



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
Кафедра автомобильного транспорта, информационных технологий и
методики обучения техническим дисциплинам

**Исследование и реализация эффективных методов управления
информационной безопасностью в профессиональной образовательной
организации**

**Магистерская диссертация по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном
образовании»
Форма обучения очная**

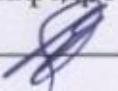
Проверка на объем заимствований:

85,01 % авторского текста

Работа рекомендована к защите

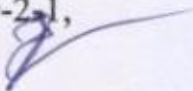
«1» 06 2022 г.

Зав. кафедрой АТИТ и МОТД

 В.В. Руднев

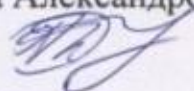
Выполнил:

Студент группы ОФ-209-210-2-1,

Ахметшин Денис Римович 

Научный руководитель:

Диденко Галина Александровна,

доцент, к.п.н. 

Челябинск, 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ	7
1.1 Понятие и сущность управления информационной безопасностью в образовательной организации.....	7
1.2 Методы управления информационной безопасностью в образовательной организации	15
1.3 Характеристика объекта исследования ГБПОУ «ЮУГК»	19
Выводы по первой главе.....	28
Глава 2. Реализация эффективных методов управления информационной безопасностью в образовательной организации ГБПОУ «ЮУГК».....	30
2.1 Рекомендации по реализации эффективных методов управления информационной безопасностью ГБПОУ «ЮУГК».....	30
2.2 Оценка эффективности предложенных рекомендаций по реализации эффективных методов управления информационной безопасностью ГБПОУ «Южно-Уральский государственный колледж» с помощью метода анализа дерева отказов.....	43
Выводы по второй главе.....	50
ЗАКЛЮЧЕНИЕ	52
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	54

ВВЕДЕНИЕ

Актуальность. С каждым годом вопросам управления информационной безопасностью уделяется все больше внимания как со стороны информационных технологий, так и со стороны высшего руководства компаний. Последние исследования, показали, что функция информационной безопасности становится все более важным элементом корпоративного управления [2].

На современном этапе развития общества информация становится одним из наиболее ценных и востребованных ресурсов, на сохранение и защиту которых выделяется все больше времени и средств. В связи с чем защита информации является одним из важных процессов любой организации. Процесс управления информационной безопасностью (ИБ) неразрывно связан с процессами защиты информации, ведь полнота и корректность его реализации во многом определяет эффективность системы защиты информации (СЗИ), однако, в типовой СЗИ подсистема управления ИБ, как правило, отсутствует. Постоянно увеличивающееся количество средств и мер защиты информации совместно с существующими недостатками типовой реализации СЗИ увеличивают нагрузку на персонал организации, увеличивая таким образом время на принятие управленческих решений. Ввиду невозможности увеличения количества ресурсов, выделяемых на процессы обеспечения и управления ИБ, до бесконечности, особо остро встает проблема рационализации их использования с учетом современных информационных технологий (ИТ) и средств обработки информации.

В отечественной и зарубежной литературе в настоящее время немалое внимание уделяется проблемам информационной безопасности [5]

Более подробно во второй половине XX века проблемы обеспечения ИБ, формализации процессных составляющих, а также составные элементы управления ИБ были рассмотрены в трудах известных российских и зарубежных ученых, таких как: О.Ю. Гаценко, Г.П. Жигулин, Ю.А.

Печеневский, М.Б. Будько, В.Г. Швед, Н.Н. Безруков, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой, О.Ю. А.А., Воробьева, Л.К. Бабенко, А.А. Анисимов, А.А. Малюк, А.Г. Корченко, Э. Уилсон, Д. Уотермен.

Принципы построения систем управления рассмотрены в работах Д. Джарратано, Г. Райли.

Потребность в создании оптимальной системы управления информационной безопасностью, а также проработка вопроса использования более совершенных методов управления информационной безопасности образовательных организаций остается **актуальной** и представляет, как научный, так и практический интерес.

Таким образом, **проблема исследования** заключается в выборе и реализации эффективных методов управления информационной безопасностью в профессиональной образовательной организации.

Объектом исследования является процесс управления информационной безопасностью в образовательной организации.

Предмет исследования: методы управления информационной безопасностью в образовательной организации ГБПОУ «Южно-Уральский государственный колледж».

Цель исследования: провести анализ существующих методов управления информационной безопасностью и разработать рекомендации по реализации эффективных методов управления информационной безопасностью в образовательной организации.

Реализация поставленной цели в магистерской диссертации потребовала постановки и последовательного решения следующих взаимосвязанных **задач:**

1. Раскрыть сущность и содержание методов управления информационной безопасностью.

2. Изучить объект защиты – ГБПОУ «Южно-Уральский государственный колледж», его структуру, информационные ресурсы и информационные потоки колледжа; проанализировать методы управления

информационной безопасностью в ГБПОУ ЮУГК; выявить уязвимости в системе защиты информации.

3. Разработать рекомендации по реализации эффективных методов управления информационной безопасностью колледжа ГБПОУ «Южно-Уральский государственный колледж».

4. Проверить предложенные рекомендации по реализации эффективных методов управления информационной безопасностью ГБПОУ «Южно-Уральский государственный колледж» с помощью метода анализа дерева отказов.

Гипотеза исследования состоит в предположении о повышении эффективности управления информационной безопасностью в образовательной организации при реализации эффективных методов управления информационной безопасностью.

Научная новизна проведенного исследования заключается в том, что показана возможность повышения эффективности управления информационной безопасностью в образовательной организации путем реализации эффективных методов управления информационной безопасностью.

Теоретическая значимость проведенного исследования состоит в обосновании реализации эффективных методов управления информационной безопасностью в ГБПОУ «Южно-Уральский государственный колледж».

Практическая значимость: разработаны рекомендации по реализации эффективных методов управления информационной безопасностью в ГБПОУ «Южно-Уральский государственный колледж».

Методологическую основу исследования составили законодательные и нормативно-правовые документы РФ, разработки в области обеспечения информационной безопасности, методы и способы построения процессов управления информационной безопасностью в целях повышения информационной безопасности в организациях, системный анализ.

Теоретическую и информационную базу исследования составляют основные положения по информационной безопасности, системный подход к исследуемому объекту и предмету, в качестве информационных источников использованы аналитические и статистические материалы по информационной безопасности, материалы научных конференций, средств массовой информации, отражающие аспекты информационной безопасности.

Структура магистерской диссертации: введение, две главы, выводы по главам, заключение, список использованных источников, приложение.

ГЛАВА 1. Теоретические аспекты управления информационной безопасностью в образовательных организациях

1.1. Понятие и сущность управления информационной безопасностью в образовательной организации

Система управления информационной безопасностью (СУИБ) является частью общей системы управления, базирующейся на анализе рисков и предназначенной для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности. СУИБ составляют организационные структуры, политика, действия по планированию, обязанности, процедуры, процессы и ресурсы. Основные цели информационной безопасности представлены на рисунке 1.



Рисунок 1 – Основные цели информационной безопасности

Для достижения заданных целей необходимо решить следующие задачи:

1. Ввод в систему терминов информационной безопасности;

2. классификации информационных ресурсов организации;
3. определения владельцев процессов, ответственных за информационную безопасность;
4. разработка спектра рисков информационной безопасности и проведения их экспертных оценок;
5. определение группы доступа к информационным ресурсам;
6. разработка системы управления рисками информационной безопасности (методы и их оценка);
7. составление перечня административных и технических мероприятий для минимизации и компенсации рисков;
8. осуществление мероприятий информационной безопасности и периодического контроля за состоянием рисков;
9. обеспечение физической безопасности и безопасности персонала;
10. разработка требований к информационной системе с точки зрения информационной безопасности;
11. контроль информационной безопасности в организации.

На рисунке 2 показаны стадии реализации СУИБ.

