МИНИСТЕРСТВО ПРОСВЩЕНИЯ 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

Оценка эффективности средств и методов защиты конфиденциональной информации в 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:
68,82% авторского текста

Работа рекомендована к защите
«26» 12 2025 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ 309-210-2-1
Лазарев Максим Александрович

Научный руководитель:
Доктор технических наук, профессор
кафедры АТ,ИТиМОТД
Белевитин Владимир Анатольевич

Челябинск
2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Новая технологическая формация, сопровождающаяся четвертой промышленной революцией (Industrie 4.0) в рамках сложной и нестабильной системы постиндустриальной реальности, делает попытку расстановки приоритетов развития технологий «цифровой трансформации», предполагающей переход к «шестому технологическому укладу» постиндустриальной эпохи. В научной литературе с различных позиций обсуждаются тренды направлений переформатирования цифровой образовательной среды в рамках утвержденного от 18.09.2023 г. № 2894-р распоряжения Правительства Российской Федерации «Стратегическое направление в области цифровой трансформации образования», относящейся непосредственно к основной сфере базовой деятельности Министерства просвещения Российской Федерации» до 2030 года.

Фундаментальной базой для эффективно-практической цифровой трансформации образования в целом согласно взглядов Президента РАО О.Ю. Васильевой и академика РАО А.М. Новикова, а, следовательно, и технологий цифровой трансформации индустрии, служат теоретические знания наук «сильной» версии из курсов дисциплин, прежде всего, математики, физики, механики, химии и информатики. В аспекте Форсайта образования 2035 становится наиболее острой необходимостью актуализация инновационного подхода к решению, в первую очередь, приоритетных задач профессионального образования по методологическому использованию взаимных пересечений предметных областей педагогики, информатики и математики в гибридно-едином концептуальном поле (на базе вероятностно-статистического подхода) отечественных программных модулей интегративно оцифрованных моделей.

Основополагающим базисом надежной значимости гаранта качества объективизации уровня успешности субъектов профессионального образования при цифровой трансформации в настоящее время служит много-

компонентный инструментарий информационно-коммуникационных технологий (ИКТ) с опорой на положения современных подходов и моделей мониторинга педагогической квалиметрии (В.Г. Горб, Л.Н. Давыдова, Н.Ф. Ефремова, Н.А. Кулемина, А.Н. Майорова, Д.Ш. Матрос, М.М. Поташ-ник, Е.И. Сахарчук и др.), научно-методологической базой которых являются труды М.Б. Гитман, А.Н. Данилова, Е.Л. Кон, Е.Н. Малышева, Д.Г. Мирошина, Б.А. Сазонова, В.Ю. Столбова, А.А. Овчинникова, В. И. Фрейман, О.Ф. Шиховой, Ю.А. Шихова, А.А. Южакова и других учёных, а также концептуальной основы педагогических измерений и образовательной квалиметрии В.С. Аванесова, А.А. Маслак, Б.Е. Механцева, Е.А. Михайлычева, С.А. Сафонцева, В.С. Черепанова и др.

Практико-организационное налаживание нормативизации научно-исследовательской ситуации с эффективно-прагматическим применением в педагогике инновационных ресурсов мониторинго-диагностического инструментария имеет ряд сформировавшихся притиворечий:

– в наукометрическом плане – между необходимостью разработки нормативных требований к объективизации оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации и явной недостаточностью современных научных разработок в таком направлении их цифровой трансформации;

– в методическом плане между имеющимися в сопредельных с педагогикой науках «сильной» версии (физики, химии, математики, информатики, механики и др.) разработок инновационного инструментария с дополнительным привлечением эффективных операций оценочного расчёта эффективности средств и методов защиты конфиденциональной информации в образовательной организации и нередко лишь частичной дискретностью, а, в большей части случаев, и отсутствием в системе педагогического знания новых исследований и разработок штатных педагогических исследовательских проблем;

– в технолого-педагогическом плане – между признанием педагогами-исследователями и теоретиками насущной необходимости в прикладных разработках по адаптации в педагогике инновационного инструментария с гибридно-дополнительным привлечением эффективных операций цифровой трансформации в системе научно-педагогических исследований.

Сформировавшиеся противоречия оказывают негативное влияние как на развитие инновационных процессов цифровой трансформации в сфере организации, управления и реализации ОПОП, так и на, по меньшей мере, удовлетворительном становлении объективно-детерминирующей диагностики мониторинга (аудита) оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации. Насущная необходимость эффективного преодоления приведенных выше противоречий обусловила предполагаемую научную и практическую значимость и актуальность проведенного исследования, целевую направленность его темы и проблематики.

Актуальность проблемы, научная и практическая значимость, а также для современных условий цифровизации образования недостаточная разработанность её на методологическом уровне обусловили выбор темы научно-педагогического исследования **«Оценка эффективности средств и методов защиты конфиденциональной информации в образовательной организации».**

Объект исследования – современная практика инновационного инструментария методологического обеспечения научно-педагогических исследований оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации.

Предмет исследования – организационно-педагогические условия инновационного конструирования диагностического инструментария в практике методологии научно-педагогических исследований (на всех этапах проведения) посредством разработки варианта опытно-экспериментального алгоритма модели генерирования расчетных операций предвари-

тельной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации как важного компонента методики профессионального образования в ракурсе трансформации научно-исследовательскоӣ культуры и цифровой грамотности педагогов-исследователей, магистрантов, аспирантов и др.

Цель исследования – инновационно-логическое конструирование варианта опытно-экспериментального алгоритма модели генерирования расчетных операций предварительной подготовки процесса повышения класса комплексной защищенности информационноӣ системы функционирования средств и методов защиты конфиденциональной информации в информационноӣ сфере образования при оценке эффективности средств и методов защиты конфиденциональной информации в образовательной организации.

Гипотеза исследования:

Эффективность практического применения в педагогическоӣ научно-исследовательскоӣ практике недостаточно детерминируется из-за отставания уровня объективизации исходных данных мониторинга (аудита) в педагогике как науки «слабой» версии в области научно-исследовательскоӣ культуры по отношению к сопредельным социальным и гуманитарным наукам, а, тем более, к наукам «сильной» версии. Успешное формирование в педагогике научно-исследовательскоӣ мультикультуры субъектов образовательной деятельности (педагогов-исследователеӣ, магистрантов, аспирантов и др.) на основе инновационных ресурсов мониторингодиагностического инструментария возможно при соблюдении набора следующих условий:

– научно-обоснованного подхода в применении экспертных и/или логических методов (включающих теории вероятности и статистики (в т.ч. непараметрическоӣ), теорию ошибок)), ресурсного потенциала вычислительной математики, педагогической квалиметрии и аппаратно-программных возможностей информационно-коммуникационных технологий;

– конструирование диагностического инструментария в практике методологии научно-педагогических исследований (на всех этапах проведения) посредством разработки варианта опытно-экспериментального алгоритма модели генерирования расчетных операций предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации как важного компонента методики профессионального образования в ракурсе цифровой трансформации.

Задачи исследования:

1. Анализ методов и средств методического подхода количественной оценки защиты информации образовательной организации, включая особенности методического подхода к оценке эффективности защиты информации в информационной сфере образования и эффективности функционирования средств и методов защиты конфиденциональной информации.

2. Определение исходных этапов успешной реализации методического подхода к оценке эффективности защиты конфиденциональной информации в информационной сфере образования.

3. Разработка практических занятий по повышению класса комплексной защищенности информационной системы функционирования средств и методов защиты конфиденциональной информации в информационной сфере образования в качестве варианта опытно-экспериментального алгоритма модели генерирования расчетных операций предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации.

Методы исследования: анализ публикаций – статей, монографий, диссертаций и авторефератов в аспекте феноменологической организации научно-педагогических исследований и различных обследований в системе организаций профессионального образования с применением опций

статистико-математических методов диагностического инструментария в практике методологии научно-педагогических исследований.

Методология запланированного исследования определяется методологией педагогических исследований (В.В. Краевский, Б.И. Коротяев и др.), методологией проблем информационной безопасности (В.Г. Герасименко, Д.П. Зегжда, А.А. Малюк, М.П. Сычев, С.П. Расторгуев и др.), вопросами информационной безопасности при применении образовательных коммуникационных технологий (И. Морев, А.В. Федоров, А.В. Шариков).

Теоретические основы исследования: теоретические разработки по научно-практическим аспектам информационной безопасности как педагогической проблемы (Р.В. Амелин, О.В. Казарин, А.А. Журин, П.Н. Корнюшин, А.А. Марков, В.А. Семененко, В.Н. Ясенев и др.), теоретические разработки по проблеме развития области информационной безопасности (Р.И. Айзман, М.А. Борисов, В.А.Г алатенко, В.В. Гафнер, Г.В. Грачев, А.А. Малюк, Л.В. Скворцов, Г.А. Стародубова).

Личный вклад автора.

1. Заключается в самостоятельно проведенном анализе методов и средств методического подхода количественной оценки защиты информации образовательной организации, включая особенности методического подхода к оценке эффективности защиты информации в информационной сфере образования и эффективности функционирования средств и методов защиты конфиденциональной информации, включая их наиболее практически значимые аспекты и особенности в ракурсе повышения класса комплексной защиты.

2. Выявлена значимость исходных этапов успешной реализации методического подхода к количественной оценке эффективности защиты конфиденциональной информации в информационной сфере образования.

3. Выполнена разработока практических занятий по повышению класса комплексной защищенности информационной системы функционирования

средств и методов защиты конфиденциональной информации в информационной сфере образования в качестве варианта опытно-экспериментального алгоритма модели генерирования расчетных операций предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации.

Теоретическая значимость результатов исследования:

Расширен на интеллектуально-логическом уровне диапазон ресурсного потенциала повышения класса комплексной защиты конфиденциональной информации в образовательной организации на основе совершенствования методического подхода количественной оценки защиты исходных принципов предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации.

2. Конкретизированы методические аспекты и особенности использования исходных принципов предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации.

Научная новизна исследования результатов исследования:

Конкретизированы методические аспекты и особенности использования исходных принципов предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации.

Практическая значимость полученных результатов:

Инновационный вариант практических занятий по повышению класса комплексной защищенности информационной системы функционирования средств и методов защиты конфиденциональной информации в информационной сфере образования в качестве варианта опытно-экспериментального алгоритма модели генерирования расчетных операций предварительной подготовки процесса оценки эффективности средств и

методов защиты конфиденциональной информации в образовательной организации.

На защиту выносятся следующие положения:

1. Анализ возможностей ресурсного потенциала методов и средств методического подхода количественной оценки защиты информации образовательной организации, включая особенности методического подхода на получение более надёжных результатов в оценке эффективности защиты информации в информационной сфере образования и эффективности функций средств и методов защиты конфиденциональной информации.

2. Обладающий новизной инструментарий комбинированной реализации принципов предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации в качестве варианта опытно-экспериментального алгоритма модели генерирования расчетных операций предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в организации образования.

Достоверность результатов обеспечивается чётким соблюдением требований методологии педагогической квалиметрии и использованием в педагогическом исследовании инновационных опций ресурсного потенциала повышения класса комплексной защиты конфиденциональной информации в образовательной организации на основе совершенствования методического подхода количественной оценки защиты исходных принципов предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации.

Структурно диссертация состоит из введения, двух глав, заключения, общим объемом 93 машинописных страниц, списка использованной литературы из 35 наименований. Работа иллюстрирована 17 рисунками и 5 таблицами.

ГЛАВА 1. МЕТОДЫ И СРЕДСТВА МЕТОДИЧЕСКОГО ПОДХОДА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ЗАЩИТЫ ИНФОРМАЦИИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.5. Особенности методического подхода к оценке эффективности защиты информации в информационной сфере образования

В современном мире невозможно представить организацию без защищаемой информации и информационных технологий. В сфере информационной безопасности (ИБ) основными её задачами является сохранять свойства информации, обеспечивать целостность данных, их конфиденциальность и доступность. Основным шагом оптимизации затрат на систему защиты информации (СЗИ) современной организации является анализ рисков ИБ и угроз с выявлением наиболее критических факторов, оказывающих наиболее отрицательное влияние на ИБ СЗИ образовательной организации. Анализ рисков используется организациями для оценки рисков и угроз в информационных системах (ИС), для определения уязвимостей и для определения защитных средств, с помощью которых обеспечивается необходимый уровень защищённости информации (рисунок 1) [1]. При этом необходимо учитывать, что в организациях у различных ИС угрозы и уязвимости имеют вес [2], что означает – главной задачей ИБ организации является управление рисками нарушения информационной целостности, а обеспечение – это главный критерий качества выполнения информационных процессов, в том числе иинформационной инфраструктурой организации в целом [3].

Одним из наиболее немаловажных процессов при организации СЗИ образовательной организации является минимизация затрат, причем этот процесс не должен приводить к существенному затруднению работы пользователей. Для СПО и ВУЗов, с учетом необходимости оптимизации затрат на СЗИ, наиболее приемлемым является комбинированный метод, заключающийся в том, что необходимо экранировать лишь определенные подразделения от внешних воздействий, организовать доступ пользова-

телей к информационной системе (ИС) и к открытым сетям автоматизированного рабочего места (АРМ) также только лишь при необходимости [4].

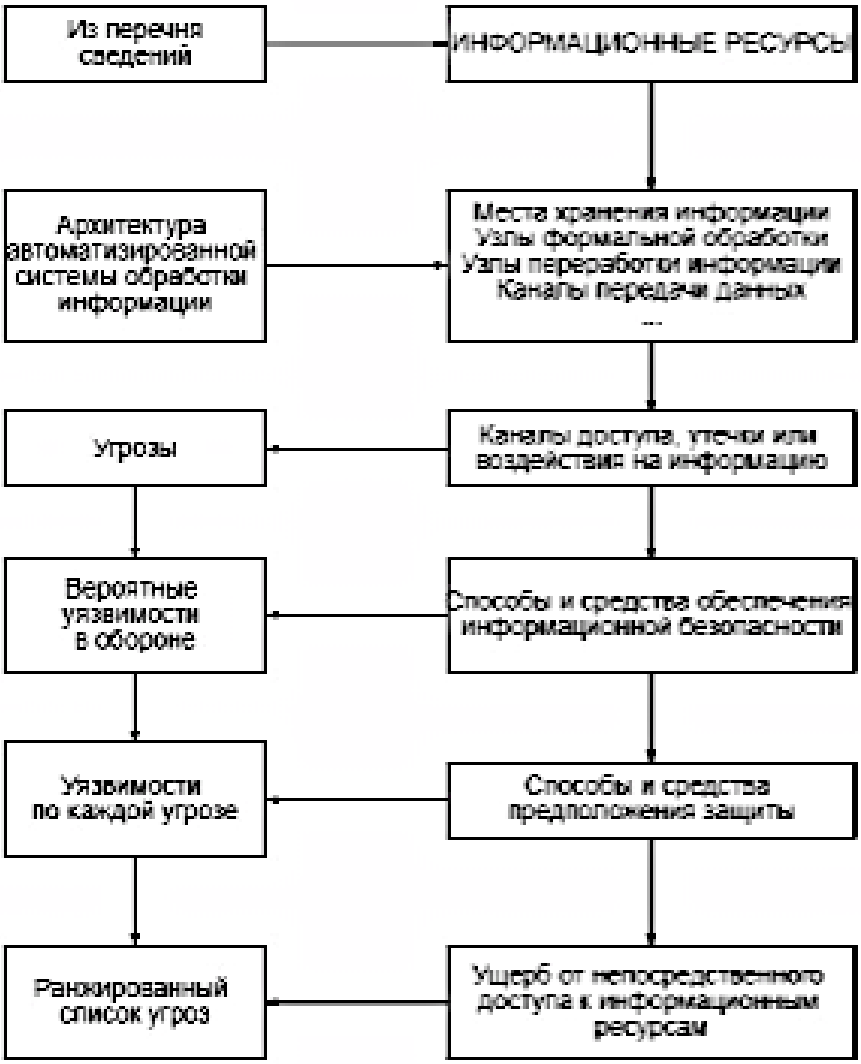


Рисунок 1.1 – Этапы сценария анализа информационных ресурсов

Приведенная в статье [1] методика разрабатывает политику ИБ организации, включающую комплекс системы защиты, который может привести режим ИБ к высокому уровню эффективности. Данная методика имеет преимущество над другими методиками за счёт того, что является положительным свойством, как в количественной, так и в качественной оценке. Вместе с тем, высокий уровень эффективности вышеупомянутого комплекса СЗИ вследствие использования многообразия мер защиты делают задачу оценки их эффективности достаточно сложной. Практическое применение вышеупомянутой методики применительно к СЗИ образо-

вательной организации представляется весьма затруднительной также из-за особенностей балльной оценки эмпирической, как правило, информации эмпирического характера.

Основные требования к качеству информации и знаний в информационной сфере образования иллюстрирует рисунок 1.2.

Рисунок 1.2 – Качество информационных ресурсов [5]

Данные нижнего ряда пирамиды информационной сферы образования, накапливаясь и подвергаясь систематизации и обобщению, должны превращаться в отфильтрованную полезную информацию, а затем накапливаться в виде знаний и использоваться на всех уровнях рядов иерархии информационной сферы образования. Это приводит к необходимости создания информационной инфраструктуры сфере образования с соответствующими техническими и программными средствами обработки данных, т.к. для её успешности, даже не говоря о повышении её эффективности, необходимо учитывать большее число факторов и невозможность проверки достоверности всех используемых данных. Только в этом случае, говоря о риске, можно предполагать, как минимум, что знаний достаточно, во-первых, для идентификации риск-факторов, а во-вторых, для их измерений (оценки). Проблема установления рациональ-

ного баланса между эффективностью и ИБ – главная проблема информационной сферы образования. Это информационная проблема. Ее решение потребует объективных знаний о рисках, определены которые на множествах факторов, влияющих на них, причём эти множества могут пересекаться (рисунок 1.3).

