оценкой их взаимосвязей; определить перечень возможных атак и описать возможные последствия реализации угроз.

В литературе, посвященной вопросам защиты информации можно найти различные варианты моделей и методик анализа и оценки угроз безопасности ИС. Это объясняется стремлением более точно и эффективно описать многообразные ситуации воздействия на информацию и определить наиболее адекватные меры парирования.

В принципе, можно пользоваться любой понравившейся моделью, необходимо только убедиться, что она описывает максимально большое число факторов, влияющих на безопасность ИС профессиональной образовательной организации. Но прежде всего следует помнить, что пользователю, то есть потребителю информации и информационных услуг, оказываемых корпоративной сетью, глубоко без разницы не получит он информацию вовремя, получит ее в искаженном виде или вообще потеряет по вине неправильной работы технических средств, пожара в серверном зале или за счет действий злоумышленника. Итог для него во всех случаях одинаков – понесенные убытки (моральные или материальные).

Для обеспечения эффективности комплексной безопасности ИС необходимо принятие как организационных, так и технических решений парирования. Такой подход позволяет дифференцировано подойти к

распределению материальных ресурсов, выделенных на обеспечение информационной безопасности.

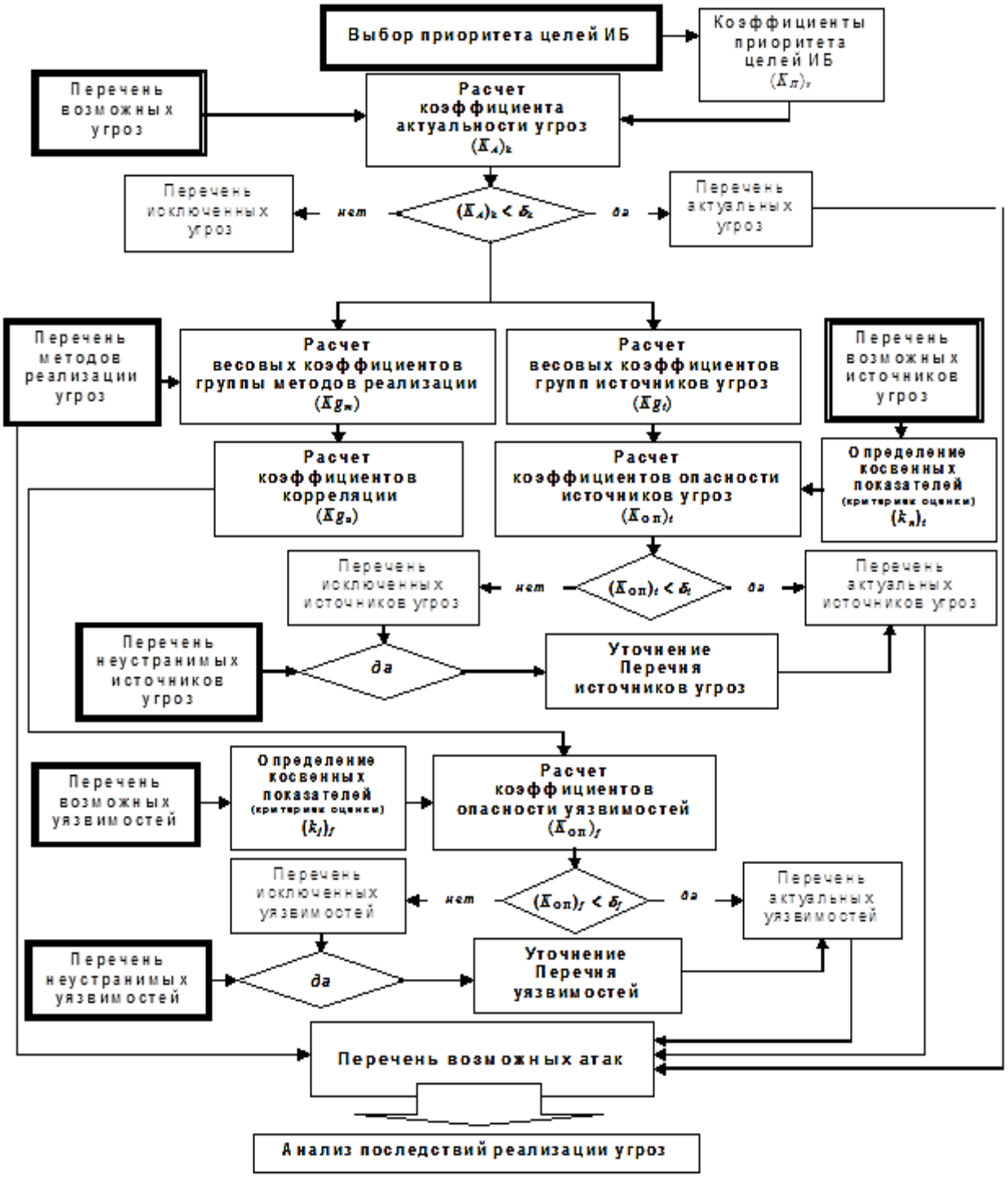

Рис. 1.7 – Алгоритм анализа и цифровой оценки угроз информационной безопасности профессиональных образовательных организаций

Важно принимать во внимание и учитывать, что цифровая оценка весовых коэффициентов каждой угрозы достаточно затруднительная процедура из-за высокой латентности их проявлений и отсутствия вразумительной статистики по этому вопросу. Поэтому в современной литературе можно найти различные шкалы оценок. Вместе с тем, на основе анализа, проводимого различными специалистами в области компьютерных преступлений и собственных наблюдений, по частоте проявления угрозы безопасности можно расставить так:

1. кража (копирование) программного обеспечения;
2. подмена (несанкционированный ввод) информации;
3. уничтожение (разрушение) данных на носителях информации;
4. нарушение нормальной работы (прерывание) в результате вирусных атак;
5. модификация (изменение) данных на носителях информации;
6. перехват (несанкционированный съем) информации;
7. кража (несанкционированное копирование) ресурсов;
8. нарушение нормальной работы (перегрузка) каналов связи;
9. непредсказуемые потери.

Современные образовательные организации широко используют в своей деятельности информационные технологии. К сожалению, информационные системы, используемые в профессиональных образовательных организациях в большинстве своем, не отвечают даже минимальным требованиям, предъявляемым к безопасным ИС. Подавляющее большинство ИС профессиональных образовательных организаций не проходят какой-либо сертификации, стандартизации, создаются буквально «на коленке» низкоквалифицированными разработчиками, очень часто на основе устарев-

ших решений. Перечисляя проблемы, характерные для таких ИС, можно отметить следующие недочеты [19]:

– Использование разнородных, устаревших и заведомо небезопасных платформ. Уязвимости в информационных системах, базах данных и других информационных средствах выявляются регулярно, и любая устаревшая платформа должна считаться заведомо небезопасной, если не проведены работы по устранению этих проблем. Во многих случаях информационные системы не связаны между собой, используют разные платформы, что резко осложняет их использование и поддержку.

– Отсутствие стандартизации. Несмотря на предпринятые попытки разработать унифицированные информационно-технические решения, большинство образовательных организаций используют те решения, которые оказались под рукой.

– Использование публичного открытого соединения. Любая ИС, претендующая на безопасность, должна организовывать передачу данных с использованием зашифрованных соединений по умолчанию во избежание перехвата данных.

– Отсутствие практики регулярного аудита безопасности. Без постоянной проверки и выявления потенциальных проблем даже качественно спроектированные информационные системы могут стать небезопасными при обнаружении новых видов уязвимостей.

– Низкая квалификация персонала пользователей ИС и специалистов по качественной поддержке ИС в эффективно работоспособном состоянии. Качественная поддержка ИС требует регулярного мониторинга их работы и превентивного устранения неполадок.

– Использование пиратского программного обеспечения. Многие образцы «взломанных» программ могут содержать в себе троянский код,

упрощающий внедрение в ИС. Кроме того, пиратское программное обеспечение часто исключает возможность его обновления, что не позволяет противостоять вновь возникающим угрозам.

– Недофинансирование. Эта проблема является корнем всех вышеперечисленных.

К решению всех описанных проблем можно подходить на различных уровнях, с привлечением различных методик анализа и оценки угроз безопасности ИС.

Выводы по главе 1.

Для повышения уровня эффективного безопасности информационной системы профессиональной образовательной организации желательно следовать следующей цепочке мероприятий: источник угрозы – уязвимость (фактор) – угроза (действие) – последствия (атака, выбор и разработка мер защиты аппаратного и используемого программного обеспечения, совершенствование политики информационной безопасности профессиональной образовательной организации).

С точки зрения базовых угроз информационной безопасности профессиональной образовательной организации существует два алгоритма расчета уровня угроз одной базовой угрозы (суммарной) или трех базовых угроз (конфиденциальности, целостности и доступности ИС профессиональной образовательной организации), по их уязвимости на основе критичности и вероятности реализации каждой конкретной угрозы.

Требующими особого внимания являются техногенные источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Эти угрозы напрямую зависят от свойств используемой техники. Данный класс источников угроз безопасности информации особенно

актуален в современных условиях, т.к в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости (факторы), приводящие к нарушению безопасности информации на конкретном объекте информатизации.

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред. Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации. Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть объективными, субъективными и случайными.

Процесс оценки угроз конфиденциальности, целостности и доступности ИС профессиональной образовательной организации и рисков можно

подразделить на девять основных этапов: определение характеристик ИС; идентификация уязвимостей; идентификация угроз; анализ регуляторов безопасности; определение вероятностей; анализ воздействий; определение рисков; рекомендуемые контрмеры; результирующая документация.