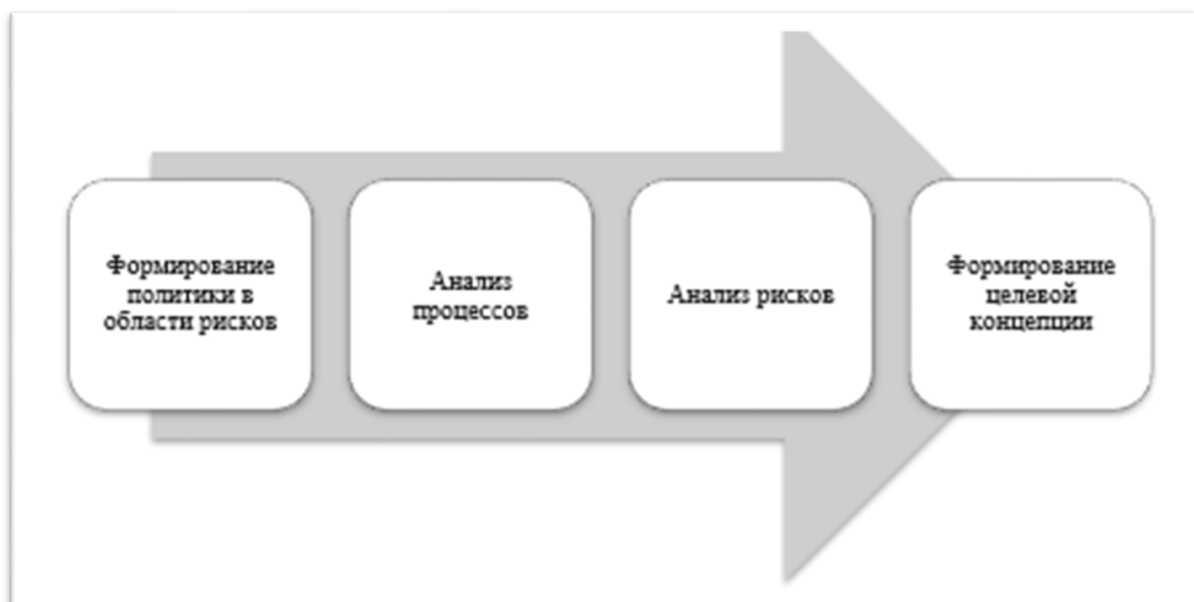


Рисунок 2 – Стадии реализации СУИБ

Формирование политики в области рисков подразумевает определение принципов управления ими для организации в целом. Эти принципы базируются на целях организации, его стратегии, также на требованиях, предъявляемых законом и стандартами в области информационной безопасности. Фактором эффективности системы управления информационной безопасностью является ее построение на базе стандарта ГОСТ Р ИСО/МЭК 27004-2021 «Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».

Стандарт ГОСТ Р ИСО/МЭК 27004-2021 определяет принципы и является руководством по разработке, внедрению, сопровождению и улучшению системы управления информационной безопасностью, а также описывает механизмы определения целей контроля, а так же устанавливает требования к системе управления информационной безопасностью организации, является руководством по определению, минимизации и управлению опасностями и угрозами, которым может подвергаться информация, и разработан в целях обеспечения помощи в выборе эффективных и адекватных средств для его защиты.

Применение стандарта в образовательной организации позволяет:

1. установить требования и цели в области информационной безопасности;
2. реализовать процесс контроля за внедрением системы управления информационной безопасностью;
3. идентифицировать и отслеживать существующие процессы управления информационной безопасностью;
4. руководству организации определить состояние процессов управления защитой информации;
5. внутренним и внешним аудиториям установить уровень соответствия политики безопасности регламентам;
6. обеспечить партнеров и поставщиков соответствующей информацией о стандартах, процедурах и политике организации.

Модель системы информационной безопасности организации – это совокупность внешних и внутренних факторов, их влияние на состояние информационной безопасности предприятия и обеспечение сохранности ресурсов. На рисунке 3 приводится модель системы управления информационной безопасностью организации.



Рисунок 3 – Модель системы управления информационной безопасностью организации

В данной модели представлены направления воздействия между следующими факторами:

- угрозами информационной безопасности, которые характеризуются вероятностью возникновения и реализации;
- уязвимостью системы информационной безопасности, влияющей на вероятность реализации угрозы;
- рисками, отражающими предполагаемый ущерб в результате реализации угрозы информационной безопасности.

Информация и материальные ресурсы, которые необходимо защищать, называются объектами защиты.

К ним относятся:

- информация в любом её виде;
- информация, хранимая и обрабатываемая посредством средств связи в виде различных носителей;
- технические средства связи и информатизации;
- помещения, предназначенные для обсуждения, обработки и хранения информации;
- информационные системы в целом, включая системы связи;
- документация на технические и программные средства связи и информатизации;
- программные средства.

Угрозы, с которыми может столкнуться образовательная организация, классифицируются по природе их возникновения, т.е. угрозы случайного или преднамеренного характера, и по тому, как они относятся к защищаемому объекту, т.е. внешние и внутренние угрозы (рисунок 4).



Рисунок 4 – Источники внутренних и внешних угроз

Нарушения в образовательной организации могут быть нескольких видов.

Организационно-правовые – это нарушения, связанные с отсутствием единой согласованной политики предприятия в сфере защиты информации, невыполнением требований нормативных документов, режимом доступа, хранения и уничтожения информации.

Организационные виды нарушений включают несанкционированное получение доступа к базам и массивам данных, несанкционированный доступ к активному сетевому оборудованию, серверам, некорректное встраивание средств защиты и ошибки в управлении ими, нарушения в адресности рассылки информации при ведении информационного обмена.

Под *физическими видами* нарушений подразумеваются повреждение аппаратных средств автоматизированных систем, линий связи и коммуникационного оборудования, кражи или несанкционированное ознакомление с содержанием носителей информации, их хищение.

К *радиоэлектронным видам* нарушений относятся, фотографирование мониторов, навязывание ложной информации в локальных вычислительных сетях, передаче данных и линиях связи.

Для противодействия угрозам и пресечения нарушений в организации организуется процесс управления рисками, который является основой системы управления информационной безопасностью организации.

Построение эффективной системы информационной безопасности – это комплексный процесс, направленный на минимизацию внешних и внутренних угроз при учете ограничений на ресурсы и время.

С точки зрения процессного подхода СУИБ организации можно представить, как процесс управления рисками, представленный на рисунке 5.

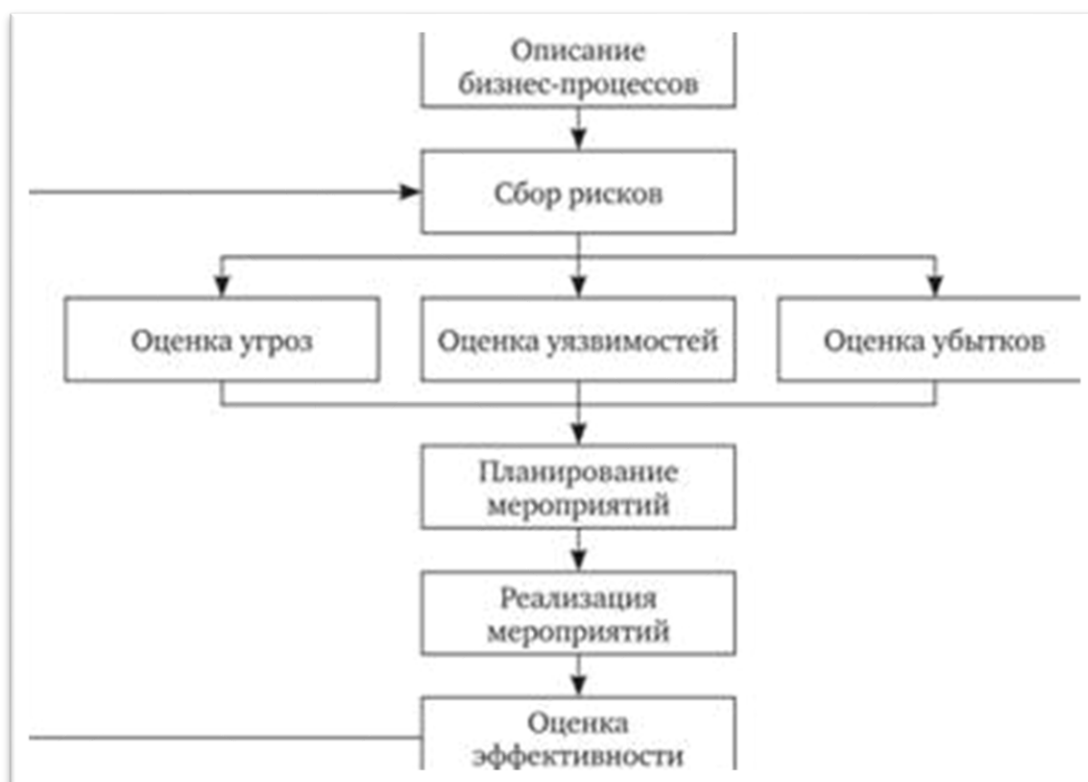


Рисунок 5 – Модель процесса управления рисками для системы информационной безопасности

Этот процесс включает в себя следующие составляющие.

1. *Описание бизнес-процессов.* Выполняется корректировка и анализ бизнес-процессов. По критериям, которые определяются в ходе формирования политики в области рисков, осуществляется идентификация бизнес-процессов.