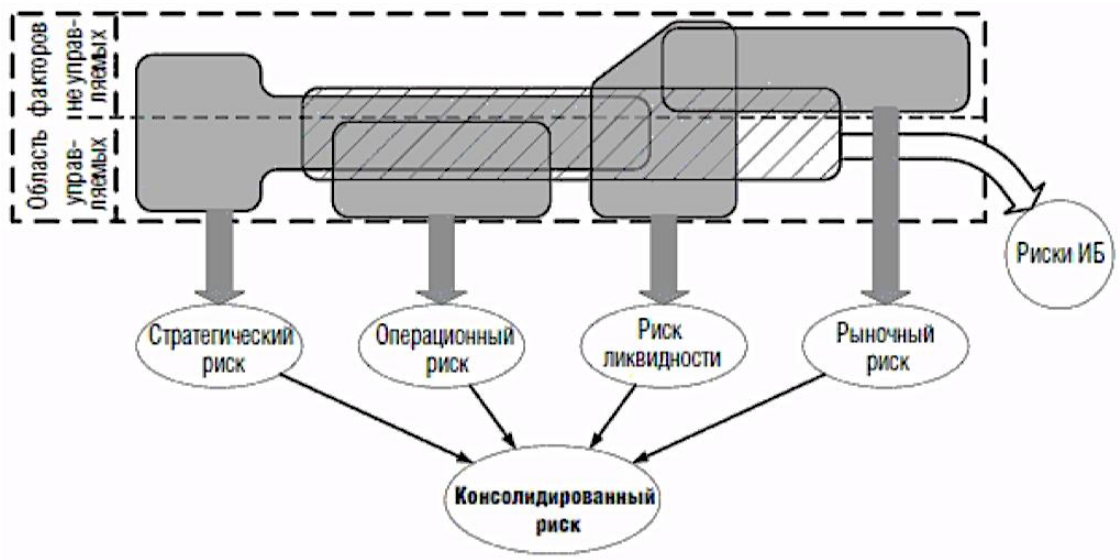


Рисунок 1.3 – Коммуникативность и взаимосвязь рисков информационных ресурсов [5]

Из всех рисков риски ИБ наиболее сложные по своей природе, имеют самую большую неопределенность как по рисковым событиям, так и по наносимому ущербу. Так, например, событие операционного риска «Отказ сервера», происшедшее вследствие влияния факторов физической природы, значительно более предсказуемо, чем отказ как следствие влияния человеческого фактора злонамеренной природы. особенностью рисковых событий и ситуаций ИБ является то, что они протяженные во времени и накапливающегося типа, т. е. любое событие в отдельности наносит очень (на практике пренебрежительно) малый ущерб. А «типовой сценарий» значимого рискового события ИБ (повлекшего значительный ущерб) сводится, как правило, к тому, что реализуется пачка событий (временной ряд) с незначительным ущербом (часто вообще без ущерба); в результате влияния пачки создается и удерживается некоторое время рисковая ситуация и, как следствие, реализуется значимое рисковое

событие. Содержательно и формально критическую часть информационной сферы организации, в т.ч. образовательной, способную наносить ущербы и приводить к негативным последствиям для целей организации, определяет пятёрка риск-факторов «А, П, И, С, Р») – активы (А), процессы (П), инструменты (И), субъекты (С) и роли (Р). У базовых рисковых событий всегда через их риск-факторы может быть идентифицирован их контекст в информационной сфере организации. Так, если пересечение контекстов событий S_i и S_j пустое, т. е.

$$K\langle S_i\rangle \cap K\langle S_{ij}\rangle \neq \varnothing,$$

то между S_i и S_j возникает связь и можно говорить о связанной цепочке событий. Можно также говорить о силе этой связи, понимая под ней значение

$$A_{ij} = K\langle S_i\rangle \cap K\langle S_j\rangle \neq \varnothing,$$

то есть чем больше A_{ij}, тем сильнее связь. Связи рисковых событий и понесенных ущербов иллюстрируются рисунком 1.4.

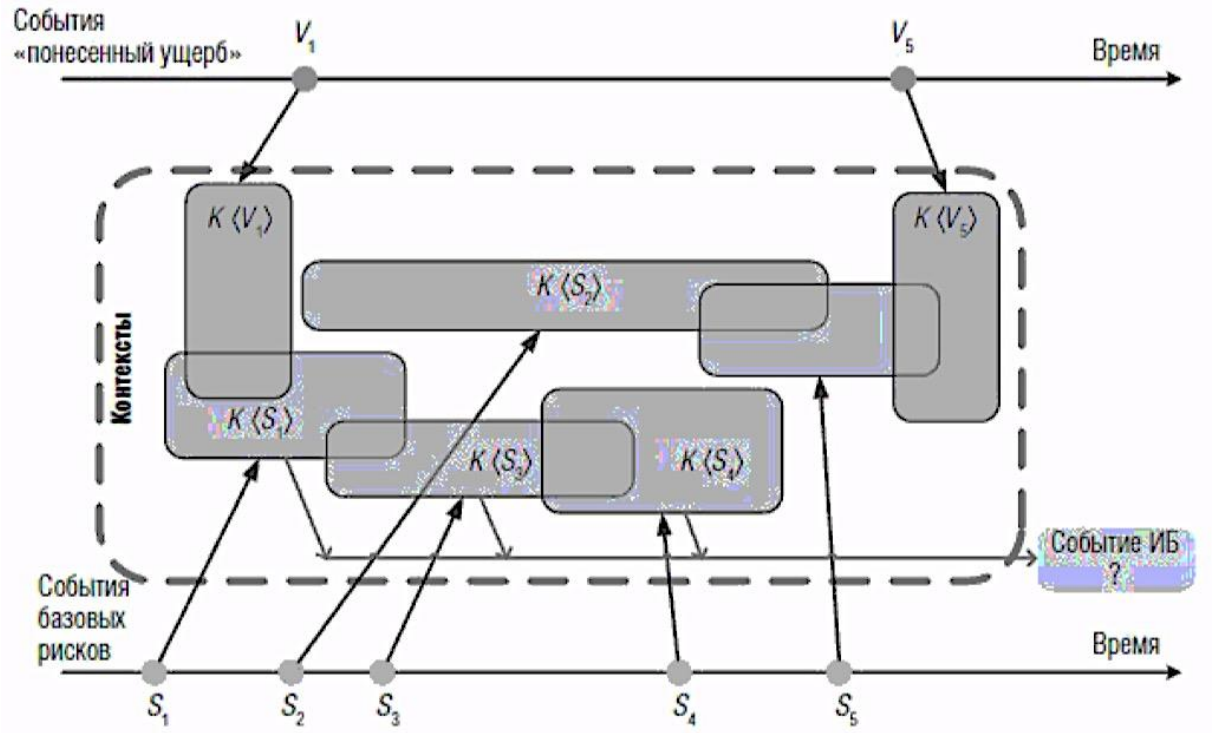


Рисунок 1.4 – Контекстная зависимость событий базовых рисков [5]

Связи событий могут быть неочевидными, особенно в случае понесенных ущербов и событий базовых рисков. В общем случае они

устанавливаются в результате расследования. Идентифицированная таким образом цепочка с сильными связями будет отображать цель и примененный способ ее реализации для нанесения ущерба. Описанные выше процедуры установления контекста базовых рисков организации в ее информационной сфере и «связывания» их с событиями ИБ являются основой построения модели ИБ организации. Однако практическая их реализация требует более детального рассмотрения проблем идентификации событий ИБ, управления ИБ, систематизации, оценивания, анализа и обобщения получаемой информации о состоянии организации и ее информационной сферы [5].

Возникновение событий ИБ обусловливает ряд следующих значимых факторов [5]:

а) неполная, недостоверная и несвоевременная внутренняя отчетность в организации и связанный с ней конфликт интересов: участвующие субъекты не заинтересованы в предоставлении отчетности, ухудшающей их статус в организации;

б) наличие стохастической составляющей (областей неформализованной деятельности), исключающей какие-либо формы контроля за деятельностью;

в) несовершенство ролей, ответственностей и организационных политик в организации и связанная с ними инсайдерская деятельность;

г) злоумышленная активность персонала;

д) противоборство организации за заимствуемые ресурсы с внешними субъектами;

е) организационное, функциональное и информационное несовершенство информационной сферы организации;

ж) слабости менеджмента в части накопления, обобщения, применения опыта для достижения целей организации;

з) неспрогнозированные изменения негативно влияющих факторов внешней среды, которые привели к увеличению базовых рисков.

Риски ИБ, реализуясь, искажают (модифицируют) тем или иным способом информационную сферу организации образования, которая, в свою очередь, один из источников (среда) факторов базовых рисков, т. е. некоторая сущность, осуществляющая «перенос» рисков ИБ в базовые риски. Эмпирическое знание о рисках основывается только на реальной фактуре, на том, что идентифицированные нами причинно-следственные связи и отношения между объектами и субъектами процесса реально происходили и наблюдались в объеме, достаточном для вывода о том, что наблюдаемое состояние процесса есть следствие (последствие), и в какой мере, тех или иных произошедших событий. Накопление эмпирических знаний формализуется в рамках модели Деминга – Шухарта (рисунок 1.5), предполагающей определенный цикл шагов, собранных в схему непрерывных циклических улучшений [5].

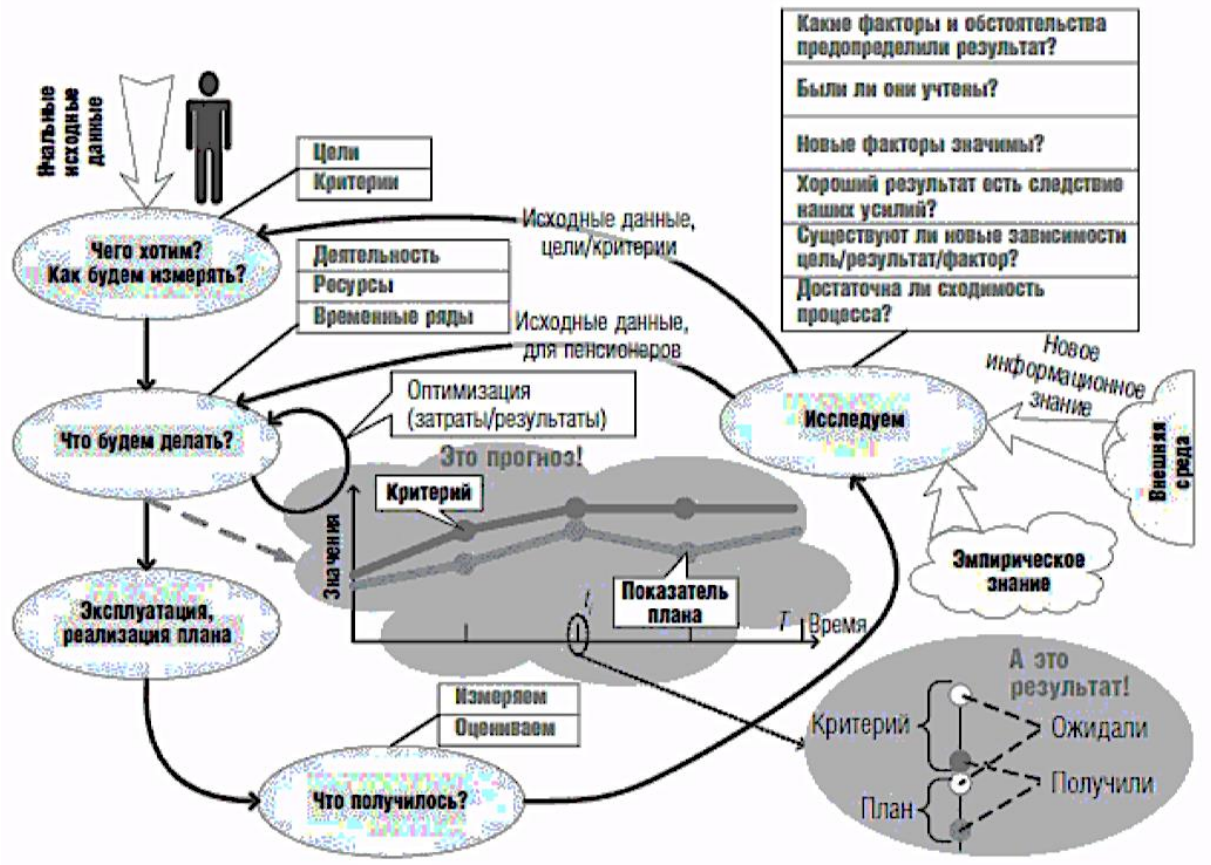


Рисунок 1.5 – Информационные сущности модели Деминга-Шухарта [5]

В рамках схемы модели Деминга-Шухарта сначала выдвигается (формулируется) некоторое предположение о достижимости определен-

ного результата в рамках фиксированного плана деятельности по выявлению и оценке эффективности информационной защиты в образовательной организации, в частности. Величина несоответствия заявленного и полученного результата в конечном счете зависит от объема использованной информации, глубины и детальности проводимого анализа, а также от природы исследуемого процесса. В ситуации, когда результат в основном зависит от управляемых факторов, предсказуемость будет очень точной, и, наоборот, при зависимости от внешних неуправляемых факторов процесс сойдется на некоторой величине неулучшаемой погрешности [5].

Основные фазы модели Деминга – Шухарта (модель Деминга) следующие (рисунок 1.6) [5]:

– «планирование»: установление целей и процессов, необходимых для выработки результатов в соответствии с требованиями клиентов и политиками организации;

– «выполнение» («реализация»): реализация запланированных процессов и решений;

– «проверка»: контроль и измерение процессов и производимых продуктов относительно политик, целей и требований к продукции и отчетность о результатах;

– «действие» («совершенствование»): принятие корректирующих и превентивных мер для постоянного совершенствования функционирования процесса.

Особенности и условия внедрения и применения модели Деминга уместны для любого вида менеджмента в организации (управленческого, производственного, обслуживающего, ресурсного и т. п.).

В общем случае этап планирования СИБ в соответствии с требованиями стандарта [11] может включать следующие 10 шагов, представленных в таблице 1.1, реальное наполнение которых определяется самой организацией.

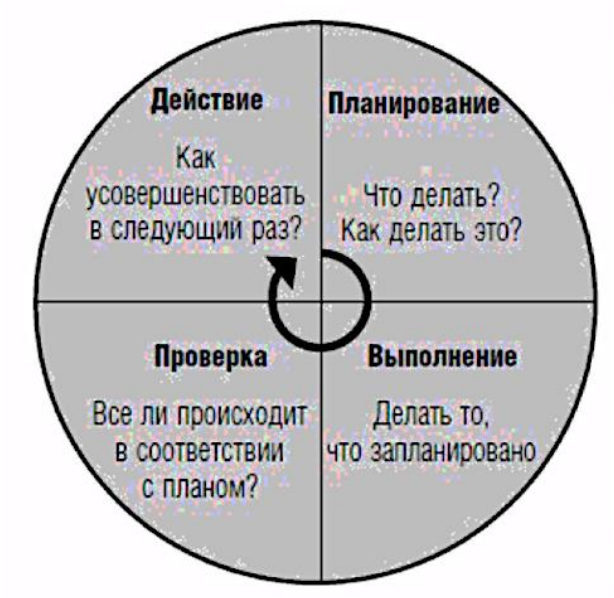


Рисунок 1.6 – Эталонная модель Деминга-Шухарта (модель Деминга) [5]

Таблица 1.1 Шаги при планировании СИБ [5]

№ п/п	Шаг
1	Определение сферы действия и границ системы менеджмента информационной безопасности в терминах специфики бизнеса, организации, местоположения, активов и технологии, включая подробности о любых исключениях из сферы действия и их обоснование
2	Определение политики системы менеджмента информационной безопасности в терминах специфики бизнеса, организации, местоположения, активов и технологии
3	Определение подхода организации к оценке риска
4	Идентификация рисков
5	Анализ и оценивание рисков
6	Идентификация и оценивание вариантов обработки риска
7	Выбор целей контроля и средств контроля для обработки рисков
8	Получение одобрение руководства по вопросу предлагаемых остаточных рисков
9	Получение санкционирования руководства для реализации и приведения в действие системы менеджмента информационной безопасности
10	Подготовка формулировки применимости требований из каталога требований стандарта

В основе методологии стандартной СИБ лежит риск-ориентированный подход. Он основывается на предположении того, что оценка риска делает возможным понимание следующих вопросов, связанных с информационными активами, которыми владеет организация:

– каковы актуальные угрозы и их источники – факторы риска;

– как часто возможно возникновение угроз;

– сколько и какие информационные активы могут подвергнуться влиянию при возникновении угрозы [5].

Важнейшим назначением оценки ИБ является создание информационной потребности для совершенствования ИБ. При этом могут решаться и другие цели проведения оценки ИБ, например [6]:

– определение степени соответствия установленным критериям отдельных областей обеспечения ИБ, процессов обеспечения ИБ, защитных мер;

– выявление влияния критических элементов (факторов) и их сочетания на ИБ организации;

– определение зрелости различных процессов обеспечения ИБ.