Оценка степени опасности угроз безопасности ИС профессиональной образовательной организации проводится по косвенным показателям. При этом в качестве критериев сравнения могут быть использованы следующие показатели: а) возможность возникновения источника угроз, позволяющая определять степень доступности к защищаемому объекту (для антропогенных источников), удаленность от защищаемого объекта (для техногенных источников) или особенности обстановки (для случайных источников); б) готовность источника угроз, как степень квалификации и привлекательности совершения деяний со стороны источника угрозы (для антропогенных источников) или наличие необходимых условий (для техногенных и стихийных источников); в) фатальность угроз, определяющая степень неустранимости последствий реализации угрозы. Каждый показатель оценивается экспертно-аналитическим методом по пятибалльной системе.

Результаты ранжирования относительно конкретного объекта защиты сводятся в таблицу, позволяющую определить наиболее опасные для данного объекта источники угроз безопасности информации.

Современные образовательные организации широко используют в своей деятельности информационные технологии. К сожалению, информационные системы, используемые в профессиональных образовательных организациях в большинстве своем, не отвечают даже минимальным требованиям, предъявляемым к безопасным ИС.

2. РАЗРАБОТКА МЕТОДИКИ АНАЛИЗА И ЦИФРОВОЙ ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЙ ПРОФЕССИОНАЛЬНЫХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИИ

2.1. Цифровая оценка угроз информационной безопасности профессиональных образовательных организаций

Обеспечение повышения эффективности профессиональных образовательных организаций базируется, в первую очередь, на превентивном выявлении возможных угроз и выделении из них наиболее потенциально опасных, что является одним из сложных и трудоемких процессов разработки концепции системы информационной безопасности (СИБ) профессиональной образовательной организации [12–13].

Основываясь на анализе угроз безопасности ИС, проведенном в работах [14–15], рассмотрим основы методики оценки данных угроз. В качестве базовых используем следующие показатели, обозначения и шкалы:

А – нарушаемые принципы безопасности:

1 – нарушение конфиденциальности личной, служебной и другой доверительной информации;

2 – нарушение целостности и достоверности хранимых данных с помощью специальных программ;

3 – нарушение доступности системы, данных и услуг всем уполномоченным пользователям;

4 – несоблюдение законов, правил, лицензий, договоров и этических норм при использовании информации.

Б – возможность предотвращения конкретных угроз для конкретной ИС в реальных условиях:

1 – легко; 2 – трудно; 3 – очень трудно; 4 – невозможно.

В – выявление (обнаружение) угрозы, оцениваемая автоматически или вручную:

1 – легко; 2 – трудно; 3 – невозможно.

Г – возможность нейтрализации/восстановления контента. Оцениваются усилия необходимые для нейтрализации угрозы (для принципов безопасности А1 и А4) или восстановления нормальной работы (для принципов безопасности А2 и А3):

1 – легко; 2 – трудно; 3 – очень трудно; 4 – невозможно.

Д – частота появления. Данная оценка отражает сравнительную характеристику частоты появления конкретной угрозы в сравнении с другими угрозами:

0 – неизвестна; 1 – низкая; 2 – средняя; 3 – высокая; 4 – сверх высокая.

Е – потенциальная опасность – оценивается опасность угрозы с точки зрения ущерба, который может понести АИС в случае реализации угрозы:

1 -– низкая; 2 – высокая; 3 – сверх высокая.

Ж – источник появления:

1 – внутренний; 2 – внешний.

З – уровень необходимых знаний - оценивается уровень профессиональной подготовки нарушителей для подготовки и реализации соответствующей угрозы:

1 – фундаментальные знания системной организации ресурсов, протоколов связи и др.; 2 – знание операционной системы; 3 – знание языков программирования; 4 – элементарные знания в области вычислительной техники.

И – затраты на проектирование и разработку злоупотребления:

1 – большие; 2 – средние; 3 – незначительные затраты.

К – простота реализации:

1 – очень трудно; 2 – трудно; 3 – относительно нетрудно; 4 – легко;

Л – потенциальное наказание в рамках существующего законодательства. Следует отметить, что здесь необходимо рассматривать такие аспекты,

как дисциплинарные взыскания, гражданская и уголовная ответственность. При оценке угроз по данному критерию следует принимать во внимание факт возможности доказательства авторства программного злоупотребления и наличие юридической ответственности за соответствующие нарушения:
1 – строгое наказание (вплоть до уголовной ответственности); 2 – незначительное наказание; 3 – наказание отсутствует.

Оперативную оценку критических угроз, активов и уязвимостей позволяет, например, проводить разработанный в университете Карнеги-Мелон (США) метод OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), подразумевающий создание состоящей из экспертов группы анализа (ГА), которая изучает информационную безопасность ИС и ведёт построение профиля угроз для каждого критического ресурса [20].

Получение полной и объективной информации для принятия обоснованных мер по повышению информационной безопасности ИС профессиональной образовательной организации в значительной мере зависит от корректности экспертных оценок уровня трудности тестовых заданий, их объективированности.

В состав экспертной группы для определения угроз безопасности ИС рекомендуется включать экспертов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций):

– от подразделений обладателей информации, содержащейся в ИС;

– от подразделений оператора информационной системы;

– от подразделения по защите информации;

– от лиц, предоставляющих услуги по обработке информации;

– от разработчика информационной системы;

– от операторов взаимодействующих внешних ИС (по согласованию).

В качестве экспертов следует привлекать специалистов, деятельность которых связана с обработкой информации в ИС, и специалистов, имеющих квалификацию и опыт работы в области применения информационных технологий и/или в области защиты информации. Эксперты ГА безопасности ИС должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения.

Не рекомендуется формировать экспертную группу из участников, находящихся в прямом подчинении. Следует учитывать, что существуют субъективные факторы, связанные с психологией принятия решений человеком. Это также может приводить как к занижению (ослаблению), так и к завышению (усилению) экспертами прогнозов и предположений при определении угроз безопасности ИС, что в свою очередь может привести к пропуску отдельных угроз безопасности ИС или к неоправданным затратам на нейтрализацию неактуальных угроз.

Оценку параметров безопасности ИС рекомендуется проводить опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений («низкий», «средний», «высокий» или «да», «нет» или иные шкалы). При этом вопросы должны быть четкими и однозначно трактуемыми, предполагать однозначные ответы.

Возможность использования метода экспертных оценок, обоснование их объективности обычно базируется на предположении о том, что неизвестная характеристика исследуемого явления есть случайная величина, отражением закона распределения которой служит индивидуальная оценка эксперта – специалиста о достоверности и значимости того или иного события [21]. При этом истинное значение характеристики находится внутри диапа-

зона оценок, получаемых от группы экспертов – специалистов.

При использовании экспертных оценок обычно предполагается, что мнение группы экспертов надёжнее, достовернее, чем мнение отдельного эксперта. Опрашиваемой группе экспертов предлагается проранжировать предварительно отобранные факторы по степени их влияния на отклик, результативный признак, по уровням трудности и, соответственно, иерархии оценочных баллов, причём предварительный отбор важных фактор может быть осуществлён на первом этапе экспертных оценок [22] оцениваемому фактору экспертами ставится в соответствие весовой коэффициент (ранговый балл, процентное отношение или другой числовой показатель) пропорционально тем или иным соображениям, интуиции, опыту и т.д. В итоге, составляется матрица рангов (таблица 2.1).

Таблица 2.1

Матрица рангов

Фактор	Ранг, назначенный экспертом*)								Сумма рангов для x_i
	1-м	2-м	3-м	4-м	5-м	6-м	7-м	8-м	
x_1	2	1	1	1	3	4	1	2	15
x_2	1	2	2	6	1	3	4	1	20
x_3	3	3	4	3	2	2	3	3	23
x_4	4	5	3	2	5	1	5	4	29
x_5	5	4	5	4	4	6	2	5	35
x_6	6	6	6	5	6	5	6	6	46
Итого	21	21	21	21	21	21	21	21	168

*) Фактор, который, с точки зрения экспертов, оказывает на изучаемый показатель наибольшее влияние, имеет наименьшую сумму рангов, а фактор, оказывающий самое слабое влияние, – наибольшую сумму рангов.

Применение весовых коэффициентов для каждого из оцениваемых факторов при использовании метода расстановки приоритетов в соответствии с необходимыми требованиями [22] значительно снижает разброс суммарных оценок экспертов. Этим достигаются более высокая точность и дос-

товерность итоговой оценки, как средневзвешенного результата суммарных оценок экспертов, которые, в свою очередь, являются итогом сложения единичных оценок по отдельным показателям.

В любом случае эксперт используется как своеобразный «измерительный инструмент». Результаты экспертных оценок, как показывает практика последних десятилетий, могут быть существенно улучшены, т.е. достигнуты быстрее, более полно, единообразно, содержать меньше противоречий и т.д. с применением математической статистики [23] и системного подхода, реализующего, по определению В.М. Глушкова [24] совокупность приёмов и методов анализа для изучения сложных объектов.

По мнению Ю.И. Черняка «Системный анализ применяется для того, чтобы поначалу хотя бы слабо структуризовать неструктуризованную, смутно определённую проблему, а затем собрать новую дополнительную информацию о ней, установить взаимосвязи составляющих, дать, где это только возможно, количественные оценки (хотя бы субъективные, экспертные) и перевести проблему в разряд структуризованных, к решению которых уже можно приложить аппарат математического моделирования и выбора оптимальных решений» [25]. Само дробление при таком подходе является, в свою очередь, своеобразным гарантом страховки экспертов от необоснованно завышенного или заниженного итогового результата количественной оценки значимости факторов безопасности ИС.