2. *Сбор рисков.* Проводится для выявления степени подверженности предприятия угрозам, которые могут нанести существенный ущерб. Для этого осуществляется анализ его бизнес-процессов и опрос экспертов предметной области. Результатом (выходом) данного процесса считается классификационный перечень всех потенциальных рисков.

К стандартным рискам информационной безопасности относятся:

- изъятие конфиденциальной информации с локальных мест;
- преднамеренное изменение информации с целью уничтожения;
- копирование важных документов и передача конкуренту;
- незаконное проникновение в корпоративную сеть;

- уничтожение по техническим причинам.

3. *Оценка рисков.* Определяются характеристики рисков и ресурсы информационной системы. Основным результатом (выходом) данного процесса является перечень всех потенциальных рисков с их количественными и качественными оценками ущерба и возможности реализации, а дополнительным – перечень рисков, которые не будут отслеживаться на предприятии.

Процесс оценки рисков состоит из следующих шагов:

- описание объекта и мер защиты;
- идентификация ресурса и определение его количественных показателей;
- анализ угроз информационной безопасности;
- оценка уязвимостей;
- оценка существующих и предполагаемых средств обеспечения информационной безопасности.

4. *Планирование мероприятий.* Целью планирования мероприятий по минимизации рисков является определение сроков и перечня работ по исключению или минимизации ущерба в случае минимизации риска.

Выделяются следующие виды мероприятий по информационной безопасности:

- организационные;
- правовые;
- организационно-технические;
- программные;
- инженерно-технические.

5. *Реализация мероприятий.* Под реализацией мероприятий по минимизации рисков подразумеваются выполнение запланированных работ, контроль качества полученных результатов и сроков. Результатом данного процесса являются выполненные работы по минимизации рисков и время их проведения.

6. *Оценка эффективности.* Оценка эффективности системы управления информационной безопасностью – это системный процесс получения и оценки объективных данных о текущем состоянии системы, действиях и событиях, происходящих в ней, устанавливающий уровень их соответствия определенным критериям.

Целями процесса являются:

- оценка текущего уровня эффективности системы;
- локализация «узких» мест в системе;
- оценка соответствия системы предприятия существующим стандартам в области информационной безопасности;
- выработка рекомендаций и регламентов по обеспечению безопасности объектов защиты.

Управление информационной безопасностью — это циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

1.2. Методы управления информационной безопасностью в образовательной организации

Управление информационной безопасностью в образовательной организации представляет собой многосторонний, разнопрофильный, и циклический процесс, который включает в себя множество подкатегорий проведения различных видов работ.

К ним относятся:

- создание мер по обработке информации;
- сбор, аналитика информации о текущем состоянии ИБ в организации;
- выявление необходимого уровня обеспечения ИБ организации;
- формирование соответствующих задач для профильных специалистов;
- оценивание информационных рисков;
- интеграция и формирование необходимых механизмов по контролю, распределению ролей и ответственности;
- обучение, повышение цифровой грамотности сотрудников и педагогических работников в сфере ИБ;
- оперативность реализации требуемых мероприятий по защите информации;
- отслеживание функционирования используемых механизмов контроля, оценка их эффективности, внедрение необходимых изменений в их работу, если требуется.

Управление информационной безопасностью актуально для образовательной организации, так она имеет разветвленную ИТ-инфраструктуру, которая требует грамотно отлаженного координирования.

Методы управления информационной безопасностью — это совокупность приемов и способов воздействия на управляемый объект для достижения поставленных целей.

В системе методов управления информационной безопасностью можно выделить:

- административные;
- инженерно-технические;
- правовые;
- теоретические;
- экономические;

— социально-психологические.

Административные методы ориентированы на мотивы поведения сотрудников, как осознанная необходимость дисциплины труда и сохранения корпоративных секретов, чувства долга и ответственности за информационную безопасность всей организации, стремление человека трудиться в определённой организации, сохраняя конфиденциальную информацию. При этом на сотрудников может возлагаться материальная ответственность, которая выражается в их обязанности возместить ущерб, причинённый организации, на котором они работают при разглашении конфиденциальной информации или нанесении ущерба информационной инфраструктуре. Административные методы управления являются мощным рычагом достижения поставленных целей только в тех случаях, когда нужно подчинить весь коллектив и направить его на решение конкретной задачи. Одним из административных методов является наставление (метод однократного применения со стороны руководителя), когда руководитель аргументированно объясняет подчиненным целесообразность введения мер по защите информации.

Организационно-административные методы, базирующиеся на власти, дисциплине и ответственности, осуществляются как прямое административное указание и адресуются конкретным лицам, отвечающим за информационную безопасность всего предприятия. При этом устанавливаются правила, регулирующие деятельность подчиненных по соблюдению законов РФ по защите информации, издаются указы и распоряжения, подписанные руководителем организации, разрабатываются рекомендации по организации и совершенствованию политики безопасности. Контроль и надзор за деятельностью сотрудников по обеспечению защиты информации возлагается на руководителей подразделений, отделов и отдельных сотрудников. Организационно-административные методы, включающие рекомендации и разъяснение, отличается от других методов четкая адресность директив, обязательность выполнения распоряжений, приказов и

указаний. Невыполнение сотрудниками приказов администрации по информационной безопасности рассматривается как прямое нарушение исполнительской дисциплины и влечет за собой определенные взыскания - предупреждение, штрафы и увольнение.

Инженерно-технические методы – это методы, которые помогают обеспечить защиту информации от утечки по техническим каналам, разработать и внедрить механизмы защиты информации, обрабатываемой на рабочих местах сотрудников в персональных компьютерах и корпоративных сетях. К ним относятся ограничения по использованию сети Интернет, установка антивирусного программного обеспечения, запрет использования флэш-карт и т.д.

Правовые методы – это методы защиты информации призваны чтобы создать и использовать нормативную базу, которую будут составлять федеральные законы и локальные акты организации.

Теоретические методы направлены на создание моделей управления доступом к информации, описание возможных информационных потоков в системе, что гарантирует выполнение требуемых свойств безопасности и проведение сертификации автоматизированных систем.

Экономические методы – это методы, которые направлены на материальное стимулирование всего коллектива и отдельных сотрудников, которые строго соблюдают все правила, приказы и требования руководителей по обеспечению информационной безопасности в организации. Дополнительное вознаграждение (премии разовые или квартальные, годовые, памятные подарки) могут получать сотрудники, которые внесли индивидуальный вклад в конечные результаты по обеспечению защиты информации в конкретные периоды времени.

Социально-психологические методы – это методы воздействия на сотрудников, которые позволяют установить назначение и место каждого сотрудника в обеспечении сохранности информации, выявить лидеров и обеспечить их поддержку, связать мотивацию людей с конечными

результатами работы по обеспечению ИБ всей организации, обеспечить эффективные коммуникации при обмене опытом и разрешении конфликтов, возникающих при утечке информации, поддерживать корпоративную культуру. К способам воздействия относятся убеждение в необходимости строгого соблюдения правил политики ИБ, вовлечение в процесс защиты информации, осуждение и порицание при утечки корпоративной информации, требование строго соблюдать законы РФ и приказы администрации, запрещение несанкционированного обмена информацией с другими организациями.

Данные методы управления ИБ находятся в постоянном динамическом равновесии, где каждый компонент дополняет другой и игнорирование одного из методов может привести к потере информации и негативно отразиться на образовательной организации.

1.3. Характеристика объекта исследования ГБПОУ «ЮУГК»

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа.

Главной целью и направлением деятельности образовательной организации является повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на системе электронного обучения E-Learning, электронных учебно-методических комплексах, а также компетентностном подходе. Данные технологии и формы обучения позволили повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда. На протяжении многих лет «Южно-Уральский государственный колледж» занимается разработкой и внедрением в учебном процессе интенсивных информационных образовательных технологий, основанных на широком

использовании компьютерной и коммуникационной техники, электронных обучающих программ, проектной культуры. Это позволяет активно решать проблемы доступности, эффективности и качества профессиональной подготовки современных специалистов для отраслей предприятий России.

Педагоги колледжа имеют опыт практической работы и глубокую теоретическую подготовку, необходимую для успешной реализации профессиональных образовательных программ. Среди них — кандидаты наук, заслуженные работники образования Российской Федерации, преподаватели высшей категории.

Для эффективного взаимодействия с учетом большого контингента обучающихся и месторасположением учебных зданий после реорганизации были присоединены два колледжа ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматике» и ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматике», которые в дальнейшем определили три образовательных комплекса:

- Информационных технологий и экономики (ул. Курчатова, д.7).
- Промышленной автоматике (ул. Доватора, д.38).
- Промышленного дизайна и торговли (ул. Блюхера, ул.1А).