Системно-ориентированная оценка ИБ прозрачна и понятна, предоставляет полную информацию для совершенствования защитных мер. Но это возможно при условии существования доверенного процесса измерения и оценивания. К проблемам системно-ориентированной оценки относятся её трудоёмкость и невозможность использования полученной информации для прогнозирования развития ИБ организации. При процессно-ориентированной оценке ИБ процесс измерения и оценивания осуществляется подобным, как при системно-ориентированной оценке, образом. Однако целью процессно-ориентированной оценки ИБ является создание документа, описывающего политику ИБ организации, распределение обязанностей по обеспечению ИБ, обучение вопросам ИБ, обработка инцидентов, связанных с ИБ. При формировании оценки соответствия процессов управления ИБ может использоваться усреднение или свёртка частных показателей, относящихся к одному процессу управления ИБ, формирование оценки на основе модели предпочтений и другое. Процессно-ориентированная оценка ИБ рекомендуется, как основная для проверки системы управления ИБ. Целесообразным является и способ оценки ИБ, сочетающий системно-ориентированную оценку ИБ и процессно-ориентированную оценку ИБ. Применение системно-ориентиро-

ванной и процессно-ориентированной оценки ИБ при условии существования доверенного процесса измерения и оценивания позволяет:

1) сформировать прозрачную и понятную оценку системы обеспечения ИБ организации в целом: оценку защитных мер и процессов управления ИБ;

2) сформировать прогноз развития ИБ организации на основании полученной оценки процессов управления ИБ [6].

1.2. Методы и средств защиты конфиденциональной информации в образовательной организации

Разнообразие и количество средств защиты информации весьма велико. В наиболее общем виде их можно разделить на организационно-правовые и инженерно-технические, последние из которых включают [7;]:

– физические средства защиты информации;

– аппаратные средства;

– программные (в том числе криптографические).

Подбор технических мер защиты для использования в конкретной органи-зации опирается на концепцию информационной безопасности, принятую в регионе. Концепция обосновывает, что именно и каким образом необходимо за-щищать.

При построении системы защиты информации с использованием технических средств необходимо следовать определенным принципам [7]:

– использование только лицензированного программного обеспечения (далее – ПО);

– использование только совместимого ПО, все части системы должны быть совместимыми друг с другом;

– управляемость, легкость администрирования системы, минимальное ис- пользование сторонней технической поддержки;

– протоколирование и документирование любых действий пользователей, осуществляемых с файлами, содержащими конфиденциальную информацию, а также случаев несанкционированного доступа;

– затраты на организацию защиты информации должны быть соразмерны величине ущерба, наносимого собственнику информации.

Физические средства защиты информации – это любые механические, электрические и электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним. К ним относятся [7]:

– замки, в том числе электронные – один из простейших и эффективных способов физически ограничить доступ к чему-либо;

– экраны, жалюзи создают препятствия для визуального съема информации с систем обработки данных;

– системы контроля и управления доступом (СКУД) – задают правила до- ступа сотрудников к определенным помещениям;

– системы видеонаблюдения, видеорегистраторы – отслеживают перемещения работников, позволяют зафиксировать факт несанкционированного проникновения в защищаемые помещения;

– датчики, выявляющие движение или превышение степени электромагнитного излучения в зоне расположения защищаемого оборудования – по сути «бюджетная версия» предыдущего пункта.

Аппаратные средства защиты информации – это любые устройства, которые либо затрудняют несанкционированный съем информации, либо помогают обнаружить потенциальные каналы утечки информации. Это самый узкоспециализированный класс средств защиты информации.

Ведущий российский разработчик средств информационной безопасности – компания «СёрчИнформ», входит в НП «Руссофт», член АПКИТ, аккредитована в качестве ИТ-компании (рисунок 1.7) с бессрочным наличием лицензии ФТЭК (рисунок 1.8) на деятельность по разработке и производству средств защиты конфиденциальной информации, свидетельств о государственной регистрации программ для ЭВМ «Сёрч Информ SIEM», «КИБСёрчИнформ» – DLP-система и др. [7].

Архитектура DLP-системы «КИБСёрчИнформ» многомодульная, осуществляет перехват и анализ информации на двух уровнях: на сетевом и на хостовом. Сетевые модули располагаются на сетевом шлюзе на платформе NetworkSniffer и отвечают за сетевой перехват. Хостовые модули устанавливаются на рабочих станциях пользователей на платформе EndpointSniffer и осуществляют перехват информации в «конечных точках».

ВЫПИСКА
ИЗ РЕЕСТРА АККРЕДИТОВАННЫХ ОРГАНИЗАЦИЙ,
ОСУЩЕСТВЛЯЮЩИХ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

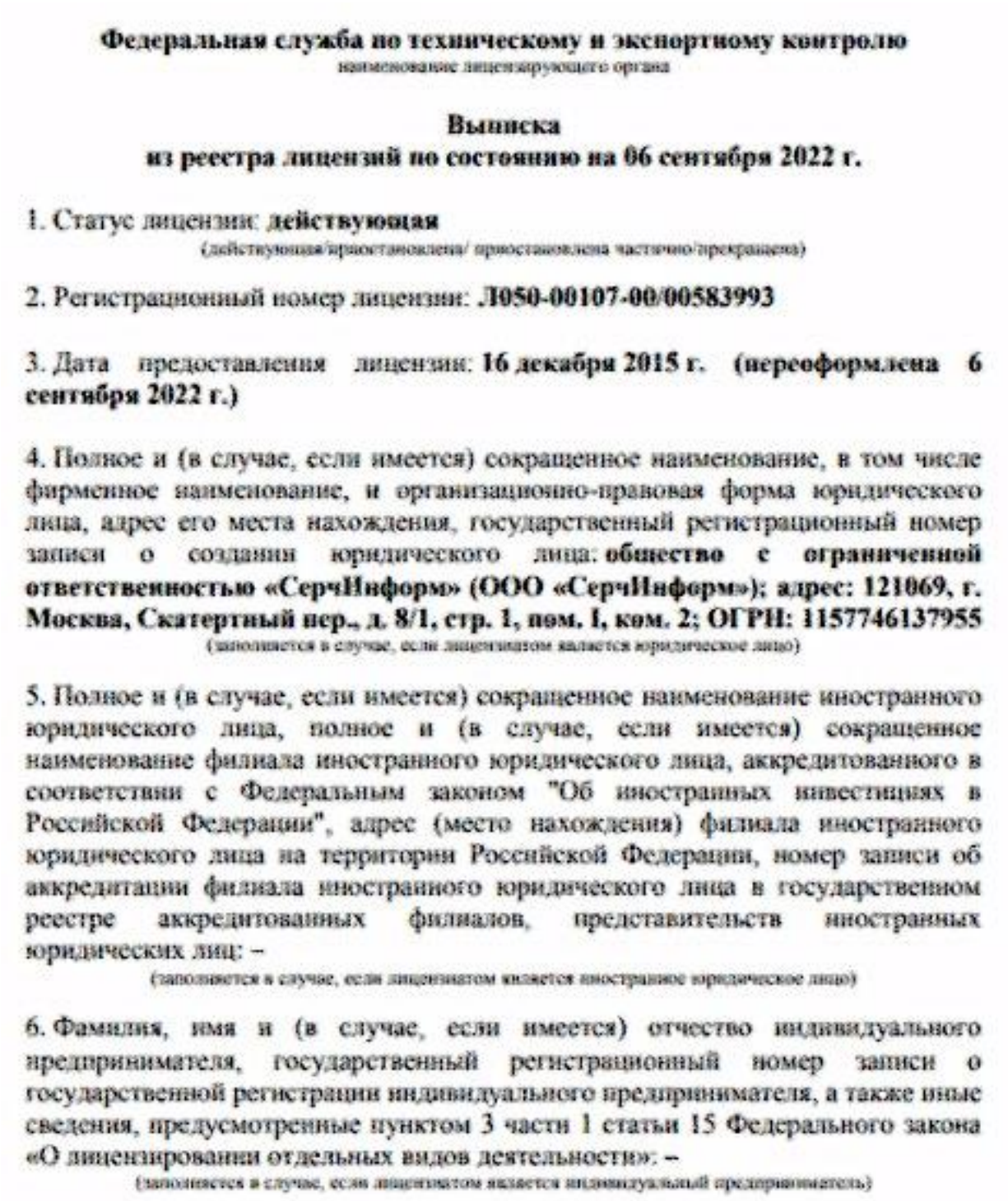
Настоящая выписка удостоверяет, что организация

Общество с ограниченной ответственностью «СерчИнформ»
(полное наименование организации)
27.02.2015, ул. Ефремова, д. 20, пом./офис I/2, г. Москва, 119048,
1157746137955
(дата, место, номер регистрации организации по ЕГРЮЛ)
получила государственную аккредитацию в соответствии с Положением о государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий, утвержденным постановлением Правительства Российской Федерации от 6 ноября 2007 г. № 758 «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий», о чем в реестр аккредитованных организаций внесена запись от «15» июля 2015 года за № 5236.

Заместитель Министра связи и массовых коммуникаций Российской Федерации — Р.Р. Исмаилов

М.П.

Рисунок 1.7 – Аккредитационная выписка компании «СёрчИнформ»



Федеральная служба по техническому и экспортному контролю

наименование лицензирующего органа

Выписка
из реестра лицензий по состоянию на 06 сентября 2022 г.

1. Статус лицензии: **действующая**

(действующая/приостановлена/ приостановлена частично/прекращена)

2. Регистрационный номер лицензии: **Л050-00107-00/00583993**

3. Дата предоставления лицензии: **16 декабря 2015 г. (переоформлена 6 сентября 2022 г.)**

4. Полное и (в случае, если имеется) сокращенное наименование, в том числе фирменное наименование, и организационно-правовая форма юридического лица, адрес его места нахождения, государственный регистрационный номер записи о создании юридического лица: **общество с ограниченной ответственностью «СерчИнформ» (ООО «СерчИнформ»); адрес: 121069, г. Москва, Скатертный пер., д. 8/1, стр. 1, пом. I, ком. 2; ОГРН: 1157746137955**

(заполняется в случае, если лицензиатом является юридическое лицо)

5. Полное и (в случае, если имеется) сокращенное наименование иностранного юридического лица, полное и (в случае, если имеется) сокращенное наименование филиала иностранного юридического лица, аккредитованного в соответствии с Федеральным законом "Об иностранных инвестициях в Российской Федерации", адрес (место нахождения) филиала иностранного юридического лица на территории Российской Федерации, номер записи об аккредитации филиала иностранного юридического лица в государственном реестре аккредитованных филиалов, представительств иностранных юридических лиц: –

(заполняется в случае, если лицензиатом является иностранное юридическое лицо)

6. Фамилия, имя и (в случае, если имеется) отчество индивидуального предпринимателя, государственный регистрационный номер записи о государственной регистрации индивидуального предпринимателя, а также иные сведения, предусмотренные пунктом 3 части 1 статьи 15 Федерального закона «О лицензировании отдельных видов деятельности»: –

(заполняется в случае, если лицензиатом является индивидуальный предприниматель)

Рисунок 1.8 – Выписка из реестра лицензии компании «СёрчИнформ»

Помимо модулей, отвечающих за перехват информации, в состав DLP-системы входят серверные компоненты, обеспечивающие централизованное управление информацией и всеми компонентами системы. AlertCenter – «мозговой центр» всей DLP-системы, который опрашивает все модули и, при наличии в перехваченной информации заданных

ключевых слов, фраз или фрагментов текста, атрибутов документов, немедленно оповещает об этом офицеров безопасности. В DLP-системе адаптирована методика управления рисками BSI/ISO/GTS (рисунок 1.9), реализующая основу международных стандартов серии ISO 27000 с определением необходимые числовые показатели для количественной оценки рисков [7].

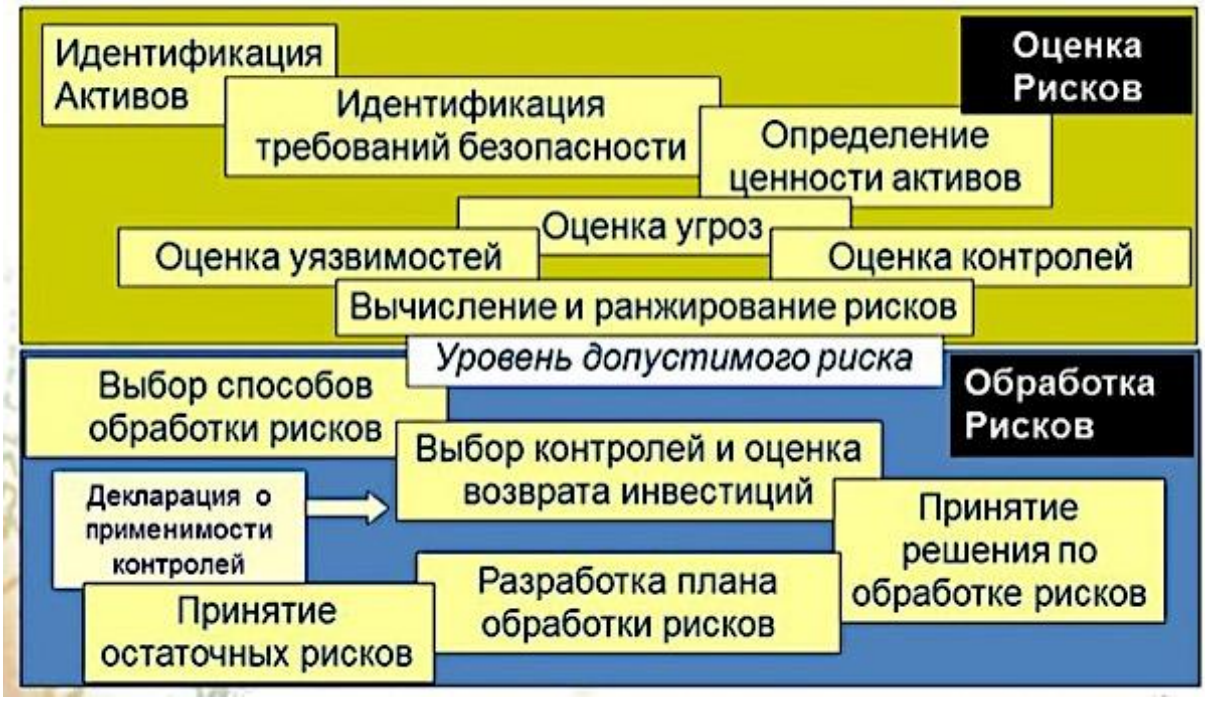


Рисунок 1.9 – Методика управления рисками BSI/ISO/GTS «СёрчИнформ»

Организационно-правовые средства и методы защиты информации связаны с изданием законодательных документов в области обеспечения информационной безопасности и созданием нормативно-правовых актов. Организационно-правовые методы защиты информации следует разделить отдельно на организационные и правовые. К организационным (административным) относятся меры, регулирующие процессы функционирования системы обработки, хранения данных, способы взаимодействия пользователей, позволяющие исключить угрозы безопасности. К ним следует отнести мероприятия, направленные на [8]:

– организацию хранения и учета документов;

– организацию уничтожения носителей информации;

– мероприятия, направленные на работу с персоналом;

– организацию контроля за работой кадров в том числе организация скрытого контроля;

– организацию пропускного режима и многое другое.

Правовые (законодательные) меры защиты информации – это действующие законодательные акты, регламентирующие порядок обращения, хранения и сохранности информации. К правовым методам защиты информации также относят нормативно-правовые акты, закрепляющие права и обязанности участников информационных отношений, осуществляющих поиск, обработку, хранение и обеспечение сохранности данных.

Помимо организационно-правовых методов защиты информации существуют инженерно-технические, включающие в себя программно-аппаратные средства защиты информации, криптографические и физические.

Многообразие классификационных характеристик позволяет рассматривать средства инженерно-технической защиты (ИТЗ) по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны служб безопасности. ИТЗ – это совокупность специальных органов, технических и программных средств и мероприятий по их использованию в интересах защиты конфиденциальной информации (рисунок 1.10) [9].

Очевидно, что такое деление средств защиты информации условно, т.к. они часто взаимодействуют и реализуются в комплексе в виде аппаратно-программных модулей с широким использованием алгоритмов закрытия информации (рисунок 1.11) [9].