Результаты субъективной оценки в значительной мере зависят от опытности и подготовленности эксперта, который каждую единичную оценку строит не на пустом месте, а как логический вывод, основанный на личном опыте и специальных знаниях [22].

В таблице 2.2 приведены выстроенные в порядке убывания уровня подвергнутых экспертной оценке угроз средние значения оценки

общесистемных угроз безопасности ИС профессиональной образовательной организации, составленные по результатам анкетирования команды экспертов, предварительно протестированных на предмет отсутствия неадекватных решений вне доверительного диапазона.

Комплексная оценка угрозы может быть рассчитана следующим образом:

$$K_i^2 = \frac{\sum_{j=1}^{m} \frac{K_{ij} + K_{j\max}}{2}}{m},$$

где K_{ij} – оценка i-й угрозы по j-му параметру;

m – количество параметров оценки;

$K_{j\,max}$ – максимальная оценка по j-му параметру.

Таблица 2.2

Оценки общесистемных угроз безопасности ИС

	Угрозы безопасности	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	Комплексная оценка
Общесистемные угрозы													
1	Ошибки пользователя	2	3.0	2.5	3.5	2.0	2.5	1.0	4.0	3.0	2.5	1.5	2.98
2	Отказ в обслуживании	3	3.0	1.5	2.5	3.0	2.0	1.5	3.5	2.5	3.0	2.5	2.95
3	Недоступность информации	2	2.5	1.0	3.0	1.5	2.5	1.0	3.5	2.5	2.5	2.5	2.83
4	Ошибки программного обеспечения	2	3.5	2.5	3.0	2.0	2.0	1.0	0.0	3.0	2.5	1.5	2.75
5	Неправильная маршрутизация	2	2.0	1.5	4.0	2.0	2.0	2.0	1.0	1.5	1.5	1.5	2.65
6	Аппаратные сбои	2	4.0	1.5	1.5	2.5	1.5	1.0	0.0	3.0	1.5	2.5	2.65
7	Перегрузка трафика	3	1.5	1.0	1.5	1.0	1.5	1.5	1.0	2.5	1.5	2.5	2.48
	Среднее значение угрозы	2.3	2.8	1.6	2.7	2.0	2.0	1.3	1.9	2.6	2.1	2.1	2.76

Примечание. Максимальные оценки для графы ***А*** - 4; для графы ***Б*** - 4; для графы ***В*** - 3; для графы ***Г*** - 4; для графы ***Д*** - 4; для графы ***Е*** - 3; для графы ***Ж*** - 2; для графы ***З*** - 4; для графы ***И*** - 3; для графы ***К*** - 4; для графы ***Л*** - 3.

Среднее значение комплексной оценки величиной 2.76 общесистемных угроз безопасности ИС профессиональной образовательной органи-

зации располагается на повышенном уровне трудностей их преодоления, нейтрализации и устранения. Наибольшую угрозу с величиной, равной 2.98, составляют ошибки пользователей, что свидетельствует, с одной стороны, о недостаточно высокой их квалификации и необходимости проведения дополнительных курсов повышения уровня правильного владения ими приемами работы на персональном компьютере, а, с другой стороны, о наличии среди штатных пользователей ИС профессиональной образовательной организации представителей, имеющих заинтересованность в корректировке контента учебных достижений обучающихся профессиональной организации.

Несколько незначительно меньшее среднее значение комплексной оценки величиной 2.95 общесистемных угроз безопасности ИС профессиональной образовательной организации составляют отказы в обслуживании, что является, по-видимому, следствием:

– физического и морального износа используемого оборудования ИС;

– низкого качества (надежности) технических, программных или программно-технических средств;

– низкого качества (надежности) сетей связи и (или) услуг связи;

– отсутствия или низкой эффективности систем резервирования или дублирования программно-технических и технических средств;

– низкого качества(надежности) инженерных систем (кондиционирования, электроснабжения, охранных систем и т. д.);

– низкого качества обслуживания со стороны обслуживающих организаций и лиц;

– исчерпания вычислительных ресурсов, недоступности обновления программного обеспечения и т.д.

Заметим, что самыми частыми и самыми опасными (с точки зрения размера ущерба) являются как непреднамеренные, так и преднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих ИС. По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок. Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе. Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль [18].

Не в меньшей степени отмеченное касается программного обеспечения ИС профессиональной образовательной организации, о чем свидетельствуют значения комплексных оценок относительно угроз аппаратных сбоев, затруднений в части доступности информации и ошибок программного обеспечения по причине неправильной маршрутизации.

Среди общесистемных угроз безопасности ИС профессиональной образовательной организации наибольшее значение величиной 2.8 принадлежит очень трудной возможности предотвращения в реальных условиях угрозы для конкретной ИС. Следом за данной общесистемной угрозой безопасности ИС в порядке понижения их значений следуют также с очень трудной возможностью усилия по нейтрализации/восстановления (для принципов безопасности А1 и А4) или восстановления нормальной работы (для принципов безопасности А2 и А3) величиной 2,7 и невысокие затраты на проектирование и разработку злоупотребления величиной 2.6.

Наименьшие значения (величиной 1.3 и 1.6) принадлежит угрозам источников их появления и обнаружения угроз (в автоматическом или ручном режимах). По остальным угрозам наблюдается средний их уровень (1.5).

В таблице 2.3 приведены средние значения оценки других злоупотреблений безопасности ИС профессиональной образовательной организации,

составленные по результатам анкетирования команды экспертов, предварительно протестированных на предмет отсутствия неадекватных решений вне доверительного диапазона.

Таблица 2.3

Оценки других злоупотреблений безопасности ИС

	Угрозы безопасности	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	Комплексная оценка
Другие злоупотребления													
1	Злоупотребления информацией	1,5	2.5	1.5	2.5	1.5	2.5	1.5	4.0	2.5	3.5	2.5	2.93
2	Другие виды мошенничества	1,5	2.0	2.0	3.5	1.5	2.5	1.5	2.5	2.0	2.5	2.0	2.80
3	Сетевые анализаторы	1,0	4.0	2.5	2.5	1.5	1.5	2.0	1.5	1.5	2.0	2.5	2.78
4	Анализ трафика	1,0	3.0	2.5	2.5	1.5	1.5	2.0	1.5	1.5	1.5	2.5	2.73
5	Кража информации	2,0	2.0	2.5	3.5	1.5	2.0	1.5	2.5	2.0	1.5	1.0	2.70
6	Повреждение данных и программ	2,5	2.0	2.0	2.5	1.0	2.5	1.0	3.5	2.5	1.5	1.0	2.68
7	Повреждение аппаратных средств	1,5	3.5	1.5	2.5	1.5	2.0	1.5	1.0	2.0	1.0	1.0	2.53

Примечание. Максимальные оценки для графы ***А*** - 6; для графы ***Б*** - 3; для графы ***В*** – 3-5; для графы ***Г*** – 2 и 5; для графы ***Д*** – кроме 6 единодушное мнение экспертов; для графы ***Е*** – 1-2 и 6; для графы ***Ж*** - 3; для графы ***З*** - 1; для графы ***И*** – 1 и 6; для графы ***К*** - 1; для графы ***Л*** – 1 и 3-4.

Среди других злоупотреблений безопасности ИС профессиональной образовательной организации наибольшее значение величиной 4,0 принадлежит очень трудной возможности по усилиям нейтрализации/восстановления (для принципов безопасности Б3 и З1). Защититься от таких методов довольно трудно. В качестве активной защиты можно применять различные генераторы шума, а в качестве пассивной – экранирование деталей компьютера или помещения целиком [26–29].

Несколько в меньшей степени величиной 3.5, но также достаточно с высокоопасным уровнем негативного влияния, обнаруживаются угрозы

нарушение целостности и достоверности хранимых данных вследствие мошенничества и кражи информации, умышленного повреждения данных и программ ИС [27]. По остальным угрозам наблюдается средний их уровень величиной 1.5.

На основе анализа вышеприведенных результатов оценки группой экспертов критических угроз, активов и уязвимостей безопасности ИС профессиональной образовательной организации (таблицы 2.2–2.3) можно сделать предварительный вывод, что комплексные оценки угроз распределены в следующих интервалах:

– до 2.70 (включительно): Неправильная маршрутизация, аппаратные сбои, перегрузка трафика (для общесистемных угроз безопасности ИС профессиональной образовательной организации), программы захвата паролей, репликаторы, воздушные змеи, атаки салями (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и кража информации, умышленное повреждение данных и программ, повреждение аппаратных средств (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации);

– от 2.71 до 2.85 (включительно): Недоступность информации, ошибки программного обеспечения (для общесистемных угроз безопасности ИС профессиональной образовательной организации), программные закладки, скрытые каналы, компьютерные вирусы, работа между строк, подкладывание свиньи (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и сетевые анализаторы, анализ трафика и другие виды мошенничества (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации);

– и больше 2.85: Ошибки пользователя, отказ в обслуживании (для общесистемных угроз безопасности ИС профессиональной образовательной организации), маскарад, люки, программы открытия паролей, троянские кони, суперзаппинг, логические бомбы (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и перехват ПЭМИН, злоупотребления информацией, перехват информации (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации).

Исходя из вышеизложенного, все угрозы безопасности, злоупотребления и мошенничества целесообразно разделить на три основные группы:

– неопасные угрозы, которые легко предотвращаются или обнаруживаются, нейтрализуются и устраняются (комплексные оценки угроз до 2.70;

– опасные, для которых процессы предотвращения, обнаружения и нейтрализации, с точки зрения технологии, не отработаны (комплексные оценки угроз от 2.71 до 2.85 (включительно);

– очень опасные, которые обладают максимальными оценками по всем параметрам и реализация процессов противостояния сопряжены с огромными затратами (комплексные оценки угроз больше 2.85) .