В образовательной организации обоснованно распределены функции структурных подразделений учреждения, а также должностные обязанности его работников на основе сочетания принципов единоначалия и коллегиальности.

ГБПОУ «ЮУГК» возглавляет директор, обеспечивающий системную работу организации, определяющий стратегию, цели, задачи и программу его развития, обеспечивающий соблюдение законности в деятельности колледжа, а также осуществляющий иные функции и полномочия, соответствующие уставным целям.

По основным направлениям деятельности управление осуществляется заместителями директора, координирующими работу структурных подразделений ГБПОУ «ЮУГК».

В колледже действуют предметно-цикловые комиссии, деятельность, осуществляющих образовательную деятельность по родственным учебным дисциплинам/модулям, в том числе по совместительству. ГБПОУ «ЮУГК» уделяет большое внимание компьютеризации образовательного процесса.

В колледже оборудованы специализированные лаборатории и студии, для всех направлений обучения.

Для оптимизации учебной деятельности организация владеет всеми необходимыми современными программными пакетами: Microsoft Visio, Cisco Packet Tracer, Microsoft Visual Studio, Dev C++, SASM, Microsoft SQL Server 2017, SQL Management Studio, Android Studio, CorelDraw X4, Atom, Notepad++, Corel Photo Paint, Blender, Unity, Adobe Flash Professional CS6, Open Server, Oracle Virtual Box, IntelliJ IDEA, JDK, Free Pascal, Inkscape, GIMP, 1С Предприятие.

Используются 33 электронных курса по учебным дисциплинам, междисциплинарным курсам и профессиональным модулям.

При подготовке специалистов по всем реализуемым основным образовательным программам используются электронные системы обучения (электронные учебники, электронные таблицы, презентации отдельных тем и предметов, лабораторные и практические работы, обучающие программы на дисках, тестовый контроль).

Система управления ГБПОУ «ЮУГК», обеспечивающая реализацию образовательных программ, являющихся основной целью деятельности учреждения, отвечает требованиям действующего законодательства Российской Федерации и Челябинской области. Организационная структура управления ГБПОУ «Южно-Уральский государственный колледж» (рисунок 6).

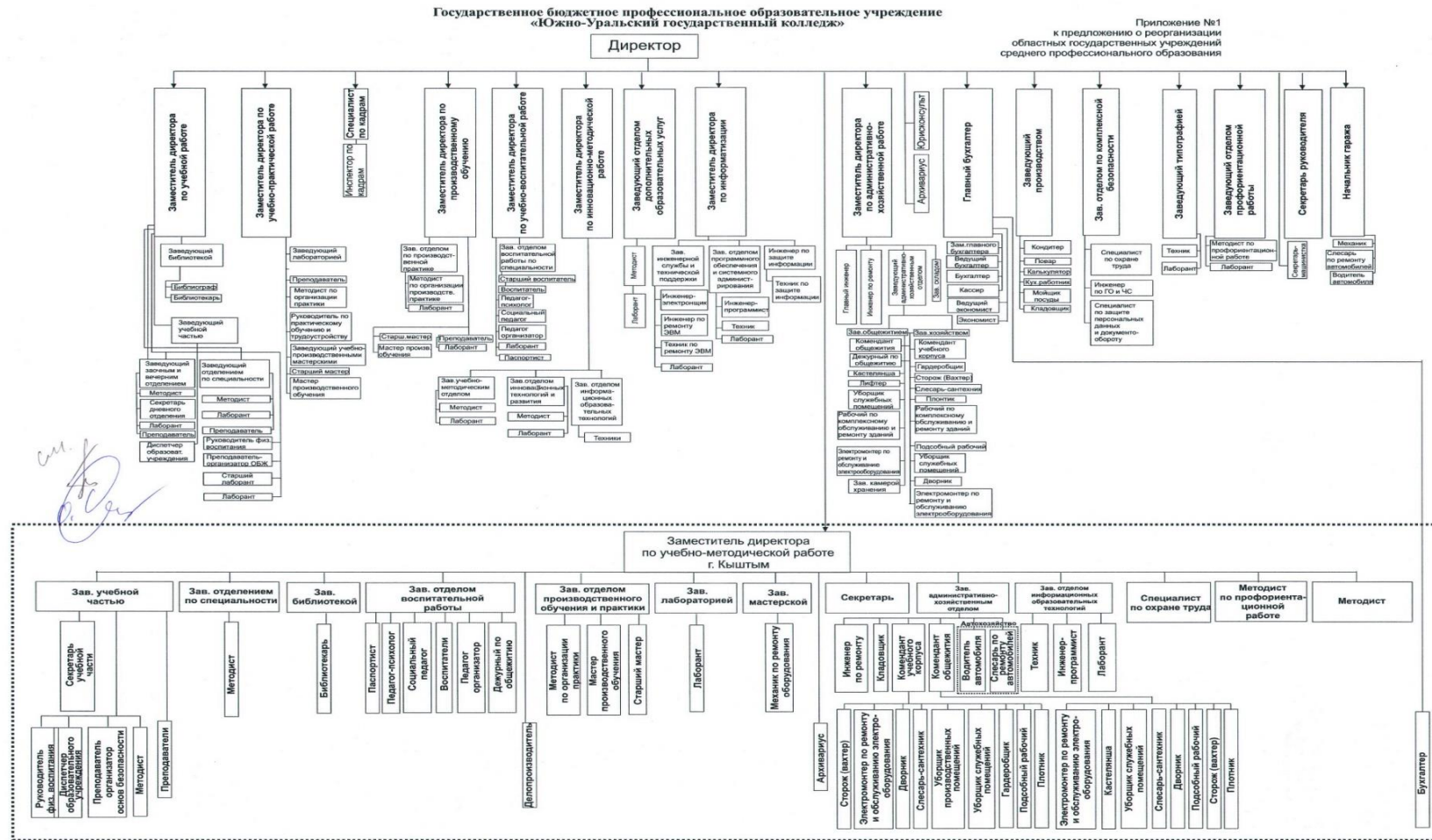


Рисунок 6 – Организационная структура управления ГБПОУ «Южно-Уральский государственный колледж»

Для обеспечения учебного процесса цикловые комиссии и отделы ГБПОУ «ЮУГК» оснащены персональными компьютерами и необходимой техникой. Для решения производственных и учебных задач в колледже организована локальная сеть на одновременную работу 678 компьютеров. Все персональные компьютеры оснащены лицензионным программным обеспечением, подключены к локальной сети и имеют доступ в сеть Интернет, через защищенное соединение. Узлы оптических линий оборудованы управляемыми коммутаторами. В каждом комплексе имеется своя локальная сеть (100/1000 Мбит/с), охватывающая учебные корпуса и общежития. Создана единая локальная сеть колледжа (оптоволокно). В комплексах все компьютеры подключены к сети Интернет со скоростью доступа до 100 Мбит/с. На программном уровне защиты используются различные для студентов и сотрудников домены.

В колледже организована система электронного обучения – Moodle, она доступна для сотрудников и студентов колледжа, каждый имеет свой индивидуальный пароль и логин, доступ к системе возможен с любых устройств. Портал построен на основе системы управления образованием (LMS). LMS позволяет управлять и распространять учебный материал и обеспечивать совместный доступ. Открыт доступ к электронным образовательным ресурсам для студентов колледжа по сети Интернет, что позволяет использовать данные ресурсы в полном объеме.

ГБПОУ «ЮУГК» занимается разработкой и внедрением в учебном процессе интенсивных информационных образовательных технологий, основанных на широком использовании компьютерной и коммуникационной техники, электронных обучающих программ, проектной культуры. Это позволяет активно решать проблемы доступности, эффективности и качества профессиональной подготовки современных специалистов для отраслей предприятий России. Однако внедрение и использование в учебном процессе большого количества информационных технологий, а также выход в сеть

Интернет могут провоцировать реализацию различных информационных угроз.

Источники информационных угроз можно классифицировать по расположению на внутренние и внешние угрозы. К внутренним угрозам относятся сотрудники организации, в том числе обслуживающий персонал, педагогический состав, а также обучающиеся. К внешним угрозам следует отнести организации-конкуренты, хакеры, бывшие сотрудники, преподаватели, студенты.

Так же источниками угроз будут являться:

- компьютеризированные учебные аудитории, в которых происходит учебный процесс;
- сеть Интернет;
- рабочие станции неквалифицированных в сфере ИБ работников.