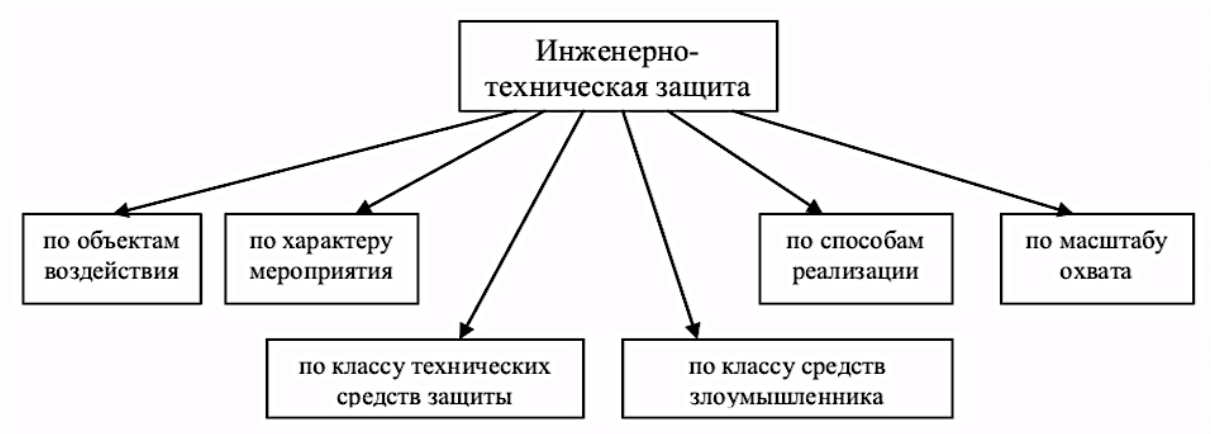


Рисунок 1.10 – Основная классификация ИТЗ

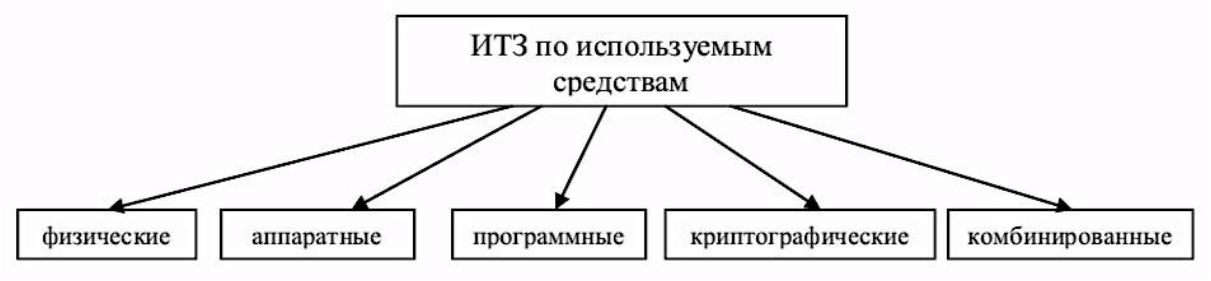


Рисунок 1.11 – Классификация ИТЗ по используемым средствам

Физические средства защиты информации – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, сооружения и организационные меры, предназначенные для создания препятствий на пути движения злоумышленников (рисунок 1.12) [9].

Рисунок 1.12 – Классификация физических систем защиты

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Системы ограждения и физической изоляции обеспечивают [9]:

– защиту объектов по периметру;

– защиту элементов зданий и помещений;

– защиту объемов зданий и помещений.

Системы контроля доступа реализуют:

– контроль доступа на охраняемые объекты;

– защиту документов, данных, фильм.

Запирающие устройства и хранилища включают:

– различные системы запирающих устройств (механические, электромеханические, электронные);

– различные системы шкафов и хранилищ;

Эти средства применяются для решения следующих задач:

– охрана территории предприятия и наблюдение за ней;

– охрана зданий, внутренних помещений и контроль за ними;

– охрана оборудования, продукции, финансов и информации;

– осуществление контролируемого доступа в здания и помещение.

Все физические средства защиты объектов можно разделить на три категории:

1. средства предупреждения;
2. средства обнаружения;
3. системы ликвидации угроз.

Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов − это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и др.). Средства пожаротушения относятся к системам ликвидации угроз.

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

– охранные и охранно-пожарные системы;

– охранное телевидение;

– охранное освещение;

– средства физической защиты.

К средствам физической защиты относятся:

– ограждение и физическая изоляция,

– запирающие устройства,

– системы контроля доступа.

К системам контроля доступа относятся:

– системы, использующие различные карты и карточки, на которых помещается кодированная или открытая информация о владельце,

– системы опознавания по отпечаткам пальцев,

– системы опознавания по голосу,

– системы опознавания по почерку,

– система опознавания по геометрии рук.

Все устройства идентификации могут работать как отдельно, так и в комплексе.

Программные и аппаратные средства защиты информации предназначены для обеспечения безопасности данных, находящихся в компьютерах, локальных сетях и информационных системах. К ним следует отнести [8]:

– антивирусную защиту;

– управление политикой безопасности;

– криптографическая защита;

– сетевая;

– идентификация и аутентификация пользователей.

Программные средства защиты информации можно разделить на следующие:

– *встроенные средства защиты информации;*

– *антивирусная программа* − программа для обнаружения компьютерных

– вредоносных программ и лечения инфицированных файлов, а также для профилактики − предотвращения заражения файлов или операционной системы вредоносным кодом;

– *межсетевые экраны* (также называемые брандмауэрами или файрволами). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода − это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой;

– *Proxy-servers* (proxy − доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью − маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях − например, на уровне приложения (вредоносные программы, код Java и JavaScript);

– *VPN* (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec;

системы защиты от НСД:

– средства собственной защиты, программным обеспечением;

предусмотренные общим

– средства защиты в составе вычислительной системы;

– средства защиты с запросом информации;

– средства пассивной защиты и т.д.

Внутренняя защита Windows 7 и 8 строится по модульному принципу. Встроенные средства защиты ОС – это не один продукт с единой консолью, а взаимодействующие компоненты (представлены в таблице 1.2). Условно их можно разделить на три зоны действия:

– первая часть модулей работает во время загрузки системы;

– вторая – во время ее работы;

– третья же активируется вручную и помогает дополнительно защитить операционную систему.

Современные методы и Физические средства защиты информации

Криптографические методы защиты информации относятся к наиболее мощным средствам. К основным еѐ элементам относится шифрование. Криптография имеет давнюю историю. В свое время она применялась в дипломатической и военной сферах. Криптографические средства защиты информации включают в себя изучение современной математики, физики, радиоэлектроники и других смежных наук.

Основная цель криптографических средств защиты информации – преобразование математическими методами информацию, для дальнейшей передачи по компьютерным сетям таким образом, чтобы они не были понятны третьим лицам. В связи с этим, суть криптографических средств защиты информации заключается в том, что даже при условии перехвата информации сторонними лицами, она не должна быть расшифрована в течение нескольких десятков лет.

В настоящее время криптография находится на стадии бурного развития. Этому способствуют развитие IT-технологий и большое количество молодых и талантливых ученых.

Таблица 1.2 – Сводная информация о встроенной защите Windows 7 и Windows 8

	Компонент	Windows 7	Windows 8
Загрузка системы	UEFI	—	+
	ASLR	+	+*
	ELAM	—	+
	Управление автозагрузкой	+	+*
	Вход в систему с помощью альтернативных паролей	—	+
Во время работы	Защитник	+	+*
	Брандмауэр	+	+
	SmartScreen	+	+*
	Запуск приложений в песочнице	—	+
	UAC	+	+
	Подсчёт сетевого трафика	—	
Дополнительно	Родительский контроль	+	+*
	Резервное копирование	+	+
	Шифрование	+	+
	Установка на накопитель	—	+
	Виртуализация	—	+

Далее рассмотрим физические средства защиты информации. К ним прежде всего следует отнести использование человеческих ресурсов и специальных технических средств защиты таких как видеонаблюдение, запирающиеся устройства и т.д. Практика показывает, что физические средства защиты – первый рубеж для злоумышленников. К физическим методам защиты информации следует отнести:

– механические преграды;

– средства для идентификации личности (сканеры сетчатки глаза, биомет-рии лица, отпечатков пальцев, геометрии руки и т.д.);

– датчики – ультразвуковые, инфокрасные, открытия окон и дверей.

Важно соблюдать правила и способы защиты информации, к

которым относятся:

– использование исключительно лицензионного программного обеспечения с возможностью своевременного обновления;

– применение современных антивирусных программ;

– необходимость удаления непрочитанных и подозрительных писем;

– не переходить по ссылкам на неизвестные ресурсы и не скачивать информацию;

– проводить резервное копирование файлов на внешние носители на тот случай, если смогут посягнуть на данные системы.

1.3. Проблема понимания сущности результата и результативности средств и методов защиты конфиденциональной информации в организации профессионального образования

В основе изучения эффективности (результативности) реализации оценки применения средств и методов защиты конфиденциональной информации в организации профессионального образования лежит проблема понимания сущности результата и его результативности для защиты конфиденциональной информации в организации профессионального образования. В связи с этим необходимо выделить следующие аспекты данной проблемы (рисунок 1.13):

– теоретический (что понимать под результатом?);

– методико-технологический (как достичь желаемых результатов?);

– рефлексивный (как оценивать и измерять результат?).

Прежде всего уточним понятие «результат» в комплексе с другими понятиями, имеющими отношение к результату образовательной деятельности.

Результат – объективная оценка достигнутой цели.

Образовательный результат – итог защиты конфиденциональной информации в организации профессионального образования.

Результативность – качественно-количественная характеристика итогов защиты конфиденциональной информации в организации профессионального образования, отражающая степень их соответствия обозначенным целям и существующим нормам.

Рисунок 1.13 – Аспекты проблемы результативности

Эффективность – понимается как результативность и представляет из себя качественно-количественную характеристику итогов защиты конфиденциональной информации в организации профессионального образования, отражающая степень их соответствия обозначенным целям и существующим нормам.

1.4. Подходы к оцениванию эффективности функционирования средств и методов защиты информации

В настоящее время выделяют три подхода к оцениванию эффективности функционирования средств и методов защиты информации (СиМЗИ) автоматизированных информационных системы (АИС) от несанкционированного доступа (СЗИ от НСД), в том числе в образовательной организации: экспертный, вероятностный, оценочный [18].

Существует множество мнений, которые определяют один из подходов приоритетнее другого, но единственным правильным выходом из сложившихся противоречий будет комплексное использование всех трех подходов к оценке эффективности функционирования СЗИ от НСД на этапах ее разработки. Поэтому предлагается использовать вероятностно-экспертный подход, основанный на математическом моделировании и экспертных оценках, который позво- ляет учитывать, как динамические, так и статические характеристики эффективности функционирования СЗИ от НСД.

Вероятностный подход используется при описании неизвестных (случайных событий), в частности, их вероятностно-временных характеристик; экспертный подход, основан на мнении экспертов в данной области и определяется достаточностью статических (практически не связанных со временем) параметров, определяющих эффективность функционирования СЗИ от НСД, к которым, например, можно отнести вычислительные ресурсы АИС и т.д., а оценочный – при определении предметной области, на первоначальном этапе разработки СЗИ от НСД [19].

Существующий ГОСТ-28806-89 трактует понятие качество СЗИ, как совокупность свойств, которые обуславливают его пригодность удовлетворять заданные или подразумеваемые потребности в соответствии с его предназначением [20]. В различных российских и международных стандартах [20–24], связанных с качеством (эффективностью функционирования СЗИ от НСД) определение качества функционирования СЗИ от НСД в АИС трактуется как степень (полноту выполнения) предъявляемых к ним требований. Качество СЗИ от НСД определяется в зависимости от того с какой целью разрабатывается данный программный продукт [25–26].

Квалиметрические измерения рассматривают качество, как ранжированную совокупность свойств, которые могут включать в себя свойства, представляющие более низкий уровень. Между всеми свойствами (показа-

телей) качества функционирования СЗИ от НСД существует взаимосвязь, которая позволяет комплексно оцениватьэти системы [27].

Проведенный анализ [20] позволил определить следующие основные свойства качества функционирования при разработке СЗИ от НСД на объектах информатизации: функциональность СЗИ от НСД; надежность СЗИ от НСД; удобство использования СЗИ от НСД; эффективность СЗИ от НСД; сопровождаемость СЗИ от НСД; мобильность СЗИ от НСД. Данный перечень свойств качества СЗИ от НСД в АИС в различных открытых литературных источниках трактуется шире [28–30], что в настоящее время при разработке СЗИ от НСД в АИС представляет собой значительную неопределенность и трудность с точки зрения сложной (иерархической) программной системы. Поэтому рассмотрим не оценку качества функционирования СЗИ от НСД, а оценку одного из свойств качества – эффективность функционирования и его атрибутов в соответствии нормативной документации ФСТЭК [31] при разработке СЗИ от НСД на объектах информатизации. Поэтому, при оптимальном выборе параметров и характеристик СЗИ от НСД предпочтение отдается измерению эффективности функционирования СЗИ от НСД в сравнении с ее различными вариантами реализации. Описание рассматриваемого свойства можно найти в теории эффективности сложных систем и процессов, так как СЗИ от НСД в АИС является сложной динамической системой, и каждая операция имеет четкую поставленную цель.

Под эффективностью функционирования СЗИ от НСД следует понимать степень соответствия результатов защиты информации в АИС, относительно поставленной цели при разра- ботке СЗИ от НСД [32]. В настоящее время существует множество понятий эффективности функционирования СЗИ от НСД и их интерпретаций, значительные расхождения имеют даже место быть в нормативных документах, поэтому стоит максимально осторожно оперировать данным определением и его смысловым значением [33–35].

При эксплуатации СЗИ от НСД эти системы, как правило, на свое функционирование в АИС требуют значительных вычислительных ресурсов, то при еѐ разработке необходимо найти разумный компромисс (с точки зрения вычислительных ресурсов) между функционированием СЗИ и АИС по своему прямому предназначению, к которым относятся (обработка, хранение и передача конфиденциальной информации). Возникает вопрос, каким способом необходимо провести оценку их эффективности функционирования? Чтобы на него ответить необходимо оценивать результаты выполняемых операций СЗИ от НСД и сопоставлять их с поставленными задачами и затратами, требуемыми для их реализации в АИС, поскольку проблема состоит в выборе лучшего из сравниваемых вариантов функционирования СЗИ от НСД. Под показателем эффективности функционирования СЗИ от НСД понимается мера степени соответствия реального результата функционирования СЗИ от НСД требуемому [23]. Каждый показатель эффективности функционирования характеризует достаточность определенного свойства СЗИ от НСД. При разработке СЗИ от НСД возникают сложности в ее оценки эффективности функционирования, а именно не все характеристики подвергаются оценке. В следствие этого, проанализируем показатели эффективности функционирования СЗИ от НСД и сопоставим их с недостатками, возникающими при разработке СЗИ от НСД в АИС, чтобы учесть все свойства, влияющие на работоспособность в целом АИС. Существует множество мнений относительно выбора атрибутов (показателей) оценки эффективности функционирования в СЗИ от НСД, приведенных в таблице 1.3.

Перечисленные атрибуты (показатели) эффективности функционирования могут классифицироваться как частные, подробнее этот вопрос освещен в [29]. Стоит заметить, что смысловые значения показателей эффективности функционирования СЗИ от НСД (таблица 1.3) принципиально схожи. К недостаткам применения СЗИ от НСД на объектах информатизации АИС критического применения можно отнести [19] (таблтца 1.4):

1. Оптимальность программного кода. В связи с тем, что СЗИ от НСД представляет собоӣ комплекс программных средств защиты информации (включая организационные меры), то и разрабатываемыӣ программныӣ код должен быть максимально оптимизированс точки зрения оптималь-ности использования ресурсов АИС.

Таблица 1.3 – **Атрибуты оценки эффективности функционирования системы защиты информации от несанкционированного доступа**

Источник Source	Атрибут свойства эффективности Attribute of the performance property
ISO/IEC 9126	*Временная эффективность* – свойство, характеризующее поведение АИС, включая и СЗИ от НСД, как при разработке, так и эксплуатации; *Ресурсоемкость* – свойство, характеризующее поведение используемых ресурсов АИС, включая и СЗИ от НСД, как при разработке, так и при их эксплуатации; *Согласованность* – свойство, характеризующее количество функций СЗИ от НСД не соответствующим стандартам. [8-11]
ГОСТ 28806	*Времяемкость* – совокупность свойств СЗИ от НСД, характеризующихся обеспечением при его функционировании временем реакции на запросы, на скорость обработки данных и на пропускную способность; *Ресурсоемкость*–совокупность свойств СЗИ от НСД, характеризующихся объемом используемых при его функционировании вычислительных ресурсов АИС и продолжительности их использования. *Функциональность* – совокупность свойств СЗИ от НСД, определяемая наличием и конкретными особенностями защитных функций, способных удовлетворять заданные или подразумеваемые потребности в защите информации на объектах информатизации [7]
ГОСТ 25010	*Результативность* – точность и полнота, с которой достигается цель функционирования СЗИ от НСД; *Производительность* – связь точности и полноты достижения пользователями целей с израсходованными вычислительными ресурсами АИС [22]
Липаев В.В.	*Временная эффективность*–свойство СЗИ от НСД, характеризующее требуемое время отклика и обработки заданий, а также производительность решения задач защиты информации с учетом количества используемых вычислительных ресурсов АИС в установленных условиях; *Используемость ресурсов*–степень загрузки доступных вычислительных ресурсов АИС в установленных условиях эксплуатации СЗИ от НСД. [14]
Боем Б.	*Рациональность*–рассматривается с точки зрения оптимальности разработки СЗИ от НСД; *Доступность*–рассматривается как селективность использования ее компонент, имеется в ввиду, что при изменении какой-либо характеристики, пользователь должен иметь доступ к необходимым данным.[15]
Петухов Г.Б.	*Результативность*–характеризуется результатом достижения цели функционирования СЗИ от НСД на объектах информатизации; *Ресурсоемкость*–характеризуется расходомвсех видов вычислительных ресурсов АИС, необходимых для проведения операции и достижения ею цели, функционирования по прямому назначению; *Оперативность*–характеризуется расходом операционного времени АИС, т.е. времени, потребного для достижения цели функционирования СЗИ от НСД. [4]
Черников Б.В.	*Уровень автоматизации* – характеризуется рациональностью функциональной структуры СЗИ от НСД, а именно с точки зрения взаимодействия с ней пользователя и использования вычислительных ресурсов АИС; *Временная эффективность* – способность СЗИ от НСД выполнять заданные действия за определенный интервал времени; *Ресурсоемкость* – минимально необходимые вычислительные ресурсы для эксплуатации СЗИ от НСД. [16]
Макколл Дж.А.	*Эффективность исполнения* – характеризуется минимальным временем функционирования СЗИ от НСД. *Эффективность хранения* – характеризуется эффективным доступом (минимальным временем) к информации, хранящейся в АИС. [23-24]
FEA Consolidated Reference Model Document	*Производительность* – свойство, характеризующее АИС или ее приложения с точки зрения времени отклика, интероперабельности, доступности пользователей и улучшения технических возможностей или характеристик; *Результативность* – степень удовлетворенности пользователей соответствующим приложением или системой, независимо от того, соответствует ли они требованиям пользователя, и их влияние на производительность операций.[25]

2. Отсутствие возможности исследовать эти системы в динамическом (временном) диапазоне.