Данное выделение может варьироваться и изменяться при изменении метода расчетов комплексной оценки. В то же время данный подход может быть полезным при оценке риска безопасности ИС профессиональной образовательной организации.

2.2. Алгоритм расчета значимости угроз информационно-безопасной сохранности контента учебных достижений обучающихся профессиональных организаций

Значимость события – это произведение вероятности P наступления события на потенциал угрозы источника этого события [30–32].

Значимость события A рассчитывается с учетом относительной значимости A^* события по формуле:

$$A = B \cdot N \cdot P, \quad (2.1)$$

$$A^* = A_i / (A_1 + A_2 + \ldots + A_n), \quad (2.2)$$

где B – вероятность наступления события, %;

N – количество всех угроз ИБ (без учета источника возникновения).

Для точных расчетов величины A значимости события угроза безопасности ИС профессиональной образовательной организации должна отвечать статистической вероятности из существующей выборки событий (из выборки совершившихся событий определяется относительная вероятность угрозы безопасности ИС профессиональной образовательной организации относительно других угроз). Так при принятии предположения, что угрозы «Сбои и отказы программно-аппаратных средств» возникают в 10 раз чаще, чем угрозы «Пожар», вероятность пожара будет около 0,5%, а вероятность угроз «Сбоя и отказы программно-аппаратных средств» будет 5%.

В первом предположении, без статистики, имея рассмотренные и сведенные в таблицы 2.2–2.3 угрозы безопасности ИС профессиональной образовательной организации, целесообразно считать их равновероятными, т.е.:

$$B_1 = B_2 = B_3 = \ldots = B_{14}, \quad (2.3)$$

где B – вероятность наступления события, %;

ij – количество всех угроз безопасности ИС профессиональной образовательной организации (без учета источника возникновения);

B_1 – сбои и отказы программно-аппаратных средств;

B_2 – угрозы со стороны обслуживающего персонала;

B_3 – ошибки руководства организации в связи с недостаточным уровнем осознания безопасности ИС профессиональной образовательной организации;

B_6 – утечка информации;

B_8 – нарушение функциональности и доступности персонала, и т.п. по таблицам 2.2–2.3.

Суммарную вероятность наступления всех угроз безопасности ИС профессиональной образовательной организации (без учета источника возникновения) принимаем за 100%, т.е. если возникнет угроза безопасности ИС профессиональной образовательной организации (без учета источника возникновения), то она будет одной из списка 14 угроз. По второму варианту берется общее число событий (нормальное функционирование и угрозы безопасности ИС профессиональной образовательной организации (без учета источника возникновения)) и угрозы безопасности ИС профессиональной образовательной организации (без учета источника возникновения) составляют от него какой-то процент и суммарная вероятность всех угроз тогда будет равна этому проценту:

$$B_l + B_2 + B_3 + \ldots + B_{14} = 1,$$

а

$$B_1 = B_2 = B_3 = \ldots = B_{14} = 1/14 = 0{,}0714 = 7{,}14\ \%$$

в первом предположении, без статистики, равновероятности всех 14 угроз безопасности ИС профессиональной образовательной организации.

В случае, если угроза безопасности ИС профессиональной образовательной организации имеет два типа источника возникновения, тогда вероятность на каждый из них приходится по 50% от определенной вероятности события. Так для первого случая получается B_1 = 7,14 %, тогда «Сбои и отказы программно-аппаратных средств от внешних источников угрозы» (B_{1-1}) и «Сбои и отказы программно-аппаратных средств от внутренних источников угрозы» (B_{1-2}) будут равны:

$$B_{1-1} = B_{1-2} = (B_1)/2 = 0{,}0714/2 = 0{,}0357 = 3{,}57\ \%.$$

Для второго случая получается B_2 = 3,57 % и только один источник угрозы (внутренний), поэтому вероятность события, которое может возникнуть только от одного типа источника (не важно внешнего или внутреннего) равна вероятности этого события. Для 3-го, 6-го и 8-го событий расчет аналогичен первому событию.

В зависимости от типа угрозы безопасности ИС профессиональной образовательной организации источники (уязвимости) подразделены на внешние и внутренние, но статистически не важно, откуда исходит угроза изнутри или снаружи, и предполагается, что внутренняя угроза $К_{внутр}$ способна нанести более значительный ущерб (к примеру, в два раза), чем внешняя $К_{внеш}$, тогда имеем зависимость:

$$К_{внутр} = М \cdot К_{внеш}, \quad (2.4)$$

где М – повышающий коэффициент угрозы, здесь М = 2.

Сумма внутренних $К_{внутр}$ и внешних $К_{внеш}$ угроз безопасности ИС профессиональной образовательной организации равна 1, т.к. внутренние $К_{внутр}$ и внешние $К_{внеш}$ угрозы описывают собой полное множество событий:

$$К_{внеш} + К_{внутр} = 1, \quad (2.5)$$

$$2 \cdot К_{внеш} + К_{внеш} = 1, \quad (2.6)$$

$$К_{внеш} = 1/3 = 0{,}333 = 33\ \%,$$

$$К_{внутр} = 1 - К_{внеш} = 1 - 0{,}333 = 0{,}667 = 67\%.$$

В первом предположении принимаем, что потенциал всех угроз безопасности ИС профессиональной образовательной организации составляет величину 100% и каждый следующий уровень потенциала угрозы от низкого к среднему и далее к высокому и очень высокому в два раза выше предыдущего. Тогда относительно потенциала угроз безопасности ИС профессиональной образовательной организации имеем множество уравнений:

$$Р_{низкий} + Р_{средний} + Р_{высокий} + Р_{очень\ высокий} = 1, \quad (2.7)$$

$$Р_{низкий} + 2 \cdot Р_{низкий} + 2 \cdot (2 \cdot Р_{низкий}) + 2 \cdot (2 \cdot (2 \cdot Р_{низкий})) = 1, \quad (2.8)$$

$$15 \cdot Р_{низкий} = 1, \quad (2.9)$$

где P – потенциал угрозы, значение которого пропорционально величине, характеризующей насколько опасен потенциал источника относительно всех источников угроз.

Раскрывая уравнения (2.8) и (2.9) имеем процентное соотношении потенциалов между собой:

$$Р_{низкий} = 1/15 = 0{,}067 = 7\%,$$

$$Р_{средний} = 2 \cdot Р_{низкий} = 2 \cdot 0{,}067 = 0{,}133 = 13\%,$$

$$Р_{высокий} = 2 \cdot Р_{средний} = 2 \cdot 0{,}133 = 0{,}266 = 27\%;$$

$$Р_{очень\ высокий} = 2 \cdot Р_{высокий} = 2 \cdot 0{,}266 = 0{,}532 = 53\%,$$

сумма которых составляет 100 %.

Потенциал угрозы безопасности ИС профессиональной образовательной организации, необходимый источнику для реализации угрозы (Р*) определяется, как сумма потенциалов угроз, которые больше или равны установленному уровню, потому что потенциал угроз выше необходимого уровня достаточен для нанесения ущерба и защита осуществлена, только для уровня угроз ниже уровня защиты:

$Р^*_{низкий} = Р_{низкий} + Р_{средний} + Р_{высокий} + Р_{очень\ высокий} = 0{,}067 + 0{,}133 + 0{,}266 + 0{,}532 = 1;$

$Р^*_{средний} = Р_{средний} + Р_{высокий} + Р_{очень\ высокий} = 0{,}133 + 0{,}266 + 0{,}532 = 0{,}93;$

$Р^*_{высокий} = Р_{высокий} + Р_{очень\ высокий} = 0{,}266 + 0{,}532 = 0{,}798;$

$Р^*_{очень\ высокий} = Р_{очень\ высокий} = 0{,}53.$

где P^* – потенциал угрозы, необходимый источнику для реализации угрозы безопасности ИС профессиональной образовательной организации.

Определяем значимости A_i наступления события в абсолютных единицах по формуле (2.1). Ниже приведены примеры расчета значимости A_i нас-

тупления события для определенных угроз безопасности ИС профессиональной образовательной организации:

$$A_{1-1} = B_{1-1} \cdot N_{1-1} \cdot P^*_{1-1} = 0{,}0135 \cdot 0{,}333 \cdot 1 = 0{,}00449;$$

$$A_{1-2} = B_{1-2} \cdot N_{1-2} \cdot P^*_{1-2} = 0{,}0135 \cdot 0{,}667 \cdot 0{,}93 = 0{,}00838;$$

$$A_2 = B_2 \cdot N_2 \cdot P^*_2 = 0{,}027 \cdot 0{,}667 \cdot 0{,}93 = 0{,}01676;$$

$$A_3 = B_3 \cdot N_3 \cdot P^*_3 = 0{,}027 \cdot 0{,}667 \cdot 1 = 0{,}01801;$$

$$A_{6-1} = B_{6-1} \cdot N_{6-1} \cdot P^*_{6-1} = 0{,}0135 \cdot 0{,}333 \cdot 0{,}53 = 0{,}00239;$$

$$A_{6-2} = B_{6-2} \cdot N_{6-2} \cdot P^*_{6-2} = 0{,}0135 \cdot 0{,}667 \cdot 1 = 0{,}00901;$$

$$A_{8-1} = B_{8-1} \cdot N_{8-1} \cdot P^*_{8-1} = 0{,}0135 \cdot 0{,}333 \cdot 0{,}8 = 0{,}00360;$$

$$A_{8-2} = B_{8-2} \cdot N_{8-2} \cdot P^*_{8-2} = 0{,}0135 \cdot 0{,}667 \cdot 1 = 0{,}00901;$$