В колледже в качестве методов управления информационной безопасностью используются:

- административно-организационные методы;
- технические методы;
- правовые методы.

Правовые методы нашли отражение в серии документов, регламентирующих все аспекты обеспечения информационной безопасности в организации. К этим документам относятся:

- Федеральный закон РФ от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
- Федеральный закон от 29.12.2010 №436-ФЗ (ред. от 29.06.2015) «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).
- Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).

— Документы, регламентирующие работу с персональными данными.

— Внутренние нормативные акты в сфере обеспечения информационной безопасности обучающихся.

Правовые методы используются при устройстве на работу, и заключаются в ответственности за разглашение персональных данных. К правовым методам относится политика безопасности колледжа. Политика безопасности, реализована на избирательном способе управления доступом. Применение избирательной политики, соответствует требованиям по информационной безопасности, разграничению доступа, подотчетности. Реализацией этой политики безопасности занимается системный администратор. Такое управление характеризуется заданным администратором множеством разрешенных отношений доступа. Чтобы предотвратить неумышленное разглашение персональных данных, каждый сотрудник подписывает приложение к трудовому договору, в котором прописана ответственность за распространение данных.

Недостатком является отсутствие в общем доступе, то есть на сайте ГБПОУ «ЮУГК» необходимой информации для ознакомления.

Организационно-техническая защита информации оперирует доступом к информации, подразумевая ограничение на работу с ней, разграничение полномочий лиц и контроль. К этим мерам относится инструктаж сотрудников, обеспечение программно-технических работ; назначение лиц, отвечающих за конкретные оборудование; физическую охрану объектов; оборудование помещения металлическими решетками, дверями, замками.

Вход на территорию осуществляется по персональным пропускам и студенческим билетам. Посетители имеют право прибывать на территории только в сопровождении сотрудника организации. В колледже осуществлена пожарно-охранная сигнализация и установлены соответствующие датчики. Непреднамеренные действия сотрудников, такие как модификация, удаление

или блокирование информации в результате неумышленных действий предотвращается разграничением прав доступа, парольной защитой.

Административно-технические методы построены на создании внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями. К ним относятся должностные инструкции, перечни сведений, не подлежащих передаче, различные регламенты, определяющие порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и документов.

К *физическим методам* относится пропускная система в помещения колледжа, раз в месяц проводится резервное копирование на локальную машину, это позволяет предотвратить потерю информации при реализации естественных угроз природного явления, таких как грозы или перегрузки систем, непреднамеренных и злоумышленных действий сотрудников и обучающихся колледжа. Организована система авторизации пользователей, прежде всего, это пароль входа пользователя в операционную систему его рабочего места. Ввод этого пароля открывает доступ к ресурсам данного компьютера и к документам, хранящимся на нем.

Для обучающихся есть единый пароль и логин, для сотрудников и педагогов предусмотрена замена пароля 1 раз в 3 месяца. Когда пользователь вводит свой пароль для входа в операционную систему, он получает доступ не только к ресурсам данного компьютера, но и к ресурсам локальной компьютерной сети.

Технические методы представляют собой комплекс работ, направленных на сохранение всех информационных активов образовательной организации. В качестве программного средства защиты от вредоносного программного обеспечения используется антивирусное решение «Kaspersky Endpoint Security для Windows», которая отвечает требованиям надежности, качества и системы защиты, предъявляемым для защиты корпоративных сетей. Предусмотрены контент-фильтры, ограничивающие доступ обучающихся на сайты с неправомерной информацией.

В ходе исследования удалось выявить ряд недостатков в области информационной безопасности:

1. В колледже отсутствуют инструкции, определяющие порядок доступа обучающихся к сети Интернет в компьютерных классах.

2. Сотрудники колледжа несут ответственность только за разглашение персональных данных, в других случаях понятие ответственности «размыто».

3. В случае перехода на дистанционное обучение сайт колледжа не выдерживает большого потока посетителей, поэтому нередки случаи Ddos-атак и срыва занятий.

4. Участники образовательных отношений не выполняют элементарные основы информационной безопасности.

Выводы по первой главе

Система управления информационной безопасностью (СУИБ) является частью общей системы управления, базирующейся на анализе рисков и предназначенной для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности. СУИБ составляют организационные структуры, политика, действия по планированию, обязанности, процедуры, процессы и ресурсы.

Фактором эффективности системы управления информационной безопасностью является ее построение на базе стандарта ГОСТ Р ИСО/МЭК 27004-2021 «Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».

Стандарт ГОСТ Р ИСО/МЭК 27004-2021 определяет принципы и является руководством по разработке, внедрению, сопровождению и улучшению системы управления информационной безопасностью, а также описывает механизмы определения целей контроля, а так же устанавливает требования к системе управления информационной безопасностью организации, является руководством по определению, минимизации и управлению опасностями и угрозами, которым может подвергаться информация, и разработан в целях обеспечения помощи в выборе эффективных и адекватных средств для его защиты.

Управление информационной безопасностью актуально для образовательной организации, так она имеет разветвленную ИТ-инфраструктуру, которая требует грамотно отлаженного координирования.

Методы управления информационной безопасности — это совокупность приемов и способов воздействия на управляемый объект для достижения поставленных целей.

В системе методов управления информационной безопасностью можно выделить:

- административные;
- инженерно-технические;

- правовые;
- теоретические;
- экономические;
- социально-психологические.

В ходе исследования удалось выявить ряд недостатков в области информационной безопасности:

1. В колледже отсутствуют инструкции, определяющие порядок доступа обучающихся к сети Интернет в компьютерных классах.

2. Сотрудники колледжа несут ответственность только за разглашение персональных данных, в других случаях понятие ответственности «размыто».

3. В случае перехода на дистанционное обучение сайт колледжа не выдерживает большого потока посетителей, поэтому нередки случаи Ddos-атак и срыва занятий.

4. Участники образовательных отношений не выполняют элементарные основы информационной безопасности.

ГЛАВА 2. Реализация эффективных методов управления информационной безопасностью в образовательной организации ГБПОУ «ЮУГК»

2.1. Рекомендации по реализации эффективных методов управления информационной безопасностью ГБПОУ «ЮУГК»

Любая организация, которая в своей деятельности обрабатывает персональные данные, обязана предпринять комплекс организационных и технических мер, направленных на их защиту. В ГБПОУ «ЮУГК» должны быть защищены главные компоненты ИБ: целостность, конфиденциальность и доступность информационных ресурсов. Поэтому в систему обеспечения информационной безопасности решено включить следующие эффективные методы управления ИБ ГБПОУ «ЮУГК»: организационно-административные методы, которые будут направлены на сотрудников организации и предполагают, что за нарушение ИБ будут предусмотрены предупреждения, штрафы и увольнение.

Организационно-административные методы регламентируют процессы создания и эксплуатации информационных объектов, а также взаимодействие пользователей и систем таким образом, что несанкционированный доступ к информации становится либо невозможным, либо существенно затрудняется.

Организационно-административные методы защиты информации охватывают все компоненты автоматизированных информационных систем на всех этапах их жизненного цикла: проектирования систем, строительства зданий, помещений и сооружений, монтажа и наладки оборудования, эксплуатации и модернизации систем.

К организационно-административным мероприятиям защиты информации относятся:

— использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;

— организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации

— организация регламентированного доступа пользователей, средствах связи и в хранилищах носителей конфиденциальной информации,

— установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;

— разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации, постоянный контроль за соблюдением установленных требований по защите информации.

Предполагается обновить локальные акты ГБПОУ «ЮУГК» и дать ознакомиться всем сотрудникам, имеющим доступ к персональным данным.

Сотрудники организации должны участвовать в различных аспектах программы информационной безопасности и обладать соответствующими навыками и знаниями. Необходимый уровень профессионализма сотрудников может быть достигнут с помощью тренингов, проводить которые могут как специалисты организации, так и внешние консультанты.

Компетентность пользователей является обязательным условием для успешного обеспечения информационной безопасности, а также позволяет гарантировать, что средства контроля работают должным образом. Пользователи не могут следовать политике, которую они не знают или не понимают. Не зная о рисках, связанных с информационными ресурсами организации, они не могут видеть необходимости исполнения политики, разработанной с целью уменьшения рисков.

Должно проходить непрерывное обучение пользователей и других сотрудников на примере рисков и соответствующих политик

Руководящая группа должна обеспечить стратегию постоянного обучения сотрудников, так или иначе влияющих на информационную безопасность организации. Группа должна сосредоточить усилия на всеобщем понимании рисков, связанных с информацией, обрабатываемой в организации, а также политиках и методах (средствах) контроля, направленных на уменьшение этих рисков.