3. Зависимость ресурсоёмкости СЗИ от НСД от вычислительных ресурсов АИС, к которым можно отнести процессорное время, оперативную память и дисковое пространство. Ограниченность перечисленных ресурсов АИС оказывает непосредственное влияние на время выполнения защитных функций СЗИ от НСД, и как следствие несоответствие предъявляемым к ней требованиям.

Таблица 1.4 – **Атрибуты оценки эффективности функционирования системы защиты информации от несанкционированного доступа**

Показатель Index	Смысловое значение показателя The meaning of the indicator	Недостаток Drawback
$V_{ВЭСЗИ}$ Временная эффективность функционирования СЗИ от НСД	Способность СЗИ от НСД соответствовать заявленным к ним требованиям (с точки зрения временных параметров их функционирования), а также находить разумный компромисс между функционированием АИС по прямому предназначению и СЗИ от НСД.	1)-3)
$V_{РСЗИ}$ Ресурсоемкость СЗИ от НСД	Аналогично предыдущему	3)
$V_{ОСЗИ}$ Оптимальность программного кода СЗИ от НСД	Корректность программного кода СЗИ от НСД	1) и 5)
$V_{ФСЗИ}$ Функциональность СЗИ от НСД	Способность СЗИ от НСД при ее разработке, соответствовать предъявляемому уровню секретности, относительно ее функциональных компонентов. Данный показатель не соответствует недостаткам, так как процедура является традиционной.	-
$V_{УСЗИ}$ Моральное старение СЗИ от НСД	Способность СЗИ от НСД выполнять свои целевые функции по истечении определенного интервала времени, связанного с жизненным циклом функционирования СЗИ от НСД в АИС	1)-5)
$V_{ИЗСЗИ}$ Изменяемость СЗИ от НСД	Возможность изменения (с точки зрения уменьшения ее защитных функций) в связи с модификацией существующего ПО АИС.	5)

4. Недостатком будет являться полная или частичная неприспособленность СЗИ от НСД выполнять возложенные на нее задачи, т.к. моральное старение СЗИ от НСД будет характеризоваться частичной или полной непригодностью адекватно реагировать на существующие деструктивные воздействия на информационный ресурс АИС.

5. Изменение структуры АИС с точки зрения программного и технического обеспечения этих систем, могут оказывать влияние на выполнение защитных функций СЗИ от НСД в АИС. В качестве примера можно

привести дублирование защитных функций СЗИ от НСД антивирусными программными средствами.

Для устранения приведенных недостатков, введены соответствующие показатели эффективности функционирования СЗИ от НСД, с помощью которых можно оценить реальную эффективность функционирования этих систем, приведенные в таблице 1.4.

Представленные показатели (атрибуты) можно структурировать в зависимости от эксплуатации СЗИ от НСД, в зависимости от имеющегося количества ресурсов АИС и от необходимого количества функций защиты СЗИ от НСД (рисунок 1.14).

Рисунок 1.14 – **Структурная схема показателей эффективности функционирования СЗИ от несанкционированного доступа в АИС**

Показатели эффективности функционирования СЗИ от НСД представлены не единственной величиной, поэтому представим ее в векторной форме (1).

$$V = V_{ВЭСЗИ}, V_{РСЗИ}, V_{ОСЗИ}, V_{ФСЗИ}, V_{УСЗИ}, V_{ИЗСЗИ}. \quad (1)$$

Из них частные показатели эффективности функционирования $V_{РСЗИ}, V_{ОСЗИ}, V_{ФСЗИ}$, $V_{УСЗИ}$, $V_{ИЗСИ}$ отражают адекватность типовой СЗИ от НСД требованиям по полноте имеющегося функционала СЗИ от НСД. Расчет данных показателей осуществляют на основе эвристических методов путем определения адекватности СЗИ от НСД предъявляемым к

ней требованиям на основе анализа её технической документации. Расчет и измерение данных показателей эффективности функционирования типовой СЗИ от НСД в АИС производится по соответствующей качественной шкале в виде булевонезависимых переменных, где 1 – значение данного показателя соответствует заявленному свойству СЗИ от НСД и можно интерпретировать как соответствие предъявляемым требованиям, а 0 – значение данного показателя не соответствует заявленному свойству СЗИ от НСД, и можно интерпретировать как несоответствие предъявляемым требованиям, где ***s*** стратегия функционирования СЗИ от НСД.

Динамический (количественный) показатель эффективности функционирования при разработке типовой СЗИ от НСД в АИС «временная эффективность функционирования СЗИ от НСД» $V_{ВЭСЗИ}$ является отражением вероятностно-временных характеристик динамики функционирования этих систем, которые оказывают прямое и непосредственное влияние на эффективность функционирования АИС по прямому назначению:

$$V_{РСЗИ}(s), V_{ОСЗИ}(s), V_{ФСЗИ}(s), V_{УСЗИ}(s), V_{ИЗСЗИ}(s) = \begin{cases} 1, \textit{соответствует свойству}; \\ 0, \textit{не соответствует свойству}. \end{cases}$$

Реализация функций СЗИ от НСД, как показывает опыт эксплуатации, ведет к значительному отвлечению вычислительных ресурсов АИС (процессорного времени и оперативной памяти), что приводит к увеличению времени отклика в этих системах и является неприемлемым для выполнения АИС своих функций по прямому назначению. Поэтому при разработке СЗИ от НСД техтребования задаются на этапе 6 [19] в виде области допустимых значений, которые могут быть получены в результате натурного эксперимента, а также при имитационном моделировании.

$$V_{ВЭСЗИ}(s) = \begin{cases} 1, \textit{если } V_{ВЭСЗИ}(s) \le V^{тр}; \\ 0, \textit{если } V_{ВЭСЗИ}(s) > V^{тр}. \end{cases}$$

Таким образом, динамический показатель эффективности функционирования $V_{ВЭСЗИ}$ СЗИ от НСД в АИС определяется как вероятность свое-

временной реализации функционала СЗИ от НСД, основанного на выбранной стратегии и описывается математическим выражением:

$$V_{ВЭСЗИ}(s) = P(s(\tau) \le s(\tau^{mp})).$$

где □□– время выполнения СЗИ от НСД своего функционала в АИС, □^{mp} – максимально допустимое время выполнения своего функционала в АИС, указанного в технической документации по эксплуатации в разделе «защита информации от НСД». Оценка данного показателя эффективности функционирования типовой СЗИ от НСД в АИС необходимо осуществить на основе анализа разработанной сети Петри как марковской цепи с конечным числом состояний, причем последнее является поглощающим [18]. Проведенный анализ одного из качественных свойств эффек- тивности функционирования, позволил учесть все характеристики, прописанные в нормативных документах и научной литературе, что позволило учесть нюансы, связанные с выбором показателей эффективности функционирования СЗИ от НСД.

Выводы по главе 1

Методический подход к оценке эффективности защиты информации в информационной сфере образования позволяет заключить, что наиважнейшими особенностями в сфере информационной безопасности и основными её задачами является насущная необходимость сохранения свойств информации, обеспечения целостности данных, их конфиденциальности и регламентируемой доступности. Представить в современных условиях образовательную организацию без защищаемой информации и информационных технологий невозможно. Основным шагом оптимизации затрат на систему защиты информации современной организации является, прежде всего, анализ рисков информационной безопасности и угроз с выявлением наиболее критических факторов, оказывающих наиболее отрицательное влияние на информационную безопасность средств и методов защиты информации образовательной организации

Главной задачей информационной безопасности образовательной организации является управление рисками нарушения информационной целостности, а обеспечение – это главный критерий качества выполнения информационных процессов, в том числе иинформационной инфраструктурой образовательной организации в целом. Одним из наиболее немаловажных процессов при организации системы защиты информации образовательной организации является минимизация затрат. Для СПО и ВУЗов, с учетом необходимости оптимизации затрат на организацию системы защиты конфиденциальной информации образовательной организации, наиболее приемлемым является комбинированный метод, заключающийся в том, что необходимо экранировать лишь определенные подразделения от внешних воздействий, организовать доступ пользователей к информационной системе и к открытым сетям автоматизированного рабочего места также только лишь при необходимости.

Главная проблема информационной сферы образования – проблема установления рационального баланса между эффективностью и информационной безопасностью образовательной организации. Это приводит к необходимости создания информационной инфраструктуры в сфере образования с соответствующими техническими и программными средствами обработки данных, т.к. для её успешности, даже не говоря о повышении её эффективности, необходимо учитывать большее число факторов и невозможность проверки достоверности всех используемых данных. Содержательно и формально критическую часть информационной системы организации, в т.ч. образовательной, способную наносить ущербы и приводить к негативным последствиям для целей организации, определяет пятёрка риск-факторов «А, П, И, С, Р») – активы (А), процессы (П), инструменты (И), субъекты (С) и роли (Р). У базовых рисковых событий всегда через их риск-факторы может быть идентифицирован их контекст в информационной сфере организации.

Глава 2. **ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ СРЕДСТВ И МЕТОДОВ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**

2.1. Процесс определения эффективности защиты информации

Процесс определения эффективности средств и методов защиты информации (СиМЗИ), в том числе конфиденциальной информации, начинается с выбора и обоснования критериев. Затем переходят к подбору или разработке методик расчета показателей эффективности.

На практике используются следующие виды критериев [10]:

– типа «эффект–затраты», характеризуемые соотношением затрат на реализацию механизма защиты и полученного эффекта (экономическая эффективность);

– позволяющие оценивать качество СиМЗИ;

– позволяющие определить достаточность применяемых мер защиты.

В настоящий момент методики расчета показателей эффективности в нормативных документах не описаны. Соответственно решение данной задачи может производиться с помощью различных средств, таких как методы моделирования процессов защиты информации, экспертные оценки, статистический анализ, метод минимизации рисков и т. д.

Ни один из методов не лишен недостатков, поэтому на практике следует их комбинировать.

Расчет значений показателей оценки выполнения требований к технологическим мерам защиты информации по направлению «Технологические меры» осуществляется для следующих показателей [11]:

$E_{ТМП}$ – оценка, характеризующая выполнение требований в рамках процесса планирования применения мер защиты информации;

$E_{ТМР}$ – оценка, характеризующая выполнение требований в рамках процесса реализации мер защиты информации;

$E_{ТМК}$ – оценка, характеризующая выполнение требований в рамках процесса контроля применения мер защиты информации;

$E_{ТМС}$ – оценка, характеризующая выполнение требований в рамках процесса совершенствования применения мер защиты информации;

$E_{ТМ}$ – обобщающий показатель уровня оценки соответствия по направлению «Технологические меры».

Значение оценки, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации ($E_{ТМП}$), рекомендуется рассчитывать по формуле:

$$E_{ТМП} = \frac{\sum_{i=1}^{N} E_{По i} + \sum_{i=1}^{N} E_{Пп i}}{2N},$$

где i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{По i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации по вопросу определения области применения меры защиты информации;

$E_{Пп i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации по вопросу определения порядка применения меры защиты информации.

В рамках процесса планирования применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Определена ли область применения меры защиты информации?»;

«Определен ли порядок применения меры защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («определено»);

0 – «нет» («не определено»).

Значение оценки, характеризующей выполнение требований в рамках процесса реализации мер защиты информации ($E_{ТМР}$), рекомендуется рассчитывать по формуле:

$$E_{ТМР} = \frac{\sum_{i=1}^{N} E_{Рмi}}{N},$$

где i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{Рмi}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса реализации мер защиты информации.

Оценку требований рекомендуется производить путем присвоения им следующих значений с точки зрения полноты их реализации:

1 – «да» («постоянно», «всегда», «в полном объеме»);

0,75 – «в основном «да» («почти постоянно», «почти всегда», «почти в полном объеме»);

0,5 – «частично» («отчасти да», «не всегда», «в некоторых случаях»);

0,25 – «в основном «нет» («непостоянно», «почти никогда»);

0 – «нет» («никогда», «ни в каких случаях»).

Значение оценки, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации ($E_{ТМК}$), рекомендуется рассчитывать по формуле:

$$E_{ТМК} = \frac{\sum_{i=1}^{N} E_{Коi} + \sum_{i=1}^{N} E_{Кпi} + \sum_{i=1}^{N} E_{Кзi}}{3N},$$

где i – порядковый номер оцениваемых требований;

N – общее количество требований;

E_{Koi} – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля области применения меры защиты информации;

E_{Kni} – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля надлежащего применения меры защиты информации;

$E_{Kзi}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля знаний работников финансовой организации в части применения меры защиты информации.

В рамках процесса контроля применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Обеспечен ли контроль области применения меры защиты информации?»;

«Обеспечен ли контроль надлежащего применения меры защиты информации?»;

«Обеспечен ли контроль знаний работников финансовой организации в части применения меры защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («контроль обеспечен»);

0 – «нет» («контроль не обеспечен»).

Значение оценки, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации ($E_{ТМС}$), рекомендуется рассчитывать по формуле:

$$E_{ТМС} = \frac{\sum_{i=1}^{N} E_{Сиi} + \sum_{i=1}^{N} E_{Сиi}}{2N},$$

где *i* – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{Сиi}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса совершенствования приме-нения мер защиты информации по вопросу анализа необходимости совер-шенствования меры защиты информации в случае обнаружения инци-дентов защиты информации;

$E_{Сиi}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса совершенствования приме-нения мер защиты информации по вопросу анализа необходимости совер-шенствования меры защиты информации в случае обнаружения недос-татков в рамках контроля применения мер защиты информации.

В рамках процесса совершенствования применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Осуществляется ли анализ необходимости совершенствования меры защиты информации в случае обнаружения инцидентов защиты информации?»;

«Осуществляется ли анализ необходимости совершенствования меры защиты информации в случае обнаружения недостатков в рамках контроля применения мер защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («анализ совершенствования осуществляется»);

0 – «нет» («анализ совершенствования не осуществляется»).

Значение обобщающего показателя уровня оценки соответствия по направлению «Технологические меры» ($E_{ТМ}$) рекомендуется рассчитывать по формуле:

$$E_{ТМ} = 0{,}2E_{ТМП} + 0{,}4E_{ТМР} + 0{,}25E_{ТМК} + 0{,}15E_{ТМС},$$

где $E_{ТМП}$ – значение оценки, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации;

$E_{ТМР}$ – значение оценки, характеризующей выполнение требований в рамках процесса реализации мер защиты информации;

$E_{ТМК}$ – значение оценки, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации;

$E_{ТМС}$ – значение оценки, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации.

Рекомендации по расчету значений показателей оценки выполнения требований к программному обеспечению автоматизированных систем и приложений защиты информации обычно включают:

1. Расчет значений показателей оценки выполнения требований к программному обеспечению автоматизированных систем и приложений защиты информации.

2. Расчет по направлению «Безопасность программного обеспечения» значений следующих показателей:

$E_{ПОП}$ – оценка, характеризующая выполнение требований в рамках процесса планирования применения мер защиты информации;

$E_{ПОР}$ – оценка, характеризующая выполнение требований в рамках процесса реализации мер защиты информации;

$E_{ПОК}$ – оценка, характеризующая выполнение требований в рамках процесса контроля применения мер защиты информации;

$E_{ПОС}$ – оценка, характеризующая выполнение требований в рамках процесса совершенствования применения мер защиты информации;

$Е_{ПО}$ – обобщающий показатель уровня оценки соответствия по направлению «Безопасность программного обеспечения».

3. Значение обобщающей оценки, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации $Е_{ПОП}$, рекомендуется рассчитывать по формуле:

$$Е_{ПОП} = \frac{\sum_{i=1}^{N} Е_{По i} + \sum_{i=1}^{N} Е_{Пп i}}{2N},$$

где i – порядковый номер оцениваемых требований;

N – общее количество требований;

$Е_{По i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации по вопросу определения области применения меры защиты информации;

$Е_{По j}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации по вопросу определения порядка применения меры защиты информации.

В рамках процесса планирования применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Определена ли область применения меры защиты информации?»;

«Определен ли порядок применения меры защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («определено»);

0 – «нет» («не определено»).

4. Значение оценки, характеризующей выполнение требований в рамках процесса реализации мер защиты информации ($Е_{ПОР}$), рекомендуется рассчитывать по формуле:

$$Е_{ПОР} = \frac{\sum_{i=1}^{N} Е_{Рмi}}{N},$$

где i – порядковый номер оцениваемых требований;

N – общее количество требований;

$Е_{РМi}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса реализации мер защиты информации.