……..;

$$A_{34-1} = B_{34-1} \cdot N_{34-1} \cdot P^*_{34-1} = 0{,}0135 \cdot 0{,}333 \cdot 1 = 0{,}00450;$$

$$A_{34-2} = B_{34-2} \cdot N_{34-2} \cdot P^*_{34-2} = 0{,}0135 \cdot 0{,}667 \cdot 0{,}93 = 0{,}00838.$$

Определим сумму всех значимостей:

$$(A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2}) =$$

$$= 0{,}00450 + 0{,}00838 + 0{,}01676 + 0{,}01802 + \ldots + 0{,}00450 + 0{,}00838 = 0{,}4789$$

и относительное значение значимости события относительно полного поля (100%) значимостей остальных событий по формуле (2):

$$A^*_{1-1} = (A_{1-1} / (A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2})) \cdot 100\ \% =$$

$$= (0{,}00450 / 0{,}4789) \cdot 100\ \% = 0{,}94\ \%;$$

$$A^*_{1-2} = (A_{1-2} / (A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2})) \cdot 100\ \% =$$

$$= (0{,}00838 / 0{,}4789) \cdot 100\ \% = 1{,}75\ \%;$$

$$A^*_2 = (A_2 / (A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2})) \cdot 100\ \% =$$

$$= (0{,}01676 / 0{,}4789) \cdot 100\ \% = 3{,}5\ \%;$$

$$A^*_3 = (A_3 / (A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2})) \cdot 100\ \% =$$

$$= (0{,}01801 / 0{,}4789) \cdot 100\ \% = 3{,}76\ \%;$$

$$A^*_{6-1} = (A_{6-1} / (A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2})) \cdot 100\ \% =$$

$$= (0{,}00239 / 0{,}4789) \cdot 100\ \% = 0{,}5\ \%;$$

$$A^*_{6-2} = (A_{6-2} / (A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2})) \cdot 100\ \% =$$

$$= (0{,}00901 / 0{,}4789) \cdot 100\ \% = 1{,}88\ \%;$$

$$A^*_{8-1} = (A_{8-1} / (A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2})) \cdot 100\ \% =$$

$$= (0{,}00360 / 0{,}4789) \cdot 100\ \% = 0{,}75\ \%;$$

$$A^*_{8-2} = (A_{8-2} / (A_{1-1} + A_{1-2} + A_2 + A_3 + \ldots + A_{34-1} + A_{34-2})) \cdot 100\ \% =$$

$$= (0{,}00901 / 0{,}4789) \cdot 100\ \% = 1{,}88\ \%.$$

В итоге относительное значение значимости события, относительно значимости всех событий, без учета типа угрозы (для отдельной угрозы) составляет следующие значения:

– сбои и отказы программно-аппаратных средств:

$$A^*_1 = A^*_{1-1} + A^*_{1-2} = 0{,}94\ \% + 1{,}75\ \% = 2{,}69\ \%;$$

– угрозы со стороны штатных пользователей и обслуживающего персонала:

$$A^*_2 = 3{,}5\ \%;$$

– ошибки руководства организации в связи с недостаточным уровнем осознания безопасности ИС профессиональной образовательной организации:

$$A^*_3 = 2{,}76\ \%;$$

– утечка информации;

$$A^*_6 = A^*_{6-1} + A^*_{6-2} = 0{,}5\ \% + 1{,}88\ \% = 2{,}38\ \%;$$

– нарушение функциональности и доступности персонала

$$A^*_8 = A^*_{8-1} + A^*_{8-2} = 0{,}75\ \% + 1{,}88\ \% = 2{,}63\ \%.$$

В результате выполненных расчетов угроз безопасности ИС профессиональной образовательной организации выясняется, что наиболее значимой угрозой информационной безопасности (из выбранных пяти) является угроза «Со стороны штатных пользователей и обслуживающего персонала» с величиной 3,5 %. В свою очередь наименее значимой является угроза

«Утечка информации» с относительным значением значимости события 2,38 %.

В результате анализа полученных данных для всех 14 угроз безопасности ИС профессиональной образовательной организации максимальной значимостью события 3,5 % обладает также угроза «Со стороны штатных пользователей и обслуживающего персонала (халатность пользователей)» с достаточно хорошей корреляцией по отношению к результатам оценки угроз группой экспертов.

2.3. Проект методики нивелирования/предупреждения угроз и уязвимостей информационно-безопасной оценки контента учебных достижений обучающихся профессиональных организаций

2.3.1. Предпосылки для разработки методики нивелирования/ предупреждения угроз и уязвимостей информационно-безопасной оценки контента учебных достижений обучающихся профессиональных организаций

Для оценки угроз и уязвимостей, в т. ч. нивелирования/предупреждения угроз и уязвимостей информационно-безопасной оценки контента учебных достижений обучающихся профессиональных организаций используются различные технологии, методы и методики, в основу которых заложены:

– экспертные оценки;

– статистические данные;

– учет факторов, влияющих на уровни угроз и уязвимостей.

Один из возможных подходов к разработке подобных методик – накопление статистических данных о реально случившихся происшествиях, анализ и классификация их причин, выявление факторов, от которых они зависят. На основе этой информации возможна оценка угроз и уязвимостей

в других информационных системах. Практические сложности в реализации этого подхода следующие: Во-первых, должен быть собран весьма обширный материал о происшествиях в области угроз и уязвимостей безопасности ИС профессиональной образовательной организации. Во-вторых, применение этого подхода далеко не всегда оправдано. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если система сравнительно невелика, использует новейшие элементы технологии (для которых пока нет достоверной статистики), оценки угроз и уязвимостей могут оказаться недостоверными.

Наиболее распространенным в настоящее время является подход, основанный на учете различных факторов, влияющих на уровни угроз и уязвимостей безопасности ИС профессиональной образовательной организации. Такой подход позволяет абстрагироваться от малосущественных технических деталей, учесть не только программно-технические, но и иные аспекты.

2.3.2 Разработка проекта методики нивелирования/предупреждения угроз и уязвимостей информационно-безопасной оценки контента учебных достижений обучающихся профессиональных организаций

Рассмотрим пример использования подхода, используемого в наиболее популярном во всем мире методе CRAMM (Code of Risk Analysis and Managment Method), в основе комплексного подхода которого сочетаются количественные и качественные методы анализа, для одного из классов угроз: «Использование чужого идентификатора штатными сотрудниками организации («маскарад»)».

Для оценки угроз безопасности ИС профессиональной образовательной организации выберем следующие косвенные факторы:

– статистика по зарегистрированным инцидентам;

– тенденции в статистке по подобным нарушениям;

– наличие в ИС информации, представляющей интерес для потенциальных внутренних или внешних нарушителей;

– моральные качества штатного персонала профессиональной образовательной организации;

– возможность извлечь выгоду из изменения обрабатываемой в системе информации;

– наличие альтернативных способов доступа к информации;

– статистика по подобным нарушениям в ИС других профессиональных образовательных организациях.

Для оценки уязвимостей безопасности ИС профессиональной образовательной организации выберем следующие косвенные факторы:

– количество рабочих мест (пользователей) в ИС профессиональной образовательной организации;

– размер рабочих групп пользователей) в ИС профессиональной образовательной организации;

– осведомленность руководства о действиях сотрудников (разные аспекты) профессиональной образовательной организации;

– характер используемого на рабочих местах оборудования и программного обеспечения ИС профессиональной образовательной организации;

– полномочия пользователей ИС профессиональной образовательной организации.

По косвенным факторам группе экспертов предложены тест-анкеты Приложения 1–2), содержащие вопросы и несколько фиксированных вариантов ответов, которые обладают определенной «стоимостью» в виде коли-

чества баллов. Итоговая оценка угрозы и уязвимости анализируемого класса определяется путем суммирования выставленных экспертами баллов.

Несомненным достоинством предложенного проекта методики оценки угроз и уязвимостей ИС профессиональной образовательной организации, реализующей подход наиболее популярного во всем мире метода CRAMM, является возможность учета множества косвенных факторов, причем не только технических). Методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что нужно изменить, чтобы улучшить оценки рисков безопасности ИС профессиональной образовательной организации. Успех такой оценки во многом зависит от квалификации привлекаемых экспертов, их практического опыта и объективированности используемых тест-анкет, а, следовательно, и квалификации разработчиков тест-анкет, включая их аудит.

Выводы по главе 2

Подвергнуты экспертной оценке общесистемные угрозы, программные и другие злоупотребления безопасности информационной системы профессиональной образовательной организации, составленные по результатам анкетирования команды экспертов, предварительно протестированных на предмет отсутствия неадекватных решений вне доверительного диапазона.

В качестве общесистемных угроз приняты к рассмотрению ошибки пользователя, отказ в обслуживании, недоступность информации, ошибки программного обеспечения, неправильная маршрутизация, аппаратные сбои, перегрузка трафика. Среднее значение комплексной оценки (2.76) общесистемных угроз безопасности ИС профессиональной образовательной организации располагается на повышенном уровне трудностей их

преодоления, нейтрализации и устранения. Наибольшую угрозу (2.98) составляют ошибки пользователей, что свидетельствует о недостаточно высокой их квалификации и необходимости проведения дополнительных курсов повышения уровня правильного владения ими приемами работы на персональном компьютере. Несколько незначительно меньшее среднее значение комплексной оценки (2.95) общесистемных угроз безопасности ИС профессиональной образовательной организации составляют отказы в обслуживании, что является, по-видимому, следствием:

– физического и морального износа используемого оборудования ИС;

– низкого качества (надежности) технических, программных или программно-технических средств;

– низкого качества (надежности) сетей связи и (или) услуг связи;

– отсутствия или низкой эффективности систем резервирования или дублирования программно-технических и технических средств;

– низкого качества (надежности) инженерных систем (кондиционирования, электроснабжения, охранных систем и т. д.);

– низкого качества обслуживания со стороны обслуживающих организаций и лиц;

– исчерпания вычислительных ресурсов, недоступности обновления программного обеспечения и т.д.