Руководящая группа должна использовать разнообразные методы обучения и поощрения чтобы сделать политику организации доступной и обучить пользователей. Стоит избегать встреч, проводимых раз в год со всеми сотрудниками организации, обучение лучше проводить в небольших группах сотрудников.

В данном случае можно прибегнуть к курсам повышения квалификации для сотрудников в области информационной безопасности, которые проводит региональный учебно-научный центр «Информационная безопасность» Южно-Уральского государственного университета. Программы повышения квалификации рассчитаны на 72 часа. По окончании программ выдается Удостоверение о повышении квалификации. Центр предлагает 5 программ на выбор, рассчитанный на разные категории слушателей.

1. «Защита персональных данных». В рамках курса изучается весь комплекс мероприятий по обеспечению правомерности обработки персональных данных с использованием правовых, организационных и технических мер, способы снижения рисков утечки персональных данных и наложения штрафных санкций со стороны государственных надзорных органов.

2. «Защита коммерческой тайны». В курсе изучаются особенности российского законодательного регулирования вопросов защиты исключительных прав на секреты производства, закрепленные в Федеральном законе от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и в других нормативных актах, а также технологии установления и поддержания режима коммерческой тайны в организации. Особое внимание уделяется

формированию перечня сведений, составляющих коммерческую тайну, разработке и вводу в действие внутренних нормативных документов предприятия, регулированию трудовых отношений, связанных с доступом к коммерческой тайне, процедуре заключения лицензионных договоров, договоров об отчуждении исключительных прав на секреты производства и коммерческой концессии, особенностям представления информации о коммерческой тайне в органы власти, порядку проведения совещаний с контрагентами, на которых раскрывается коммерческая тайна, способам минимизации рисков, вызванных угрозами конфиденциальным сведениям.

3. «Расследование компьютерных инцидентов». В курсе изучаются все аспекты деятельности службы безопасности (отдела информационной безопасности) организации при реагировании на инциденты в информационной системе, в том числе – методика предупреждения таких инцидентов, ликвидации нанесенного ими ущерба, пресечения хакерской активности, перекрытия каналов незаконного съема информации и выявления виновных лиц. Слушатели изучают методики анализа рисков и уязвимостей безопасности информационных систем организации, основные способы обеспечения непрерывности функционирования информационной системы в случае возникновения компьютерных инцидентов и скорейшего устранения их последствий. В завершение курса слушатели самостоятельно проводят полный цикл расследования компьютерных инцидентов с составлением необходимых документов.

4. «Документирование защиты информации и организация конфиденциального делопроизводства». Цель курса – подготовка слушателей к проведению комплекса мероприятий по защите информации в организации с учетом требований нормативно-правовых документов, регламентирующих защиту информации в организации, в том числе – информации ограниченного доступа и ведения конфиденциального делопроизводства. Особое внимание уделяется практическим аспектам реализации всего процесса конфиденциального делопроизводства – от составления перечня информации

ограниченного доступа до особенностей электронного конфиденциального документооборота, использования электронной цифровой подписи. Детально рассматриваются обязанности сотрудников, организующих, осуществляющих и контролирующих конфиденциальное делопроизводство. Специалисты, обучающиеся на курсе, получают практические знания и навыки, позволяющие создать или усовершенствовать существующую систему конфиденциального делопроизводства на предприятиях и в организациях любой формы собственности и отраслевой принадлежности.

5. «Культура информационной безопасности». Актуальность программы обусловлена, во-первых, технологизацией образовательного процесса, а, следовательно, – возрастающими требованиями к развитию компьютерной грамотности руководителя, учителя, специалиста муниципальных образовательных учреждений, во-вторых, – существующими тенденциями современного информационного общества, которые повышают зависимость безопасности общества, каждого конкретного человека от качества информационной инфраструктуры, достоверности, целостности используемой информации, ее защищенности от несанкционированной модификации. Обучение направлено на формирование навыков работы с офисными программами и Интернетом, изучение основ защиты информации, а также развитие компетенций в области обеспечения личной информационно-психологической безопасности и защиты детей, подрастающего поколения от негативных информационных воздействий (агрессия, экстремизм, деструктивные организации, зависимость от информационного шума, сообщества в социальных сетях, провоцирующих суицидальное поведение и пр.). Программа рассчитана на специалистов образовательных учреждений.

Слушателям предлагаются также курсы повышения квалификации по программам «Программно-аппаратная защита информации», «Криптографическая защита информации», «Инженерно-техническая защита информации» и др.

Обучение в РУНЦ ИБ ЮУРГУ ведется по модульному принципу с использованием дистанционных технологий. Кроме образовательной деятельности Центр активно ведет научные и хозяйственные исследования по актуальным проблемам защиты информации.

В качестве инженерно-технических методов, организация может приобрести специализированное решение для управления ИБ.

Обработать вручную большое количество инцидентов нарушений ИБ и выявить инциденты невозможно. Для этого предложено использовать специализированные решения SIEM (Security Information and Event Management) для автоматизации данных процессов. Приложение собирает и автоматически анализирует события различных корпоративных систем с целью выявления угроз и нарушений политик ИБ. Сложный механизм работы SIEM сводится к довольно простому алгоритму (рисунок 7).



Рисунок 7 – Алгоритм работы SIEM

Для ГБПОУ «ЮУГК» было выбрано решение «KOMRAD Enterprise SIEM». Это гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации. Она позволяет осуществлять централизованный сбор событий ИБ, выявлять инциденты ИБ и оперативно на них реагировать. Применение комплекса позволяет эффективно

выполнять требования, предъявляемые регуляторами к защите персональных данных, к обеспечению безопасности государственных информационных систем и контролю критической информационной инфраструктуры предприятия. КОМРАД позволяет отправлять данные о событиях и инцидентах ИБ во внешние системы.

КОМРАД Enterprise SIEM реализует следующие меры информационной безопасности:

- сбор, запись и хранение информации о событиях безопасности;
- обнаружение, идентификация и регистрация инцидентов;
- информирование об инцидентах и реагирование;
- хранение событий в течение необходимого срока;
- управление активами;
- просмотр и анализ информации о действиях пользователей;

Лицензии на КОМРАД Enterprise SIEM являются бессрочными, стоимость определяется составом коллекторов и возможностью масштабирования решения (таблица 1).

Таблица 1 – Виды лицензий КОМРАД Enterprise SIEM

Показатель	Ничего лишнего	Все в одном	Безлимит
	Base	All-in-One	Enterprise
Цена	500 000 руб.	1 500 000 руб.	2 500 000 руб.
Syslog	1 на выбор	1	2
WMI		1	2
СУБД		1	2
Файловый		1	2
SNMP		1	2
Кол-во событий	500	Без ограничений	
Сертификат на обучение сотрудников администрированию	0	1	2
Территориально-распределенная установка	Нет		Да
Техническая поддержка	1 год уровня «Стандарт» включена в стоимость лицензии		

Графический конструктор директив делает процесс работы с директивами корреляции простым и наглядным (рисунок 8).

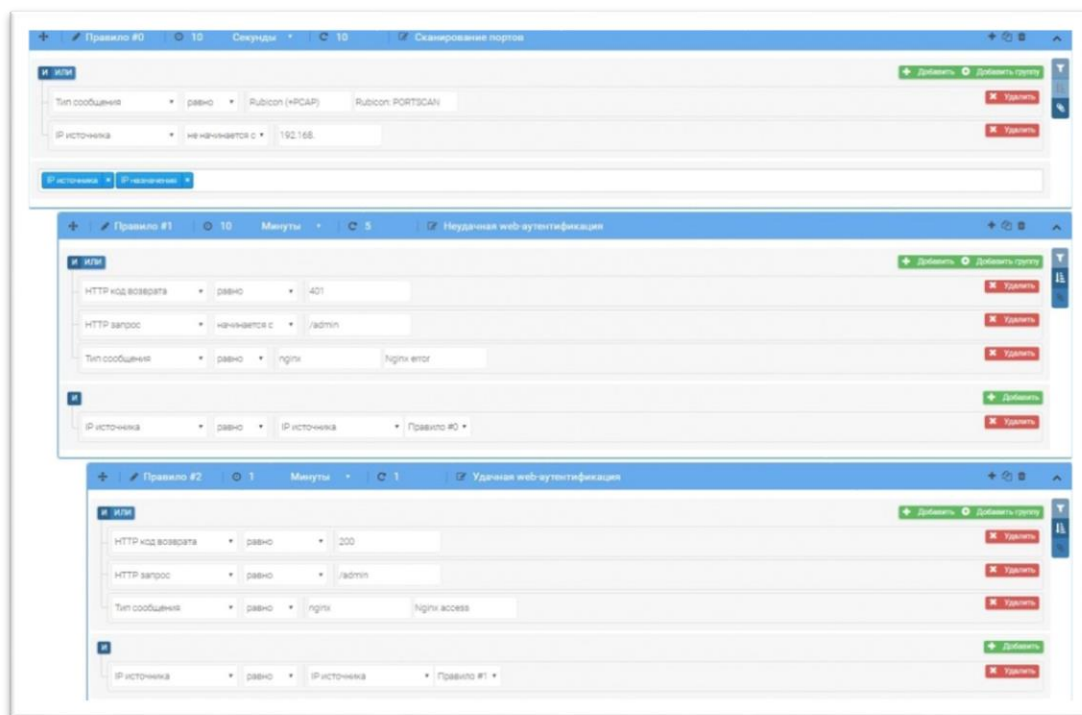


Рисунок 8 – Графический конструктор директив

Каждое правило директивы формируется при помощи графического конструктора запросов. Обновленный механизм наследования между правилами расширяет диапазон задач, решаемых с помощью модуля корреляции. Предусмотрено визуальное иерархическое разделение правил по уровням. Для удобного просмотра «большой» директивы реализована возможность свернуть правило.