Оценку требований рекомендуется производить путем присвоения им следующих значений с точки зрения полноты их реализации:

1 – «да» («постоянно», «всегда», «в полном объеме»);

0,75 – «в основном «да» («почти постоянно», «почти всегда», «почти в полном объеме»);

0,5 – «частично» («отчасти да», «не всегда», "в некоторых случаях»);

0,25 – «в основном «нет» («непостоянно», «почти никогда»);

0 – «нет» («никогда», «ни в каких случаях»).

5. Значение оценки, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации ($Е_{ПОК}$), рекомендуется рассчитывать по формуле:

$$Е_{ПОК} = \frac{\sum_{i=1}^{N} Е_{Коi} + \sum_{i=1}^{N} Е_{Кпi} + \sum_{i=1}^{N} Е_{Кзi}}{3N},$$

где i – порядковый номер оцениваемых требований;

N – общее количество требований;

E_{Koi} – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля области применения меры защиты информации;

E_{Kni} – значение оценки *i*-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля надлежащего применения меры защиты информации;

$E_{Kзi}$ – значение оценки *i*-й меры защиты информации, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации по вопросу контроля знаний работников финансовой организации в части применения меры защиты информации.

В рамках процесса контроля применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Обеспечен ли контроль области применения меры защиты информации?»;

«Обеспечен ли контроль надлежащего применения меры защиты информации?»;

«Обеспечен ли контроль знаний работников финансовой организации в части применения меры защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («контроль обеспечен»);

0 – «нет» («контроль не обеспечен»).

6. Значение оценки, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации ($E_{ПОС}$), рекомендуется рассчитывать по формуле:

$$E_{\text{пос}} = \frac{\sum_{i=1}^{N} E_{\text{Сн}i} + \sum_{i=1}^{N} E_{\text{Сн}i}}{2N},$$

где i – порядковый номер оцениваемых требований;

N – общее количество требований;

$E_{\text{Сн}i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации по вопросу анализа необходимости совершенствования меры защиты информации в случае обнаружения инцидентов защиты информации;

$E_{\text{Сн}i}$ – значение оценки i-й меры защиты информации, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации по вопросу анализа необходимости совершенствования меры защиты информации в случае обнаружения недостатков в рамках контроля применения мер защиты информации.

В рамках процесса совершенствования применения мер защиты информации оценку требований рекомендуется осуществлять по следующим вопросам:

«Осуществляется ли анализ необходимости совершенствования меры защиты информации в случае обнаружения инцидентов защиты информации?»;

«Осуществляется ли анализ необходимости совершенствования меры защиты информации в случае обнаружения недостатков в рамках контроля применения мер защиты информации?».

Оценку ответов на вопросы рекомендуется производить путем присвоения им следующих значений:

1 – «да» («анализ совершенствования осуществляется»);

0 – «нет» («анализ совершенствования не осуществляется»).

7. Значение обобщающего показателя уровня оценки соответствия по направлению «Безопасность программного обеспечения» ($Е_{ПО}$) рекомендуется рассчитывать по формуле:

$$Е_{ПО} = 0,2Е_{ПОП} + 0,4Е_{ПОР} + 0,25Е_{ПОК} + 0,15Е_{ПОС},$$

где $Е_{ПОП}$ – значение оценки, характеризующей выполнение требований в рамках процесса планирования применения мер защиты информации;

$Е_{ПОР}$ – значение оценки, характеризующей выполнение требований в рамках процесса реализации мер защиты информации;

$Е_{ПОК}$ – значение оценки, характеризующей выполнение требований в рамках процесса контроля применения мер защиты информации;

$Е_{ПОС}$ – значение оценки, характеризующей выполнение требований в рамках процесса совершенствования применения мер защиты информации.

2.2. Выбор мер защиты информации для их реализации в информационной системе образовательной организации

Выбор мер защиты информации для их реализации в информационной системе включает (рисунок 2.1):

– определение базового набора мер защиты информации для установленного класса защищенности информационной системы;

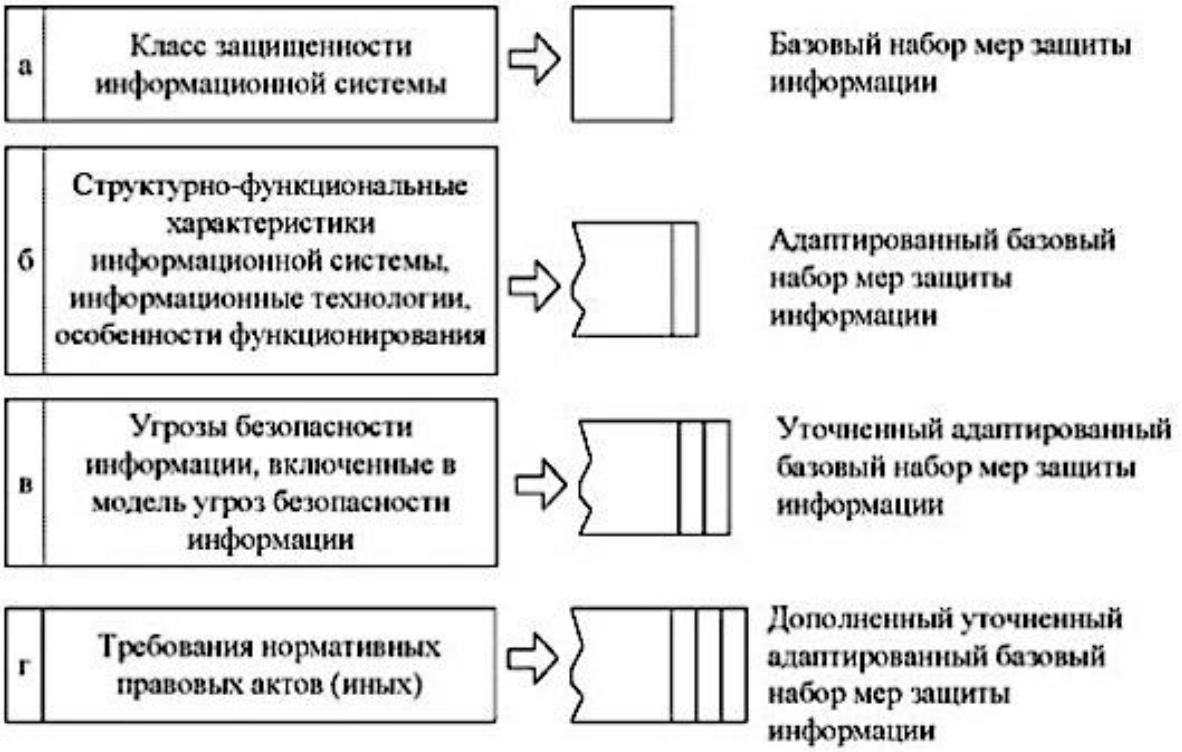


Рисунок 2.1 – Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе образовательной организации

– адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы;

– уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации для блокирования (нейтрализации) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

– дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты конфедициональных данных.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

Определение базового набора мер защиты информации для установленного класса защищенности информационной системы является первым шагом в выборе мер защиты информации, подлежащих реализации в информационной системе. Определение базового набора мер защиты информации основывается на классе защищенности информационной системы. Базовый набор мер защиты информации, выбранный в соответствии с классом защищенности информационной системы, подлежит адаптации применительно к структурно-функциональным характеристикам и особенностям функционирования информационной системы, уточнению в зависимости от угроз безопасности информации и при необходимости дополнению мерами защиты информации, включенными в иные нормативные правовые акты, нормативные и методические документы по защите информации.

Вторым шагом является изменение изначально выбранного базового набора мер защиты информации в части его максимальной адаптации применительно к структуре, реализации и особенностям эксплуатации информационной системы. При адаптации базового набора мер защиты информации учитываются:

– цели (обеспечение конфиденциальности, целостности и (или) доступности информации) и задачи защиты информации в информационной системе;

– перечень мероприятий проводимых оператором по обеспечению безопасности в рамках организации в целом;

– применяемые информационные технологии и структурно-функциональные характеристики информационной системы.

Адаптация базового набора мер защиты информации, как правило, предусматривает исключение мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе.

Требования к усилению регистрации событий безопасности:

1) в информационной системе должны обеспечиваться интеграция результатов мониторинга (*просмотра и анализа*) записей регистрации (аудита) из разных источников (журналов, хранилищ информации о событиях безопасности) и их корреляция с целью выявления инцидентов безопасности и реагирования на них;

2) в информационной системе обеспечивается интеграция процессов мониторинга (просмотра, анализа) результатов регистрации событий безопасности с результатами анализа уязвимостей, проводимого в с целью усиления возможностей по выявлению признаков инцидентов безопасности;

3) в информационной системе обеспечивается полнотекстовый анализ привилегированных команд;

4) обеспечивается анализ записанных сетевых потоков (дампов).

Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

– получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

– получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);

– контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению антивирусной защиты:

1) в информационной системе должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов);

2) в информационной системе должно обеспечиваться автоматическое обновление базы данных признаков вредоносных компьютерных вирусов (программ) на всех компонентах информационной системы;

3) в информационной системе должен обеспечиваться запрет изменений настроек системы обновления базы данных признаков вредоносных компьютерных программ (вирусов) на автоматизированных рабочих местах и серверах;

4) в информационной системе должна обеспечиваться возможность возврата (отката) к предыдущим обновлениям базы данных признаков вредоносных компьютерных программ (вирусов).

Требования к усилению средств обнаружения вирусов:

1) в информационной системе обеспечивается применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках, передаваемых в рамках сегмента (сегментов) информационной системы;

2) в информационной системе обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы;

3) обнаружение и реагирование (уведомление администратора безопасности, блокирование трафика и иные действия по реагированию) на компьютерные атаки в масштабе времени, близком к реальному;

4) в информационной системе защита информации, собранной и сгенерированной системой обнаружения вторжений, от несанкционированного доступа, модификации и удаления;

5) в информационной системе обеспечивается применение систем обнаружения вторжений уровня узла на автоматизированных рабочих местах и серверах информационной системы;

6) в информационной системе обеспечивается применение систем обнаружения вторжений на прикладном уровне базовой эталонной модели взаимосвязи открытых систем.

Требования к реализации анализа (контроля) защищенности информации: В информационной системе должны осуществляться выявление (поиск), анализ и устранение уязвимостей.

При выявлении (поиске), анализе (контроля) и устранении уязвимостей в информационной системе должны проводиться:

– выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

– разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

– анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

– устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

– информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится с перио-

дичностью, установленной оператором. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.

Требования к усилению анализа (контроля) уязвимостей:

1) в информационной системе обеспечивается использование для поиска (выявления) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей;

2) в информационной системе обеспечивается уточнение перечня сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях;

3) в информационной системе определяется информация об информационной системе, которая может стать известной нарушителям и использована ими для эксплуатации уязвимостей (в том числе уязвимостей «нулевого дня» – уязвимостей, описание которых отсутствует в базах данных разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения,

технических средств), и принимаются меры по снижению (исключению) последствий от эксплуатации нарушителями неустранимых уязвимостей;

4) в информационной системе предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности);

5) в информационной системе применяются автоматизированные средства для сравнения результатов сканирования уязвимостей в разные периоды времени для анализа изменения количества и классов (типов) уязвимостей в информационной системе;

6) в информационной системе применяются автоматизированные средства для обнаружения в информационной системе неразрешенного программного обеспечения (компонентов программного обеспечения) и уведомления об этом уполномоченных должностных лиц (администратора безопасности);

7) в информационной системе проводится анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в информационной системе для нарушения безопасности информации;

8) в информационной системе обеспечивается проведение выявления уязвимостей «нулевого дня», о которых стало известно, но информация о которых не включена в сканеры уязвимостей;

9) в информационной системе обеспечивается проведение выявления новых уязвимостей, информация о которых не опубликована в общедоступных источниках;

10) в информационной системе осуществляется выявление (поиск) уязвимостей в информационной системе с использованием учетных записей на сканируемых ресурсах;

11) в информационной системе используется тестирование информационной системы на проникновение.

В информационной системе должен осуществляться контроль точности, полноты и правильности данных, вводимых в информационную систему. Контроль точности, полноты и правильности данных, вводимых в информационную систему, обеспечивается путем установления и проверки соблюдения форматов ввода данных, синтаксических, семантических и (или) иных правил ввода информации в информационную систему (допустимые наборы символов, размерность, область числовых значений, допустимые значения, количество символов) для подтверждения того, что ввод информации соответствует заданному оператором формату и содержанию. Вводимые данные должны проверяться на наличие конструкций, которые могут быть интерпретированы программно-техническими средствами информационной системы как исполняемые команды.

2.3. Определение класса защищенности информационной системы

Устанавливаются четыре класса защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4)), определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Класс защищенности информационной системы определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности, целостности или доступности информации:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

– высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

– средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

– низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недос-

таточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Для определения степени возможного ущерба от нарушения конфиденциальности, целостности или доступности могут применяться национальные стандарты и (или) методические документы, разработанные и утвержденные ФСТЭК России.

2.4. Разработка практических занятий

2.4.1. Практическое занятие: Тема: «Нарушения конфиденциальности, целостности и доступности информации»

Цель занятия: закрепить умения и навыки при изучении нарушения конфиденциальности, целостности и доступности информации.

Порядок выполнения занятия:

1. Дать характеристику конфиденциальности.
2. Дать характеристику целостности.
3. Дать характеристику доступности.
4. Охарактеризовать защиту информации.
5. Перечислить и охарактеризовать виды защиты информации.
6. Основные понятия теории информационной безопасности
7. Каковы основные задачи защиты информации?
8. Вывод.

Краткие теоретические сведения

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (согласно ФЗ-149 «Об информации, информационных технологиях и о защите информации»);

Конфиденциальность – обеспечение доступа к информации только авторизованным пользователям.

Целостность – обеспечение достоверности и полноты информации и методов ее обработки. (ГОСТ Р ИСО/МЭК 17799-2005, ст. 2.1).

Целостность информации — состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право (Р 50.1.056-2005, ст. 3.1.6).

Доступность — обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Угроза раскрытия заключается в том, что информация становится известна неавторизованному пользователю. Она возникает всякий раз, когда получен несанкционированный доступ к секретной (конфедициальной) информации, хранящейся в вычислительной системе, или передаваемой от одной системы к другой. Иногда в связи сугрозой информации используется термин «утечка информации».

Угроза целостности включает в себя любое несанкционированное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую.

Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий умышленно блокируется доступ к некоторому ресурсу вычислительной системы.

Контролируемая зона — территория вокруг предприятия, на которой исключено неконтролируемое пребывание посторонних лиц и любого вида транспорта, не имеющих постоянного или разового пропуска на эту территорию.

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Несанкционированный доступ (НСД) к информации – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС, преднамеренное

обращение субъекта к компьютерной информации, доступ к которой ему не разрешен, независимо от цели обращения.

Администратор АС – физическое лицо, ответственное за функционирование АС в установленном штатном режиме работы.

Администратор безопасности – физическое лицо, ответственное за защиту АС от НСД к информации.

Информация, составляющая коммерческую тайну – информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

Режим разграничения доступа – порядок доступа к компьютерной информации в соответствии с установленными правилами.

Защита информации – это деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Виды защиты информации (согласно ГОСТ Р 50922-2006):

– правовая защита информации: разработка законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

– криптографическая защита информации: Защита информации с помощью ее криптографического преобразования.

– техническая защита информации: обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств.

– физическая защита информации: путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

2.4.2. Практическое занятие: Тема: «Аудит информации»

Цель занятия: изучение основных задач, моделирование и реализация процесса с утечкой и искажением информации.

Порядок выполнения занятия

1. Описать назначения аудита клавиатуры.
2 Объяснить механизма прерываний в ОС MS-DOS.
3 Охарактеризовать аудит информации.
4 Назначение аудита информации.
5 Разновидности аудита информации.
6 Этапы работ при проведении аудита безопасности.
7 Вывод.

Краткие теоретические сведения

Несмотря на то, что в настоящее время ещё не сформировалось устоявшегося определения аудита безопасности, в общем случае его можно представить в виде процесса сбора и анализаинформации об АС, необходимой для последующего проведениякачественной или количественной оценки уровня защиты от атак злоумышленников. Существует множество случаев, в которых целесообразно проводить аудит безопасности. Вот лишь некоторые:

1. Аудит АС с целью подготовки технического задания на проектирование и разработку системы защиты информации.

2. Аудит АС после внедрения системы безопасности для оценки уровня её эффективности.

3. Аудит, направленный на приведение действующей системы безопасности в соответствие требованиям российского или международного законодательства;

4. Аудит, предназначенный для систематизации и упорядочивания существующих мер защиты информации.

5. Аудит, в целях расследования произошедшего инцидента, связанного с нарушением информационной (кофедициональной) безопасности.

Как правило, для проведения аудита привлекаются внешние компании, которые предоставляют консалтинговые услуги в области информационной безопасности. Инициатором процедуры аудита может являться руководство предприятия, служба автоматизации или служба информационной безопасности. В ряде случаев аудит также может проводиться по требованию страховых компаний или регулирующих органов. Аудит безопасности проводится группой экспертов, численность и состав которой зависит от целей и задач обследования, а также сложности объекта оценки.