В качестве программных злоупотреблений приняты к рассмотрению маскарад, люки, программы открытия паролей, троянские кони, суперзаппинг, логические бомбы, пинание, раздеватели – пиратство, повторное использование объектов, программные закладки, скрытые каналы, компьютерные вирусы, работа между строк, подкладывание свиньи, программы захвата паролей, репликаторы, воздушные змеи, атаки салями. Среди программных злоупотреблений безопасности ИС профессиональной образователь-

ной организации наибольшее значение (3.5) принадлежит очень трудной возможности по усилиям нейтрализации/восстановления (для принципов безопасности А1 и А4) или восстановления нормальной работы (для принципов безопасности А2 и А3) вследствие программного злоупотребления «маскарад». Несколько в меньшей степени (2.5), но также достаточно с высокоопасным уровнем негативного влияния, обнаруживаются угрозы нарушения целостности и достоверности хранимых данных с помощью специальных программ, а также доступности ИС, данных и услуг всем уполномоченным пользователям вследствие программных злоупотреблений «люки», «троянские кони», «суперзаппинг», «логические бомбы». По остальным угрозам наблюдается средний их уровень.

В качестве других злоупотреблений и видов мошенничества приняты к рассмотрению перехват ПЭМИН, злоупотребления информацией, перехват информации, сетевые анализаторы, анализ трафика, кража информации, умышленное повреждение данных и программ, повреждение аппаратных средств и другие виды мошенничества. Среди других злоупотреблений и видов мошенничества безопасности ИС профессиональной образовательной организации наибольшее значение (3.5) принадлежит очень трудной возможности по усилиям нейтрализации/восстановления (для принципов безопасности А1 и А4) или восстановления нормальной работы (для принципов безопасности А2 и А3) вследствие злоупотребления «Перехват ПЭМИН». Несколько в меньшей степени (2.5), но также достаточно с высокоопасным уровнем негативного влияния, обнаруживаются угрозы нарушение целостности и достоверности хранимых данных с помощью специальных программ, а также доступности ИС, данных и услуг всем уполномоченным пользователям вследствие других злоупотреблений и других видов мошенничества, использования сетевых анализаторов, анализ трафика, кражи инфор-

мации, умышленного повреждения данных и программ ИС. По остальным угрозам наблюдается средний их уровень.

На основе анализа полученных результатов экспертной оценки критических угроз, активов и уязвимостей безопасности ИС профессиональной образовательной организации сформулирован предварительный вывод, что комплексные оценки угроз распределены в следующих интервалах:

– до 2.70 (включительно): Неправильная маршрутизация, аппаратные сбои, перегрузка трафика (для общесистемных угроз безопасности ИС профессиональной образовательной организации), программы захвата паролей, репликаторы, воздушные змеи, атаки салями (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и кража информации, умышленное повреждение данных и программ, повреждение аппаратных средств (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации);

– от 2.71 до 2.85 (включительно): Недоступность информации, ошибки программного обеспечения (для общесистемных угроз безопасности ИС профессиональной образовательной организации), программные закладки, скрытые каналы, компьютерные вирусы, работа между строк, подкладывание свиньи (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и сетевые анализаторы, анализ трафика и другие виды мошенничества (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации);

– и больше 2.85: Ошибки пользователя, отказ в обслуживании (для общесистемных угроз безопасности ИС профессиональной образовательной организации), маскарад, люки, программы открытия паролей, троянские кони,

суперзаппинг, логические бомбы (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и перехват ПЭМИН, злоупотребления информацией, перехват информации (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации).

В результате вероятностного анализа полученных данных для 34-х угроз безопасности ИС профессиональной образовательной организации максимальной значимостью события 3,76 % обладает также угроза «Халатность пользователей» с достаточно хорошей корреляцией по отношению к результатам экспертной оценки угроз безопасности ИС профессиональной образовательной организации.

Разработан проект методики количественной оценки угроз и уязвимостей ИС профессиональной образовательной организации путем суммирования выставленных экспертами баллов на вопросы предложенных им тест-анкет. Несомненным достоинством предложенного проекта методики оценки угроз и уязвимостей ИС профессиональной образовательной организации, реализующей подход наиболее популярного во всем мире метода CRAMM, является возможность учета множества косвенных факторов, причем не только технических. Методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что нужно изменить, чтобы улучшить оценки рисков безопасности ИС профессиональной образовательной организации. Успех такой оценки во многом зависит от квалификации привлекаемых экспертов, их практического опыта и объективированности используемых тест-анкет, а, следовательно, и квалификации разработчиков тест-анкет, включая их аудит.

ЗАКЛЮЧЕНИЕ

Для определения уровня безопасности информационной системы профессиональной образовательной организации желательно следовать следующей цепочке: источник угрозы – уязвимость (фактор) – угроза (действие) – последствия (атака, выбор и разработка мер защиты аппаратного и используемого программного обеспечения, совершенствование политики информационной безопасности профессиональной образовательной организации).

С точки зрения базовых угроз информационной безопасности профессиональной образовательной организации существует два алгоритма расчета уровня угроз одной базовой угрозы (суммарной) или трех базовые угрозы (конфиденциальности, целостности и доступности ИС профессиональной образовательной организации), по их уязвимости на основе критичности и вероятности реализации каждой конкретной угрозы.

Требующими особого внимания являются техногенные источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Эти угрозы напрямую зависят от свойств используемой техники. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости (факторы), приводящие к нарушению безопасности информации на конкретном объекте информатизации.

Уязвимости присущи объекту информатизации, неотделимы от него и

обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред. Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации. Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть объективными, субъективными и случайными.

Процесс оценки угроз конфиденциальности, целостности и доступности ИС профессиональной образовательной организации и рисков можно подразделить на девять основных этапов: определение характеристик ИС; идентификация уязвимостей; идентификация угроз; анализ регуляторов безопасности; определение вероятностей; анализ воздействий; определение рисков; рекомендуемые контрмеры; результирующая документация.

Оценка степени опасности угроз безопасности ИС профессиональной образовательной организации проводится по косвенным показателям. При этом в качестве критериев сравнения могут быть использованы следующие показатели: а) возможность возникновения источника угроз, позволяющая определять степень доступности к защищаемому объекту (для антропогенных источников), удаленность от защищаемого объекта (для техногенных

источников) или особенности обстановки (для случайных источников); б) готовность источника угроз, как степень квалификации и привлекательности совершения деяний со стороны источника угрозы (для антропогенных источников) или наличие необходимых условий (для техногенных и стихийных источников); в) фатальность угроз, определяющая степень неустранимости последствий реализации угрозы. Каждый показатель оценивается экспертно-аналитическим методом по пятибалльной системе.

Результаты ранжирования относительно конкретного объекта защиты сводятся в таблицу, позволяющую определить наиболее опасные для данного объекта источники угроз безопасности информации.

Современные образовательные организации широко используют в своей деятельности информационные технологии для ведения журналов, контроля успеваемости, административно-хозяйственной деятельности и т.п. К сожалению, информационные системы, используемые в профессиональных образовательных организациях в большинстве своем, не отвечают даже минимальным требованиям, предъявляемым к безопасным ИС.

Подвергнуты экспертной оценке общесистемные угрозы, программные и другие злоупотребления безопасности информационной системы профессиональной образовательной организации, составленные по результатам анкетирования команды экспертов, предварительно протестированных на предмет отсутствия неадекватных решений вне доверительного диапазона.

В качестве общесистемных угроз приняты к рассмотрению ошибки пользователя, отказ в обслуживании, недоступность информации, ошибки программного обеспечения, неправильная маршрутизация, аппаратные сбои, перегрузка трафика. Среднее значение комплексной оценки (2.76) общесистемных угроз безопасности ИС профессиональной образовательной

организации располагается на повышенном уровне трудностей их преодоления, нейтрализации и устранения. Наибольшую угрозу (2.98) составляют ошибки пользователей, что свидетельствует о недостаточно высокой их квалификации и необходимости проведения дополнительных курсов повышения уровня правильного владения ими приемами работы на персональном компьютере. Несколько незначительно меньшее среднее значение комплексной оценки (2.95) общесистемных угроз безопасности ИС профессиональной образовательной организации составляют отказы в обслуживании, что является, по-видимому, следствием:

– физического и морального износа используемого оборудования ИС;

– низкого качества (надежности) технических, программных или программно-технических средств;

– низкого качества (надежности) сетей связи и (или) услуг связи;

– отсутствия или низкой эффективности систем резервирования или дублирования программно-технических и технических средств;

– низкого качества (надежности) инженерных систем (кондиционирования, электроснабжения, охранных систем и т. д.);

– низкого качества обслуживания со стороны обслуживающих организаций и лиц;

– исчерпания вычислительных ресурсов, недоступности обновления программного обеспечения и т.д.