Средство для визуального анализа инцидента избавляет администратора ИБ от необходимости ручного анализа таблиц из тысяч событий при расследовании инцидента (рисунок 9).

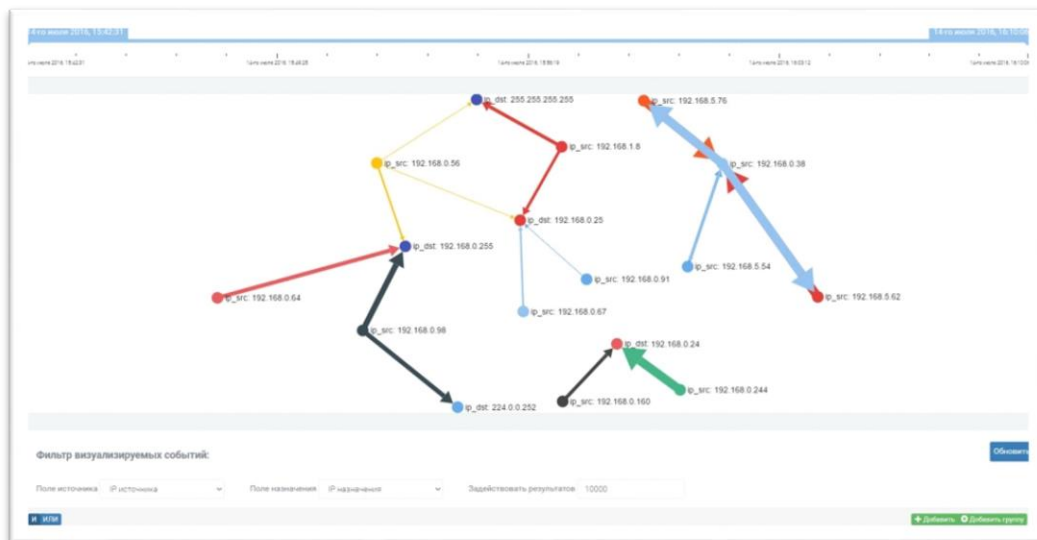


Рисунок 9 – Визуализация событий

Система позволяет пользователю построить визуальную модель совокупности событий и отследить развитие инцидента во времени. Визуализация событий облегчает проведение анализа атаки и расследование инцидента.

Графический конструктор запросов позволяет строить запросы к базе событий любой сложности без единой строчки на языке сценариев.

Любой запрос можно сохранить в системе, задав ему название и описание (рисунок 10).

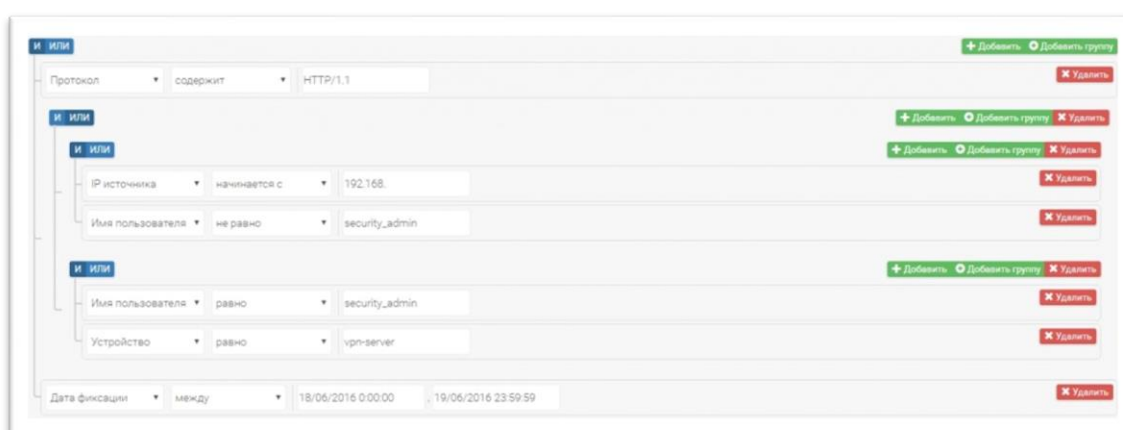


Рисунок 10 – Графический конструктор запросов

В обновленной подсистеме визуализации есть возможность строить графики и диаграммы для произвольной выборки событий и сохранять их в

виджете. Виджет — это интерактивный блок визуализации данных, отражающий динамику их изменения в системе. Каждый виджет имеет ряд параметров для гибкой настройки под конкретные потребности пользователя системы (рисунок 11).

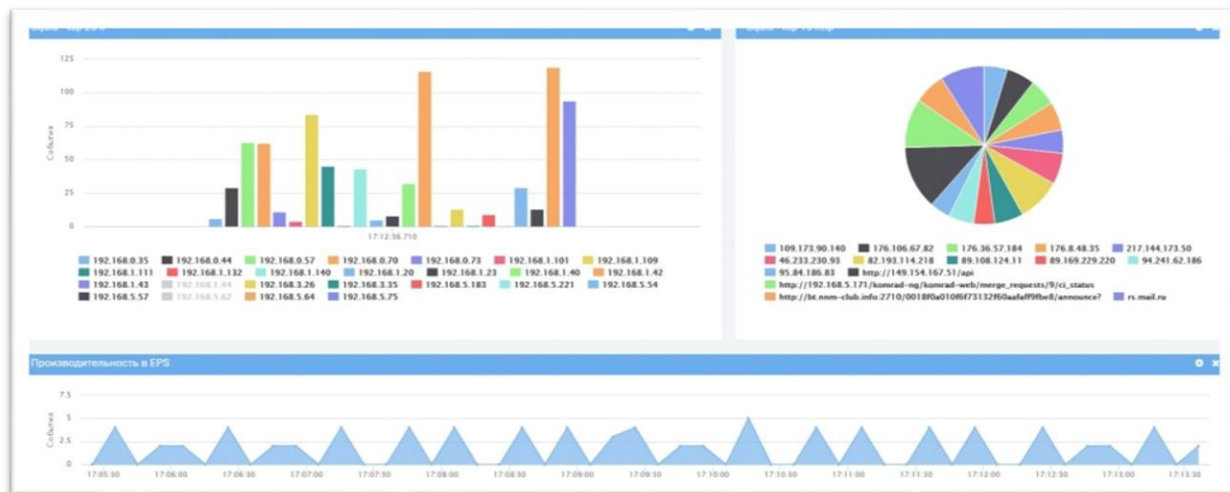


Рисунок 11 – Визуализация событий с помощью виджета

Система позволяет осуществлять контроль соответствия требованиям различных нормативных актов и стандартов информационной безопасности (рисунок 12).