Виды аудита безопасности: в настоящее время можно выделить следующие основные виды аудита информационной безопасности:

− экспертный аудит безопасности, в процессе которого выявляются недостатки в системе мер защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре обследования;

− оценка соответствия рекомендациям Стандарта ISO 17799, а также требованиям руководящих доку-ментов ФСТЭК (Гостехкомиссии);

− инструментальный анализ защищённости АС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;

− комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

Каждый из вышеперечисленных видов аудита может проводиться по отдельности или в комплексе в зависимости от тех задач, которые необходимо решить предприятию. В качестве объекта аудита может выступать как АС компании в целом, так и её отдельные сегменты, в которых проводится обработка информации, подлежащей защите.

Состав работ по проведению аудита безопасности: В общем случае аудит безопасности, вне зависимости от формы его проведения, состоит из четырёх основных этапов, каждый из которых предусматривает выполнение определённого круга задач (рисунок 2.2).

Рисунок 2.2 − Основные этапы работ при проведении аудита безопасности

На первом этапе совместно с Заказчиком разрабатываетсярегламент, устанавливающий состав и порядок проведения работ. Основная задача регламента заключается в определении границ, в рамках которых будет проведено обследование. Регламент является тем документом, который позволяет избежать взаимных претензий по завершению аудита, поскольку чёткоопределяет обязанности сторон. Как правило, регламент содержит следующую основную информацию:

− состав рабочих групп от Исполнителя и Заказчика, участвующих в процессе проведения аудита;

− перечень информации, которая будет предоставлена Исполнителю для проведения аудита;

− список и местоположение объектов Заказчика, подлежащих аудиту;

− перечень ресурсов, которые рассматриваются в качестве объектов защиты (информационные ресурсы, программные ре-

сурсы, физические ресурсы и т.д.);

− модель угроз информационной безопасности, на основе которой проводится аудит;

− категории пользователей, которые рассматриваются в качестве потен-циальных нарушителей;

− порядок и время проведения инструментального обследования автоматизированной системы Заказчика.

На втором этапе, в соответствии с согласованным регламентом, осуществляется сбор исходной информации. Методы сбора информации включают интервьюирование сотрудников Заказчика, заполнение опросных листов, анализ предоставленной организационно-распоря-дительной и технической документации, использование специали-зированных инструментальных средств.

Третий этап работ предполагает проведение анализа собранной информации с целью оценки текущего уровня защищённости АС Заказ-чика.

Четвёртый этап По результатам проведённого анализа на четвёртом этапе проводится разработка рекомендаций по повышению уровня защищённости АС от угроз информационной безопасности.

Качество проводимого аудита безопасности во многом зависит от полноты и точности информации, которая была получе-на в процессе сбора исходных данных. Поэтому информация должна включать в себя существующую организационно-распорядительную документацию, по вопросам информационной безопасности; сведения о программно-аппа-ратном обеспечении АС; информацию о средствах защиты, установленных в АС и т.д.

Более подробный перечень исходных (начальных) данных пред-ставлен в таблице 2.1.

Таблица 2.1 – Перечень исходных данных, необходимых для проведения аудита безопасности

Тип информации	Описание состава исходных данных
Организационно-распорядительная документация по вопросам *информационной безопасности*	– политика *информационной безопасности АС*; – руководящие документы (приказы, распоряжения, инструкции) по вопросам хранения, порядка доступа и передачи информации; – *регламенты* работы пользователей с информационными ресурсами *АС*
Информация об *аппаратном обеспечении хостов*	– перечень серверов, *рабочих станций* и *коммуникационного оборудования*, установленного в *АС*; – информация об аппаратной конфигурации серверов и *рабочих станций*; – информация о периферийном оборудовании, установленном в *АС*
Информация об общесистемном ПО	– информация об операционных системах, установленных на рабочих станциях и серверах *АС*; – данные о СУБД, установленных в *АС*
Информация о прикладном ПО	– перечень прикладного ПО общего и специального назначения, установленного в *АС*; – описание функциональных задач, решаемых с помощью прикладного ПО, установленного в *АС*
Информация о средствах защиты, установленных в *АС*	– информация о производителе средства защиты; – конфигурационные настройки средства защиты; – схема установки средства защиты

Окончание таблицы 2.1.

Информация о *топологии АС*	– карта *локальной вычислительной сети*, включающей схему распределения серверов и *рабочих станций* по сегментам сети; – информация о типах каналов связи, используемых в *АС*; – информация об используемых в *АС сетевых протоколах* – схема *информационных потоков АС*

Сбор исходных данных может осуществляться с использованием следующих методов:

− интервьюирование сотрудников Заказчика, обладающих необходимой информацией. При этом интервью, как правило, проводится как с техническими специалистами, так и с представителями руководящего звена компании. Перечень вопросов, которые планируется обсудить в процессе интервью, согласовывается заранее;

− предоставление опросных листов по определённой тематике, самостоятельно заполняемых сотрудниками Заказчика. В тех случаях, когда представленные материалы не полностью дают ответы на необходимые вопросы, проводится дополнительное интервьюирование;

− анализ существующей организационно-технической документации, используемой Заказчиком;

− использование средств, которые позволяют получить необходимую информацию о составе и настройках программно-аппаратного обеспечения автоматизированной системы Заказчика. Оценка уровня безопасности АС

После сбора необходимой информации проводится её анализ с целью оценки текущего уровня защищённости системы.

Методология анализа рисков в общем виде была рассмотрена врамках «Моделирование угроз ИБ: различные подходы». В процессе проведения аудита безопасности могут использоватьсспециализированные программные комплексы, позволяющие автоматизировать процесс ана-

лиза исходных данных и расчёта значений рисков. Примерами таких комплексов являются «Гриф» и «Кондор» (компании «Digital Security»), а также «АванГард» (Института Системного Анализа РАН).

Результаты аудита безопасности

На последнем этапе проведения аудита информационной безопасности разрабатываются рекомендации по совершенствованию организационно-технического обеспечения предприятия. Такие рекомендации могут включать в себя следующие типы действий, направленных на минимизацию выявленных рисков:

– уменьшение риска за счёт использования дополнительных организационных и технических средств защиты, позволяющих снизить вероятность проведения атаки или уменьшить возможный ущерб от неё. Так, например, установка межсетевых экранов в точке подключения АС к сети Интернет позволяет существенно снизить вероятность проведения успешной атаки на общедоступные информационные ресурсы АС, такие как Web -серверы, почтовые серверы и т.д.;

– уклонение от риска путём изменения архитектуры или схемы информационных потоков АС, что позволяет исключить возможность проведения той или иной атаки. Так, например, физическое отключение от сети Интернет сегмента АС, в котором обрабатывается конфиденциальная информация, позволяет исключить атаки на конфиденциальную информацию из этой сети;

– изменение характера риска в результате принятия мер по страхованию. В качестве примеров такого изменения характера риска можно привести страхование оборудования АС от пожара или страхование информационных ресурсов от возможного нарушения их конфиденциальности, целостности или доступности. В настоящее время российских компаний уже предлагают услуги по страхованию информационных рисков;

– принятие риска в том случае, если он уменьшен до того уровня, на котором он не представляет опасности для АС.

Как правило, разработанные рекомендации направлены не на полное устранение всех выявленных рисков, а лишь на их уменьшение до приемлемого остаточного уровня. При выборе мер по повышению уровня защиты АС учитывается одно принципиальное ограничение – стоимость их реализации не должна превышать стоимость защищаемых информационных ресурсов.

В завершении процедуры аудита его результаты оформляются в виде отчётного документа, который предоставляется Заказчику. В общем случае этот документ состоит из следующих основных разделов:

– описание границ, в рамках которых был проведён аудит безопасности; описание структуры АС Заказчика;

– методы и средства, которые использовались в процессе проведения аудита;

– описание выявленных уязвимостей и недостатков, включая уровень их риска;

– рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности;

– предложения по плану реализации первоочередных мер, направленных на минимизацию выявленных рисков.

2.4.3. Практическое занятие: Тема: «Защита от утечек информации»

Цель занятия: применение методов и технологий испытания аппаратного уровня комплексной защиты информации.

Порядок выполнения занятия

1 Раскрыть понятие утечки информации.

2 Что подразумевается под каналом утечки информации?

3 Перечислить виды возможных технических каналовутечки информации.

4 Привести примеры утечек информации.

5 Раскрыть понятие акустоэлектрический канал утечки информации.

6 Вывод.

Краткие теоретические сведения

Защита информации от утечки по техническим каналам это комплекс организационных, организационно-технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

Утечка – бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

В основе утечки конфиденциальной информации техническим каналам лежит неконтролируемый перенос ценных сведений посредством акустических, электромагнитных, радиационных и других полей и материальных средств.

Причиной утечки является несовершенство норм по сохранению информации в аппаратных средствах, а также указанных норм.

Защита информации от утечки по акустическому виброакустическому каналу предполагает применение архитектурно-планировочных, пространственных, пассивных (звукоизоляция) и активных (звукоподавление) мероприятий.

Тестовые испытания защиты информации от утечки по акустическому и виброакустическому каналам включают:

− измерение звукоизоляции выделенных помещений;

− измерение виброизоляции выделенных помещений;

− измерение электроакустических преобразований вспомо- гательных технических средств.

Защита от утечки за счет паразитных электромагнитных излучений и наводок (ПЭМИН) требует строгого исполнения порядка размещения аппаратных средств в пространстве объекта и относительно друг друга.

Тестовые испытания защиты информации от утечки за счет наводок и ПЭМИ включают:

− измерение ПЭМИ рабочих станций (АРМ) пользователей, серверов, устройств вывода (ввода) информации, коммуникационного оборудования и кабельных соединений;

− измерение наводок информационных сигналов на вспомогательные средства, имеющие выход за пределы контролируемой зоны;

− измерение наводок информационных сигналов на кабельное и коммуникационное оборудование.

Проверку эффективности защиты по указанным каналам проводят с применением шумомера, электронного стетоскопа, селективного нановольтметра, измерительного приемника, анализатора спектра и иных специализированных измерительных приборов.

Канал утечки информации состоит из источника сигнала, физической среды его распространения и приемной аппаратуры на стороне злоумышленника. Движение информации в таком канале осуществляется только в одну сторону — от источника к злоумышленнику. На рисунке 2.3 приведена структура канала утечки информации.

Рисунок 2.3 – Структура канала утечки информации

Под каналом утечки информации физический путь от источника конфиденциальной информации к злоумышленнику, по которому несанкционированное получение имеет место быть.

Применительно к практике с учетом физической природы образования каналы утечки информации квалифицируются на группы:

– визуально-оптические;

– акустические (включая и акустико-преобразовательные);

– электромагнитные (включая магнитные и электриче-

– материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида твердые, жидкие, газообразные).

Для выполнения работы по проверке провести необходимые измерения с использованием объекта проверки и измерительных приборов по выбору преподавателя.

2.4.4. Практическое занятие: Тема: «Анализ трафика»

Цель занятия: применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки

Порядок выполнения занятия

1 Охарактеризовать угрозы пассивного анализа.

2 Что положено в основу атаки?

3 Раскрыть понятие «трафик» в вычислительной системе.

4 Описать роль анализа трафика системы.

5 Средства позволяющие реализовать пассивный анализ.

6 Охарактеризовать программу-сниффер.

7 Вывод.

Краткие теоретические сведения

Анализ трафика и сбор критичной информации программами пассивного анализа является одним из методов получения критичной информации о корпоративной информационной системе.

Для реализации необходимо иметь специализированное программное обеспечение.

Проведение анализа трафика и сбор критичной информации применением программ пассивного анализа (программ-снифферов и программ обнаружения вторжений) включает:

− получение информации об используемых аутентификационных протоколах, процедурах доступа;

− обнаружение в открытом трафика передаваемых регистрационных имен;

− идентификаторов и паролей пользователей, определение текстовых паролей, паролей на доступ в удаленные системы;

− проверка паролей, используемых при аутентификации службами SMB, POP3, IMAP, Telnet, HTTP, FTP и др. (протоколы прикладного уровня);

− определение почтовых ящиков на общедоступных почтовых серверах;

− анализ почтового трафика на предмет выявления писем, отвечающих определенным признакам;

− диагностика проблем при сетевом обмене хостов;

− проверочная рассылка электронной почты;

− определение свойств реализации стека TCP;

− определение маршрутов хождения пакетов;

− тестирование правильности настроек систем контроля трафика.

2.4.5. Практическое занятие «Оценка уязвимости коммутируемого доступа»

Цель занятия: применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки с целью установления уязвимостей.

Порядок выполнения занятия

1 Раскрыть понятие коммутируемый доступ.

2 Перечислить виды коммутируемого доступа.

3 Описать сложность использования коммутируемого до-

4 Перечислить слабости коммутируемого доступа.

5 Описать методы противодействия данной атаке.

6 Вывод.

Краткие теоретические сведения

Оценка уязвимости коммутируемого доступа вычислительную сеть предприятия является одним из методов получения критичной информации о корпоративной информационной системе. Для реализации необходимо иметь специализированное программное обеспечение.

Уязвимость слабое место в информационной системе, которое может привести к нарушению безопасности. Различают человеческую уязвимость и техническую уязвимость, возникающую в результате неисправности технологического компонента информационной системы.

Коммутируемый доступ, при котором обеспечивается установление соединений только по необходимости.

Оценка уязвимости коммутируемого доступа включает:

− определение каналов удаленного доступа с коммутируемым подключением, которые могут быть использованы для вхождения во внутреннюю сеть через телефонные сети общего пользования;

− анализ защищенности каналов удаленного доступа с ком-мутируемым подключением.

2.4.6. Практическое занятие: «Аудит комплексной защиты информации»

Цель занятия: применение принципов организации проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Порядок выполнения занятия

1. Перечислить виды аудита информационной системы.

2. Перечислить источники успеха аудита.

3. Раскрыть понятие «сюрвей».

4. Описать сложность применения аудита.

5. Перечислить и охарактеризовать слабости внутреннего аудита силами предприятия.

6. Приведите несколько примеров успешного применения аудита.

7. Вывод.

Краткие теоретические сведения

Аудит комплексной защиты информации является основой построения системы защиты информации предприятия. Для его проведения и получения достоверных результатов требуется, как правило, привлечение организаций.

При создании любой информационной системы (ИС) на базе современных компьютерных технологий неизбежно возникает вопрос о защищенности этой системы от внутренних и внешних угроз безопасности информации. Но прежде чем решить, как и от кого защищать информацию, необходимо уяснить реальное положение в области обеспечения безопасности информации на предприятии и оценить степень защищенности информационных активов. Для этого проводится комплексное обследование защищенности ИС (или аудит безопасности), основанные на выявленных угрозах безопасности информации и имеющихся методах их парирования, результаты которого позволяют:

1. Оценить необходимость и достаточность принятых меробеспечения безопасности информации;

2. сформировать политику безопасности;

3 Правильно выбрать степень защищенности информационной системы.

4. Выработать требования к средствам и методам защиты.

5. Добиться максимальной отдачи от инвестиций в созданиии обслуживании СОБИ.

Комплексное обследование (аудит безопасности информации) защищенности представляет собой системный процесс получения и оценки

объективных данных о текущем состоянии обеспечения безопасности информации на объектах информатизации, действиях и событиях, происходящих в информационной системе, определяющих уровень их соответствия определенному критерию. Поскольку информационная безопасность должна быть обеспечена не только на техническом, но и на организационно-административном уровне, должный эффект может дать только комплексный подход к обследованию (аудиту), то есть:

1. Проверка достаточности принятых программно-аппаратных и технических мер защиты (соответствие установленным требованиям применяемых в ИС программно-аппаратных средств защиты).

2. Проверка достаточности инженерно-технических, правовых, экономических и организационных мер защиты (физической защиты, работы с персоналом, регламентации его действий).

Процесс комплексного обследования защищенности информационной системы состоит из трех основных частей:

1. Сбор необходимых исходных данных и их предварительный анализ (или стадия планирования);

2. Оценка соответствия состояния защищенности ИС предъявляемым требованиям и стандартам (стадии моделирования, тестирования и анализа результатов).

3. Формулирование рекомендаций по повышению безопасности информации в обследуемой ИС (стадии разработки предложений и документирования полученных результатов).

На разных этапах обследования используются различные методы: технические, аналитические, экспертные, расчетные. При этом, результаты, полученные одними методами, могут дублироваться (дополняться) результатами, полученными другими методами. Совокупность всех применяемых методов позволяет дать объективную оценку состояния обеспечения безопасности информации на обследуемом объекте.

Основными группами методов при обследовании являются:

1. Экспертно-аналитические методы предусматривают проверку соответствия обследуемого объекта установленным требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации оборудования предъявляемым требованиям по размещению, монтажу и эксплуатации технических и программных средств.

2. Экспертно-инструментальные методы предполагают проведение проверки функций или комплекса функций защиты информации с помощью специального инструментария (тестирующих средств) и средств мониторинга, а также путем пробного запуска средств защиты информации и наблюдения реакции за их выполнением. В процессе испытаний технических и программных средств используются тестирующие средства, принятые в установленном порядке.

3. Моделирование действий злоумышленника («дружественный взлом» системы защиты информации) применяются после анализа результатов, полученных в ходе использования первых двух групп методов, они необходимы как для контроля данных результатов. Этим методом подтверждаются также реальные возможности потенциальных злоумышленников (как внутренних, легально допущенных к работе с тем или иным уровнем привилегий в ИС, так и внешних в случае подключения ИС к глобальным информационным сетям). Кроме того, подобные методы могут использоваться для получения дополнительной исходной информации об объекте, которую не удалось получить другими методами.

Выводы по главе 2.