В качестве программных злоупотреблений приняты к рассмотрению маскарад, люки, программы открытия паролей, троянские кони, суперзаппинг, логические бомбы, пинание, раздеватели – пиратство, повторное использование объектов, программные закладки, скрытые каналы, компьютерные вирусы, работа между строк, подкладывание свиньи, программы захвата паролей, репликаторы, воздушные змеи, атаки салями. Среди програм-

мных злоупотреблений безопасности ИС профессиональной образовательной организации наибольшее значение (3.5) принадлежит очень трудной возможности по усилиям нейтрализации/восстановления (для принципов безопасности А1 и А4) или восстановления нормальной работы (для принципов безопасности А2 и А3) вследствие программного злоупотребления «маскарад». Несколько в меньшей степени (2.5), но также достаточно с высокоопасным уровнем негативного влияния, обнаруживаются угрозы нарушения целостности и достоверности хранимых данных с помощью специальных программ, а также доступности ИС, данных и услуг всем уполномоченным пользователям вследствие программных злоупотреблений «люки», «троянские кони», «суперзаппинг», «логические бомбы». По остальным угрозам наблюдается средний их уровень.

В качестве других злоупотреблений и видов мошенничества приняты к рассмотрению перехват ПЭМИН, злоупотребления информацией, перехват информации, сетевые анализаторы, анализ трафика, кража информации, умышленное повреждение данных и программ, повреждение аппаратных средств и другие виды мошенничества. Среди других злоупотреблений и видов мошенничества безопасности ИС профессиональной образовательной организации наибольшее значение (3.5) принадлежит очень трудной возможности по усилиям нейтрализации/восстановления (для принципов безопасности А1 и А4) или восстановления нормальной работы (для принципов безопасности А2 и А3) вследствие злоупотребления «Перехват ПЭМИН». Несколько в меньшей степени (2.5), но также достаточно с высокоопасным уровнем негативного влияния, обнаруживаются угрозы нарушение целостности и достоверности хранимых данных с помощью специальных программ, а также доступности ИС, данных и услуг всем уполномоченным пользователям вследствие других злоупотреблений и других видов мошенни-

чества, использования сетевых анализаторов, анализ трафика, кражи информации, умышленного повреждения данных и программ ИС. По остальным угрозам наблюдается средний их уровень.

На основе анализа полученных результатов экспертной оценки критических угроз, активов и уязвимостей безопасности ИС профессиональной образовательной организации сформулирован предварительный вывод, что комплексные оценки угроз распределены в следующих интервалах:

– до 2.70 (включительно): Неправильная маршрутизация, аппаратные сбои, перегрузка трафика (для общесистемных угроз безопасности ИС профессиональной образовательной организации), программы захвата паролей, репликаторы, воздушные змеи, атаки салями (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и кража информации, умышленное повреждение данных и программ, повреждение аппаратных средств (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации);

– от 2.71 до 2.85 (включительно): Недоступность информации, ошибки программного обеспечения (для общесистемных угроз безопасности ИС профессиональной образовательной организации), программные закладки, скрытые каналы, компьютерные вирусы, работа между строк, подкладывание свиньи (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и сетевые анализаторы, анализ трафика и другие виды мошенничества (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации);

– и больше 2.85: Ошибки пользователя, отказ в обслуживании (для общесистемных угроз безопасности ИС профессиональной образовательной ор-

ганизации), маскарад, люки, программы открытия паролей, троянские кони, суперзаппинг, логические бомбы (для программных злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации) и перехват ПЭМИН, злоупотребления информацией, перехват информации (для других злоупотреблений по отношению к безопасности ИС профессиональной образовательной организации).

В результате вероятностного анализа полученных данных для 34-х угроз безопасности ИС профессиональной образовательной организации максимальной значимостью события 3,76 % обладает также угроза «Халатность пользователей» с достаточно хорошей корреляцией по отношению к результатам экспертной оценки угроз безопасности ИС профессиональной образовательной организации.

Разработан проект методики количественной оценки угроз и уязвимостей ИС профессиональной образовательной организации путем суммирования выставленных экспертами баллов на вопросы предложенных им тест-анкет. Несомненным достоинством предложенного проекта методики оценки угроз и уязвимостей ИС профессиональной образовательной организации, реализующей подход наиболее популярного во всем мире метода CRAMM, является возможность учета множества косвенных факторов, причем не только технических. Методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что нужно изменить, чтобы улучшить оценки рисков безопасности ИС профессиональной образовательной организации. Успех такой оценки во многом зависит от квалификации привлекаемых экспертов, их практического опыта и объективированности используемых тест-анкет, а, следовательно, и квалификации разработчиков тест-анкет, включая их аудит.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Риски информационной безопасности веб-приложений [Электронный ресурс] – Режим доступа: https://habrahabr.ru/company/pentestit/blog/279219/.

2. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.

3. IT-Project Management [Электронный ресурс] – Режим доступа: https:// itproject management.wordpress.com/2008/04/17/Разбираемся-с-терминами-уязвимость-у/.

4. Вихорев С.В. Классификация угроз информационной безопасности [Электронный ресурс] – Режим доступа: http://www.cnews.ru/reviews/free/oldcom/ security/elvis_class.shtml.

5. Стандарт ISO:17799-00 (Стандарт Великобритании BS 7799-95 "Практические правила управления информационной безопасностью").

6. Руководящий документ. "Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации", Гостехкомиссия России, Сб-к руководящих документов по защите информации от несанкционированного доступа, М.: 1998., п. 4.

7. Виды угроз информационной безопасности и классификация источников угроз [Электронный ресурс] – Режим доступа: http://www.intuit.ru/studies/ courses/17846/1242/lecture/27498.

8. Угрозы безопасности для информационной системы вуза [Электронный ресурс] – Режим доступа: http://security.ase.md/publ/ru/pubru91/.

9. Домарев В. В. Безопасность Информационных Технологий. Методология создания систем защиты, Москва-Санкт-Петербург-Киев, 2002.

10. Международный стандарт ISO/IEC 17799. Информационные технологии: Свод практических правил управления защитой информации, ISO/IEC, 2000.
11. Идентификация угроз. Детальное рассмотрение процесса оценки рисков [Электронный ресурс] – Режим доступа: http://www.jetinfo.ru/stati/upravlenie-riskami-obzor-upotrebitelnykh-podkhodov-chast-2.
12. Оценка угроз безопасности информационным системам [Электронный ресурс] – Режим доступа: http://security.ase.md/publ/ru/pubru01.html.
13. Шнайдерман И.Б. Концепция системы информационной безопасности автоматизированных информационных систем / И.Б. Шнайдерман, С.А. Охрименко, Г.А. Черней // Автоматизация и современные технологии. – 1996. – № 8. – С.26–29.
14. Охрименко С.А. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) / С.А. Охрименко, Г.А. Черней // НТИ. Сер.1, Орг. и методика информ. работы. – 1996. – № 5. –С. 5–13.
15. Черней Г.А. Безопасность автоматизированных ИС / Г.А. Черней, С.А. Охрименко, Ф.С. Ляху. – Кишинев:Ruxanda, 1996. –186 с.
16. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – кн.1,2
17. Бадретдинова Р.Р. Разработка системы оценки и мониторинга рисков информационной безопасности на примере образовательной организации общего образования [Электронный ресурс] – Режим доступа: degree_work_file.
18. Васильев Р.А. Курс лекций по информационной безопасности образования [Электронный ресурс] – Режим доступа: http://5_____pdf.

19. Каберник В.В. Информационная безопасность образовательных учреждений в контексте противодействия угрозам терроризма и экстремизма [Электронный ресурс] – Режим доступа: http://Informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdeniy-v-kontekste-protivodeystviya-ugrozam-terrorizma-i-ekstremizma.
20. Астахов А. Искусство управления информационными рисками [Электронный ресурс] – Режим доступа: http://xn----7sbab7afcqes2bn.xn--p1ai/content/octave.
21. Жаринова И.А. Диагностика сформированности конструкторско-технологических знаний и умений у будущего учителя технологии. Канд. дис., Екатеринбург, 2001.
22. Блюмберг В.А. Какое решение лучше? Метод расстановки приоритетов / В.А. Блюмберг, В.Ф. Глущенко. – Л.: Лениздат, 1982. – 89 с.
23. Шляхтенко С.Г. Категории качества и количества / С.Г. Шляхтенко. – Л.: Изд. ЛГУ, 1968.
24. Глушков, В.М. Введение в АСУ. Изд. 2-е / В.М. Глушков. – Киев, Техника, 1974.
25. Черняк Ю.И. Системный анализ в управлении экономикой / Ю.И. Черняк. – М.: Экономика. 1971.
26. Новые технологии перехвата данных: ПЭМИН («TEMPEST») [Электронный ресурс] – Режим доступа: https://www.mipko.ru/blog/2011/01/perehvat-dannyh-s-klaviatury/.
27. Макаренко С.И. Информационная безопасность: учеб. пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
28. Белевитин, В.А. Магистерская диссертация: рекомендации по подготовке и защите: учебно-методич. пособие / В.А. Белевитин, Е.А. Гнатышина, И.Г. Черновол. – Челябинск, 2016.

29. Защита компьютерной информации от утечки по ПЭМИН [Электронный ресурс] – Режим доступа: www.support17.com/component/content/39.html?.
30. Вероятность произведения событий [Электронный ресурс] – Режим доступа: www life-prog.ru/1_32219_veroyatno...niya-sobitiy.html.
31. Вероятность наступления события [Электронный ресурс] – Режим доступа: www.infourok.ru/issledovatelskaya...bitiya-993492.html/.
32. Метод и модель формирования системы обеспечения информационной безопасности [Электронный ресурс] – Режим доступа: aspirantura.ifmo.ru/file/other/FiaRFzLArW.pdf.
33. Корбаинова Е.В. Определение основных характеристик модели защиты информации, основанной на иммунных принципах / Е.В. Корбаинова, А.С. Згурский // Сб-к статей XI конференции «Фундаментальные и прикладные исследования, разработка и применение высоких технологий». Том 1 – СПб, 2011. – С. 114–116.
34. Згурский А.С. Алгоритм оценки степени потребности информационного актива в свойствах безопасности / А.С. Згурский, Е.В. Корбаинова // Научно-технический вестник Поволжья, Том №2 – Казань, 2011, С. – 95–98.
35. Згурский А.С. Основные угрозы и источники-субъекты угроз информационной безопасности организаций РФ // Сб-к тезисов седьмой междун. науч.-практич. конференции «Современные проблемы гуманитарных и ЕСтественных наук». Москва, 2011, – С. 58–59.
36. Электронный учебник по разработке информационной безопасности персональных компьютеров // Help Antivirus – URL: http://helpantivirus.ru/developmentsafety/Menu.php.
37. Галатенко В. А. Основы информационной безопасности. – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2008. – 208 с.

38. Астахов А. Анализ защищенности корпоративных автоматизированных систем // Jet Info [Электронный ресурс] – Режим доступа: – URL: www.jetinfo.ru\2002\7\1\article1.7.2002.html.

39. Доля А. Внутренние угрозы ИТ-безопасности. // Byte-Россия [Эл. ресурс] – N 12, 2004. – URL: www.bytemag.ru/?ID=603365.

40. Атака через Интернет / Медведовский И. Д., Семьянов П. В., Платонов В. В.; под ред. П. Д. Зегжды. – СПб.: изд. НПО «Мир и семья-95», 1997.

41. Мэйволд Э. Безопасность сетей: курс лекций для Интернет- университета информационных технологий / Э. Мэйволд.– М.: Интернет-университет информационных технологий [Электронный ресурс] – Режим доступа: – www.INTUIT.ru, 2006. – URL: www.intuit.ru/department/security/netsec/.

42. Васенин В.А. Информационная безопасность и компьютерный терроризм / В.А. Васенин // Научные и методологические проблемы информационной безопасности. — М.: МЦПМО, 2004.

43. Зегжда Д.П.. Как построить защищенную информационную систему / Д.П. Зегжда, А.М. Ивашко. – СПб.: Мир и семья. – 2007.

44. Расторгуев С.П. Философия информационной войны / С.П. Расторгуев. – М.: Вузовская книга. – 2001.

45. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности личности / Г.Л. Смолян // Информационное общество. – М.:, 1999.

46. Черешкин Д.С. Сетевая информационная революция / Д.С. Черешкин, Г.Л. Смолян // Информационные ресурсы России, № 4. – 1997.

47. Антопольский А.А. Ответственность за правонарушения при работе с конфиденциальной информацией / А.А. Антопольский // Административная ответственность. – М.: ИГиП РАН, – 2001.

48. Бачило И.Л. Информационное право: основы практической информатики / И.Л. Бачило. – М.: Юринформцентр, – 2001.

49. Астахова Л.В. Информационная безопасность: герменевтический подход. – М.: РАН, 2010.

50. Ващекин Н.П. Цивилизация и Россия на пути к устойчивому развитию: проблемы и перспективы / Н.П. Ващекин, В.А. Лось, А.Д. Урсул. – М.: МГУК, 1999.

51. Ващекин Н.П. Безопасность и устойчивое развитие России / Н.П. Ващекин, М.И. Дэлиев, А.Д. Урсул. – М.: МГУК, 1998.

52. Bynum T. Ethical Challenges to Citizens of the Automatic Age: Norbert Wiener on the Information Society *II* Journal of Information, Communication and Ethics in Society. – 2004. – № 2(2).

53. Johnson D. Computer Ethics. – New Jersey: Prentice Hall, 2001.

54. Ван Дюн Дж. Роль человеческого фактора в совершении преступлений в сфере компьютеров / Дж. Ван Дюн // Компьютеризация общества и человеческий фактор. – М., 1988.

55. Капурро Р. Информационная этика / Р. Капурро // Информационное общество. – 2010. – Вып. 5.

56. Maner V. Unique Ethical Problems in Information Technology // Science and Engineering Ethics 1996. – № 2(2).

57. Moor J. Why We Need Better Ethics for Emerging Technologies // Ethics and Information Technology, 2005. – Vol. 7(3).

58. Himrna K. E. The handbook of information and computer ethics / K.E. Himrna, H.T. Tavani. – New Jersey: Wiley-Interscience, 2008.

59. Freeman L.. Information Ethics: Privacy and Intellectual Property. – Hersey: Information Science Publishing, 2005.

Приложение 1

Тест-анкета оценки угроз безопасности ИС
профессиональной образовательной организации

1. Сколько раз за последние 3 года сотрудники организации пытались получить несанкционированный доступ к хранящейся в ее ИС информации с использованием прав других пользователей?

a) Ни разу (0 баллов); b) Один или два раза (10 баллов); c) В среднем один раз в год (20 баллов); d) В среднем более одного раза в год (30 баллов); e) Неизвестно (10 баллов).

2. Какова тенденция в статистике такого рода попыток несанкционированного проникновения в информационную систему?

a) К возрастанию (10 баллов); b) Оставаться постоянной (10 баллов); c) К снижению (10 баллов).

3. Хранится ли в информационной системе информация (например, личные дела), которая может представлять интерес для сотрудников организации и побуждать их к попыткам не санкционированного доступа к ней?

a) Да (5 баллов); b) Нет (0 баллов).

4. Известны ли случаи нападения, угроз, шантажа, давления на сотрудников со стороны по сторонних лиц?

a) Да (10 баллов); b) Нет (0 баллов).

5. Существуют ли среди персонала группы лиц или отдельные лица с недостаточно высокими моральными качествами?

a) Нет, все сотрудники отличаются высокой честностью и порядочностью (0 баллов); b) Существуют группы лиц и отдельные личности с недостаточно высокими моральными качествами, но это вряд ли может спровоцировать их на несанкционированное использование системы (5 баллов); c) Существуют группы лиц и отдельные личности с настолько

низкими моральными качествами, что это повышает вероятность несанкционированного использования системы сотрудниками (10 баллов).

6. Хранится ли в информационной системе информация, несанкционированное изменение которой может принести прямую выгоду сотрудникам?

a) Да (5 баллов); b) Нет (0 баллов).

7. Предусмотрена ли в информационной системе поддержка пользователей, обладающих техническими возможностями совершить подобные действия?

a) Нет (0 баллов); b) Да (5 баллов).

8. Существуют ли другие способы просмотра информации, позволяющие злоумышленнику добраться до нее более простыми методами, чем с использованием «маскарада»?

a) Да (10 баллов); b) Нет (0 баллов).

9. Существуют ли другие способы несанкционированного изменения информации, позволяющие злоумышленнику достичь желаемого результата более простыми методами, чем с использованием «маскарада»?

a) Да (10 баллов); b) Нет (0 баллов).

10.Сколько раз за последние 3 года сотрудники пытались получить несанкционированный доступ к информации, хранящейся в других подобных системах в вашей организации?

a) Ни разу (0 баллов); b) Один или два раза (5 баллов); c) В среднем раз в год (10 баллов); d) В среднем чаще одного раза в год (15 баллов); e) Неизвестно (10 баллов).

Итог тест-анкетирования по сумме выставленных экспертами баллов: Степень угрозы при количестве баллов: До 9 баллов – Очень низкая; От 10 до 19 баллов – Низкая; От 20 до 29 баллов – Средняя; От 30 до 39 баллов – Высокая 40 и более 40 баллов – Очень высокая.

Приложение 2

Тест-анкета оценки уязвимостей безопасности ИС
профессиональной образовательной организации

1. Сколько людей имеют право пользоваться информационной системой?

a) От 1 до 10 (0 баллов); b) От 11 до 50 (4 балла); c) От 51 до 200 (10 баллов); d) От 200 до 1000 (14 баллов).

2. Пользователи информационной системой ведут себя необычным образом?

a) Да (0 баллов); b) Нет (10 баллов).

3. Какие устройства и программы доступны пользователям?

a) Только терминалы или сетевые контроллеры, ответственные за предоставление и маршрутизацию информации, но не за передачу данных (5 баллов);

b) Только стандартные офисные устройства и программы и управляемые с помощью меню подчиненные прикладные программы (0 баллов);

c) Пользователи могут получить доступ к операционной системе, но не к компиляторам (5 баллов);

d) Пользователи могут получить доступ к компиляторам (10 баллов);

4. Возможны ли ситуации, когда сотрудникам, предупрежденным о предстоящем сокращении или увольнении, разрешается логический доступ к информационной системе

a) Да (10 баллов); b) Нет (0 баллов).

5. Каковы в среднем размеры рабочих групп сотрудников пользовательских подразделе ний, имеющих доступ к информационной системе?

a) Менее 10 человек (0 баллов); b) От 11 до 20 человек (5 баллов); c) Свыше 20 человек (10 баллов).

6. Станет ли факт изменения хранящихся в информационной системе дан-

ных очевидным сразу для нескольких человек (в результате чего его будет очень трудно скрыть

a) Да (0 баллов); b) Нет (10 баллов).

7. Насколько велики официально предоставленные пользователям возможности по про смотру всех хранящихся в системе данных?

a) Официальное право предоставлено всем пользователям (2 балла); b) Официальное право предоставлено только некоторым пользователям (0 баллов).

8. Насколько необходимо пользователям знать всю информацию, хранящуюся в системе?

a) Всем пользователям необходимо знать всю информацию (4 балла); b) Отдельным пользователям необходимо знать лишь относящуюся к ним информацию (0 баллов).

Итог тест-анкетирования по сумме выставленных экспертами баллов:

Степень уязвимости при количестве баллов: До 9 баллов – Низкая: От 10 до 19 баллов – Средняя; 20 и более баллов – Высокая.