Оценка эффективности средств и методов защиты информации в целом, в том числе конфиденциальной информации, начинается с выбора и обоснования критериев:

– типа «эффект–затраты», характеризуемые соотношением затрат на реализацию механизма защиты и полученного эффекта (экономическая эффективность);

– позволяющие оценивать качество оценки эффективности средств и методов защиты информации;

– позволяющие определить достаточность применяемых мер защиты.

Решение задачи расчета показателей эффективности средств и методов защиты информации может производиться с помощью таких различных средств, как методы моделирования процессов, экспертные оценки, статистический анализ, метод минимизации рисков и защиты информации, а также иных подходов. Ни один из методов не лишен недостатков, вследствие чего на практике следует их комбинировать, то есть, и в частности, и в целом, осуществлять их генерирование:

1. Расчета значений показателей оценки выполнения требований к технологическим мерам защиты информации по направлению «Технологические меры» оценка, характеризующая выполнение требований в рамках процесса планирования применения мер защиты информации с использованием оценок, характеризующих выполнение требований в рамках: процесса реализации мер защиты информации; контроля применения мер защиты информации; процесса совершенствования применения мер защиты информации и др.

2. Расчета значений показателей оценки выполнения требований к программному обеспечению автоматизированных систем, к примеру, и др.

Примечательно, что на первый план выдвигается выполнение оценок наиболее критичных требований, прежде всего, к технологическим мерам защиты информации по направлению «Технологические меры» с последующим синтез-объединением в ракурсе с оценочным выполнением требований непосредственно к программному обеспечению, как правило, автоматизированной разновидности информационных систем путем присвоения оценкам выполнения требований значений с точки зрения полноты

определения их реализации: 1 – «да» (определено «постоянно», «всегда», «в полном объеме»); 0,75 – «в основном «да» («почти постоянно», «почти всегда», «почти в полном объеме»); 0,5 – «частично» («отчасти да», «не всегда», «в некоторых случаях»); 0,25 – «в основном «нет» («непостоянно», «почти никогда»); 0 – «нет» («никогда», «ни в каких случаях»).

В итоге, выбор мер защиты информации (первый шаг в выборе мер защиты информации) для их реализации в информационной системе включает: определение базового набора мер защиты информации (БНМЗИ) с установлением класса защищенности (К1, К2 или К3) информационной системы; адаптацию БНМЗИ применительно к составу и особенностям функционирования информационной системы; уточнение адаптированного БНМЗИ с учетом не включенных в модель угроз безопасности информации; дополнение уточненного и затем адаптированного БНМЗИ мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты конфедициональных данных.

Для надёжной минимизации рисков и гарантированной на достаточном уровне защиты информации с необходимостью в процессе комбинирования нескольких методов при оценке эффективности информационной системы применительно к исходным данным должна осуществляться их объективизация, базовыми компонентами которой являются контроль точности, полноты и правильности вводимых в информационную систему данных. Тем самым достигается повышение уровня значимости обрабатываемоӣ информации и, соответственно, уровня детерминации подвергаемой оценке эффективности средств и методов защиты конфедициональных данных информационной системы в процессе её аудита. В свете таких обстоятельств выполнена, в обеспечение надёжности итогового результата аудита оценки эффективности средств и методов подвергаемой контролю информационной системы, выполнена разработка практических занятий: «Нарушения конфиденциальности, целостности и

доступности информации», «Аудит информации», «Защита от утечек информации», «Анализ трафика» с формулировками целей занятий, кратких теоретических сведений и порядка выполнения занятий.

В итоге разработан вариант опытно-экспериментального алгоритма модели генерирования расчетных операций предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации как важного компонента методики профессионального образования в ракурсе трансформации научно-исследовательскоӣ культуры и цифровой грамотности педагогов-исследователей, магистрантов, аспирантов и др.

ЗАКЛЮЧЕНИЕ

Методический подход к оценке эффективности защиты информации в информационной сфере образования позволяет заключить, что наиважнейшими особенностями в сфере информационной безопасности и основными её задачами является насущная необходимость сохранения свойств информации, обеспечения целостности данных, их конфиденциальности и регламентируемой доступности. Представить в современных условиях образовательную организацию без защищаемой информации и информационных технологий невозможно. Основным шагом оптимизации затрат на систему защиты информации современной организации является, прежде всего, анализ рисков информационной безопасности и угроз с выявлением наиболее критических факторов, оказывающих наиболее отрицательное влияние на информационную безопасность средств и методов защиты информации образовательной организации

Главной задачей информационной безопасности образовательной организации является управление рисками нарушения информационной целостности, а обеспечение – это главный критерий качества выполнения информационных процессов, в том числе иинформационной инфраструктурой образовательной организации в целом. Одним из наиболее немаловажных процессов при организации системы защиты информации образовательной организации является минимизация затрат. Для СПО и ВУЗов, с учетом необходимости оптимизации затрат на организацию системы защиты конфиденциальной информации образовательной организации, наиболее приемлемым является комбинированный метод, заключающийся в том, что необходимо экранировать лишь определенные подразделения от внешних воздействий, организовать доступ пользователей к информационной системе и к открытым сетям автоматизированного рабочего места также только лишь при необходимости.

Главная проблема информационной сферы образования – проблема установления рационального баланса между эффективностью и информационной безопасностью образовательной организации. Это приводит к необходимости создания информационной инфраструктуры в сфере образования с соответствующими техническими и программными средствами обработки данных, т.к. для её успешности, даже не говоря о повышении её эффективности, необходимо учитывать большее число факторов и невозможность проверки достоверности всех используемых данных. Содержательно и формально критическую часть информационной системы организации, в т.ч. образовательной, способную наносить ущербы и приводить к негативным последствиям для целей организации, определяет пятёрка риск-факторов «А, П, И, С, Р») – активы (А), процессы (П), инструменты (И), субъекты (С) и роли (Р). У базовых рисковых событий всегда через их риск-факторы может быть идентифицирован их контекст в информационной сфере организации.

Оценка эффективности средств и методов защиты информации в целом, в том числе конфиденциальной информации, начинается с выбора и обоснования критериев:

– типа «эффект–затраты», характеризуемые соотношением затрат на реализацию механизма защиты и полученного эффекта (экономическая эффективность);

– позволяющие оценивать качество оценки эффективности средств и методов защиты информации;

– позволяющие определить достаточность применяемых мер защиты.

Решение задачи расчета показателей эффективности средств и методов защиты информации может производиться с помощью таких различных средств, как методы моделирования процессов, экспертные оценки, статистический анализ, метод минимизации рисков и защиты информации, а также иных подходов. Ни один из методов не лишен недостатков,

вследствие чего на практике следует их комбинировать, то есть, и в частности, и в целом, осуществлять их генерирование:

1. Расчета значений показателей оценки выполнения требований к технологическим мерам защиты информации по направлению «Технологические меры» оценка, характеризующая выполнение требований в рамках процесса планирования применения мер защиты информации с использованием оценок, характеризующих выполнение требований в рамках: процесса реализации мер защиты информации; контроля применения мер защиты информации; процесса совершенствования применения мер защиты информации и др.

3. Расчета значений показателей оценки выполнения требований к программному обеспечению автоматизированных систем, к примеру, и др.

Примечательно, что на первый план выдвигается выполнение оценок наиболее критичных требований, прежде всего, к технологическим мерам защиты информации по направлению «Технологические меры» с последующим синтез-объединением в ракурсе с оценочным выполнением требований непосредственно к программному обеспечению, как правило, автоматизированной разновидности информационных систем путем присвоения оценкам выполнения требований значений с точки зрения полноты определения их реализации: 1 – «да» (определено «постоянно», «всегда», «в полном объеме»); 0,75 – «в основном «да» («почти постоянно», «почти всегда», «почти в полном объеме»); 0,5 – «частично» («отчасти да», «не всегда», «в некоторых случаях»); 0,25 – «в основном «нет» («непостоянно», «почти никогда»); 0 – «нет» («никогда», «ни в каких случаях»).

В итоге, выбор мер защиты информации (первый шаг в выборе мер защиты информации) для их реализации в информационной системе включает: определение базового набора мер защиты информации (БНМЗИ) с установлением класса защищенности (К1, К2 или К3) информационной системы; адаптацию БНМЗИ применительно к составу и особенностям функционирования информационной системы; уточнение адаптированного

БНМЗИ с учетом не включенных в модель угроз безопасности информации; дополнение уточненного и затем адаптированного БНМЗИ мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты конфедициональных данных.

Для надёжной минимизации рисков и гарантированной на достаточном уровне защиты информации с необходимостью в процессе комбинирования нескольких методов при оценке эффективности информационной системы применительно к исходным данным должна осуществляться их объективизация, базовыми компонентами которой являются контроль точности, полноты и правильности вводимых в информационную систему данных. Тем самым достигается повышение уровня значимости обрабатываемоӣ информации и, соответственно, уровня детерминации подвергаемой оценке эффективности средств и методов защиты конфедициональных данных информационной системы в процессе её аудита. В свете таких обстоятельств выполнена, в обеспечение надёжности итогового результата аудита оценки эффективности средств и методов подвергаемой контролю информационной системы, выполнена разработка практических занятий: «Нарушения конфиденциальности, целостности и доступности информации», «Аудит информации», «Защита от утечек информации», «Анализ трафика» с формулировками целей занятий, кратких теоретических сведений и порядка выполнения занятий.

В итоге разработан вариант опытно-экспериментального алгоритма модели генерирования расчетных операций предварительной подготовки процесса оценки эффективности средств и методов защиты конфиденциональной информации в образовательной организации как важного компонента методики профессионального образования в ракурсе трансформации научно-исследовательскоӣ культуры и цифровой грамотности педагогов-исследователей, магистрантов, аспирантов и др.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Громов, Ю.Ю. Оценка эффективности систем защиты информации и анализ рсков информационной безопасности в организации / Ю.Ю. Громов, П.И. Карасев, Ю.А. Губсков, В.А. Котюкова // Информационная безопасность. 2022. – Т. 25. – Вып. – С. 187–192. – DOI 10.36622/VSTU. 2022.25.2.003. – URL: https://docs.yandex.ru/docs/view?tm=1756984705&tld =ru&lang=ru&name=МАКЕТ%20сиб%20Т25%20ВЫП2-3.pdf&text=оценка% 20эффективности%20средств%20и%20методов%20защиты%20конфиденциальной%20информации%20в%20образовательной%20организации (дата обращения 07.09.25).

2. Баранова, Е.К. Информационная безопасность и защита информации: учеб. пособие. 3-е изд. перераб. и доп / Е.К. Баранова, Л.В. Бабаш. Москва: РИОР ИНФРА-М, 2016. 322 с.

3. Управление рисками при внедрении информационных технологий на промышленных предприятиях. – URL: https://elar.urfu.ru/bitstream/10995/ 50431/1/m_th_k.a.krinitsyn_2017.pdf (дата обращения 21.10.25).

4. Трещев, И.А. Система защиты конфиденциальной информации для высших учебных заведений «Электронный университет» / И.А. Трещев, Я.Ю. Григорьев, А.А. Воробьев // Интернет-журнал «НАУКОВЕДЕНИЕ». 2013. – № 1. – С. 1–8. – URL: https:// naukovedenie.ru/PDF/44tvn113.pdf (дата обращения 07.09.25).

5. Андрианов, В.В. Оценка информационной безопасности бизнеса / В.В. Андрианов, В.Б. Голованов, Н.А. Голдуев, С.Л. Зефиров. – URL: https://pqm-online.com/assets/files/lib/books/andrianov.pdf (дата обращения 07.09.25).

6. Зефиров, С.Л. Способы оценки информационной безопасности организации / С.Л. Зефиров, В.М. Алексеев. – URL: https://cyberleninka.ru/article/n/sposoby-otsenki-informatsionnoy-bezopasnosti-organizatsii/viewer (дата обращения 07.09.25).

7. Методические рекомендации по организации информационной безопасности в образовательном учреждении. – URL: https://dpo-kipr.ru/wp-content/uploads/2022/11/Metodicheskie_rekomendacii_po_obespecheniju_informacionnoj_bezopasnosti.pdf (дата обращения 07.09.25).

8. Борлавкова, М.А. Современные методы и средства защиты информации / М.А.Борлавкова // Вестник Академии знаний. 2023. – № 54. – С. 68–72.

9. Маркина, Т.А. Средства защиты вычислительных систем и сетей: учеб. пособие / Т.А. Маркина. Санкт-Петербург: Университет ИТМО, 2016. – 71 с.

10. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты. Киев: ДиаСофт, 2002.

11. Методические рекомендации «По расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению оценки выполнения требований к обеспечению защиты информации». – URL: https://www.garant.ru/products/ipo/prime/doc/411567551/ (дата обращения 07.09.25).

12. Прохорова О.В. Информационная безопасность и защита информации: уч-к. – Самара: Самарский гос. архитектурно-строительный ун-т, 2017 – 113 с.: табл., схем., ил. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения 07.09.25).

13. Вальке, А.А. Электронные средства сбора и обработки информации: учебное пособие / А.А. Вальке, В.А. Захаренко. Омск: Изд-во ОмГТУ, 2017. – 112 с. – URL: http://biblioclub.ru/index.php?page=book&id=493448 (дата обращения 07.09.25).

14. Сычев, А.Н. ЭВМ и периферийные устройства: учебн. пособие. – Томск: ТУСУР, 2017. – 131 с.: ил. – URL: http://biblioclub.ru/index.php?page=book&id=481097 (дата обращения 07.09.25).

15. Громов, Ю.Ю. Программно-аппаратные средства защиты информационных систем: учебн. пособие. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ»,

2017. – 194 с. – URL: http://biblioclub.ru/index.php?page=book&id=499013 (дата обращения 07.09.25).

16. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий / В.А. Сердюк. – Москва: Изд-й дом Высшей школы экономики, 2015 – 574 с. – URL: http://biblioclub.ru/index.php?page=book&id=440285 (дата обращения 07.09.25).

17. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – URL: index.php?page=book&id=428820 (дата обращения 07.09.25).

18. Качаева, Г.И. Показатели эффективности функционирования при разработке систем защиты информации от несанкционированного доступа в автоматизированных информационных системах / Г.И. Качаева, А.Д. Попов, Е.А. Рогозин // Вестник Дагестанского гос. техн. ун-та. Технические науки. 2018. – Т. 45. – No 1. – С. 147–159 . – DOI: 10.21822/2073-6185-2018-45-1-147-159.

19. Рогозин, Е.А. Проектирование систем защита информации от несанкционированного доступа в автоматизированных системах органов внутренних дел / Е.А. Рогозин, А.Д. Попов, Т.В. Шагиров. // Вестник Воронежского института МВД России. – 2016. – No 2. – С. 174 – 183.

20. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – URL: https://fstec.ru/component/attachments/download/299 (дата обращения: 26.08.2025).

21. ГОСТ 28806-90 Качество программных средств. Термины и определения. – URL: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf (дата обращения: 23.09.2025).

22. ISO/IEC TR 9126-2:2003 Software engineering – Product quality – Part 2: External metrics. – URL: https://www.iso.org/standard/22750.html (дата обращения: 26.06.2025).

23. ISO/IEC TR 9126-3:2003 Software engineering – Product quality – Part 3: Internal metrics. – URL: https://www.iso.org/standard/22891.html (дата обращения: 26.06.2025).

24. ISO/IEC TR 9126-4:2004 Software engineering – Product quality – Part 4: Quality in use metrics. – URL: https://www.iso.org/standard/39752.html (дата обращения: 26.06.2025).

25. СЗИ «Страж NT». Руководство администратора. – URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (дата обращения: 23.09.2025).

26. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. – URL: http://www.rubinteh.ru/public/opis30.pdf (дата обращения: 23.09.2025).

27. Липаев, В.В. Качество программных средств: методич. рекомендации / В.В. Липаев, под. общ. ред. А.А. Полякова. Москва: Янус-К, 2002. 400 с.

28. Боэм, Б. Характеристики качества программного обеспечения / Б. Боэм, Дж. Браун, Х. Каспар и [др.], пер. с англ. Е.К. Масловского. Москва: Мир, 1981. 208 с.

29. Черников, Б.В. Оценка качества программного обеспечения: Практикум: учебное пособие / Б.В. Черников, Б.Е. Поклонов. Москва: ИД «ФОРУМ»: ИНФРА-М, 2012. 400 с.

30. Герасименко, В.А. Основы информации / В.А. Герасименко, А.А. Малюк Москва: МИФИ, 1997. 537 с.

31. Петухов, Г.Б. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем / Г.Б. Петухов, Якунин В.И. Москва: АСТ, 2006. 504 с.

32. ГОСТ Р 50922–2006 Защита информации. Основные термины и определения. – Москва: Стандартинформ, 2006. – 12 с.

33. Юсупов, Р.М. Особенности оценивания эффективности информационных систем и технологий / Р.М. Юсупов, А.А. Мусаев // Труды СПИИРАН. – 2017. – No 2 (51). – С. 5–34.

34. The Research and Discussion on Effectiveness Evaluation of Software Protection / Huaijun Wang; Dingyi Fang; Junhuai Li; Yong Chang; Lei Yu // 12-th International Conference on Computational Intelligence and Security (CIS): 2016. – IEEE Conferences. – Pp. 628–632

35. Method to Evaluate Software Protection Based on Attack Modeling / Huaijun Wang; Dingyi Fang; Ni Wang; Zhanyong Tang; Feng Chen; Yuanxiang Gu // IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year: 2013 Pages: 837 – 844 Cited by: Papers (1) IEEE Conferences.