Идентификатор	Наименование	Цель	Статус	Действие	Примечание
A.5.1	Политика информационной безопасности	Цель: Обеспечить участие высшего руководства организации в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами	Применяется	Реализовано	None
A.5.1.1	Документирование политики информационной безопасности		Применяется	Реализовано	None
A.5.1.2	Анализ политики информационной безопасности		Применяется	Реализовано	None
A.6 Организация информационной безопасности					
A.6.1	Внутренняя организация	Цель: Обеспечение управления информационной безопасностью в организации			
A.6.1.1	Обязанности руководства по обеспечению информационной безопасности		Применяется	Реализовано	None
A.6.1.2	Координация вопросов обеспечения информационной безопасности		Применяется	Не реализовано	None
A.6.1.3	Распределение обязанностей по обеспечению информационной безопасности		Применяется	Реализовано	None
A.6.1.4	Процедура получения разрешения на использование средств обработки информации		Применяется	Реализовано	None
A.6.1.5	Соглашения о соблюдении конфиденциальности		Применяется	Реализовано	None
A.6.1.6	Взаимодействие с компетентными органами		Применяется	Реализовано	None
A.6.1.7	Взаимодействие с ассоциациями и профессиональными группами		Не применяется	Не реализовано	None
A.6.1.8	Независимая проверка (аудит) информационной безопасности		Применяется	Не реализовано	None

Статистика

- A.5 Политика безопасности
- A.6 Организация информационной безопасности
- A.7 Управление активами
- A.8 Правила безопасности, связанные персоналом
- A.9 Физическая защита и защита от воздействия окружающей среды
- A.10 Управление средствами коммуникаций и их функционированием
- A.11 Контроль доступа
- A.12 Разработка, внедрение и обслуживание информационных систем
- A.13 Управление инцидентами информационной безопасности
- A.14 Управление непрерывностью бизнеса
- A.15 Соответствие требованиям

Рисунок 12 – Нормативные акты и стандарты ИБ

Диаграмма распределения событий по времени позволяет быстро выявлять аномалии и уточнять временной интервал отображаемых событий.

Выбрать интервал времени для отображения можно при помощи простых манипуляций мышью в интересующей области диаграммы. После выбора интервала график автоматически перестраивается, и таким образом распределение событий за выбранный интервал времени уточняется (рисунок 13).

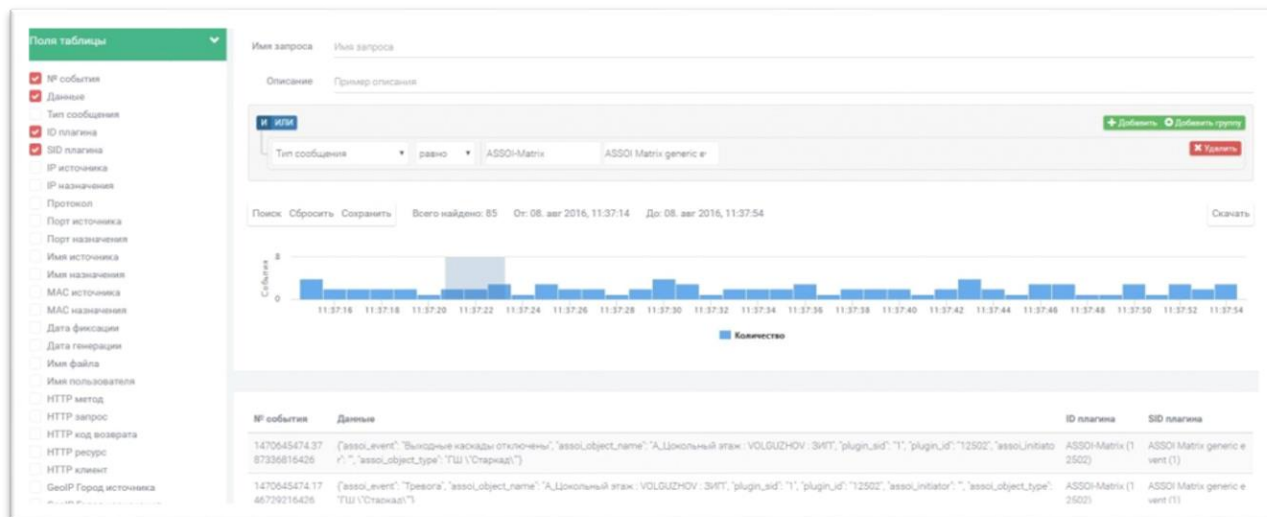


Рисунок 13 – Диаграмма распределения событий по времени

Цена продукта зависит от особенностей и требований пользователя. КОМРАД включен в единый реестр российского программного обеспечения.

События по информационной безопасности поступают в КОМРАД Enterprise SIEM из различных источников: операционные системы, системы управления базами данных, сетевого оборудования, средств защиты информации, прикладного программного обеспечения и т. д. Для сбора событий используются коллекторы. Некоторые из них работают в пассивном режиме, ожидая входящих данных на определённых сетевых портах (Syslog, xFlow), другие сами инициируют соединения для извлечения необходимой информации (SQL, файловый, SNMP). Для сбора событий с Windows-машин используется специальный WMI-агент. Коллекторы могут быть установлены как на одном узле с основными компонентами системы, так и на выделенных серверах. Важнейшими коллекторами, которые позволяют организовать сбор событий с абсолютного большинства источников, являются Syslog-коллектор и WMI-агент. Подключение источника для передачи событий по Syslog

состоит в активации Syslog-коллектора и настройке отправки сведений на определённый порт и IP-адрес. Для Syslog-коллектора можно установить параметры пропускной способности, ограничивающие число одновременных соединений, а также размер входящих сообщений (рисунок 14).

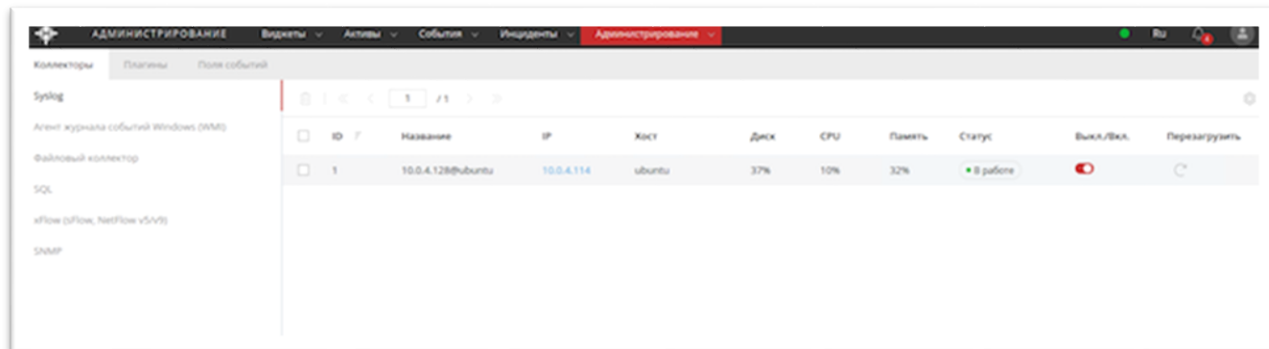


Рисунок 14 – Управление Syslog-коллекторами

Подключение Windows-машины в качестве источника событий доступно для администраторов системы за три простых шага, а именно: одной командой установить агент на нужный узел, в конфигурационном файле указать IP-адрес коллектора KOMRAD Enterprise SIEM, после чего применить настройки. WMI-агент также позволяет собирать данные из локальных файлов журналов. Агенты устанавливаются в качестве службы Windows и управляются через веб-интерфейс администратора KOMRAD Enterprise SIEM (рисунок 15).

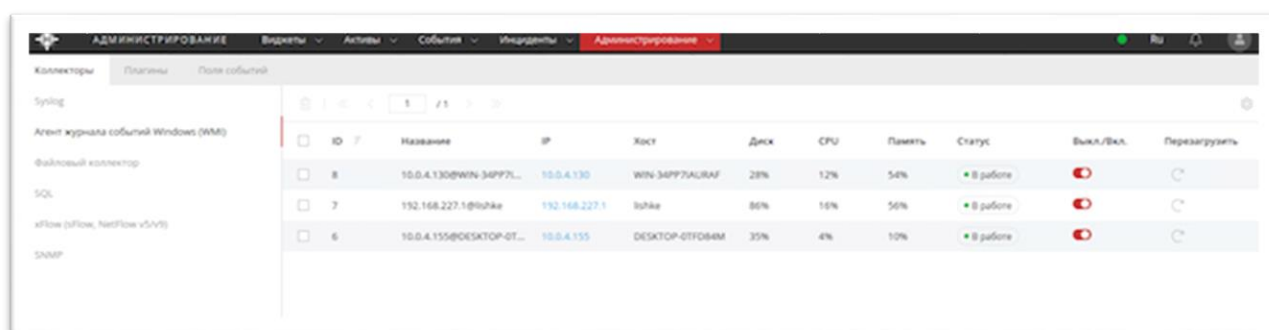


Рисунок 15 – Управление WMI-агентами

В случае отсутствия соединения между WMI-агентом и сервером KOMRAD Enterprise SIEM события будут собираться в свою локальную базу

данных во избежание их потери, а при возобновлении соединения поступают по назначению (рисунок 16).

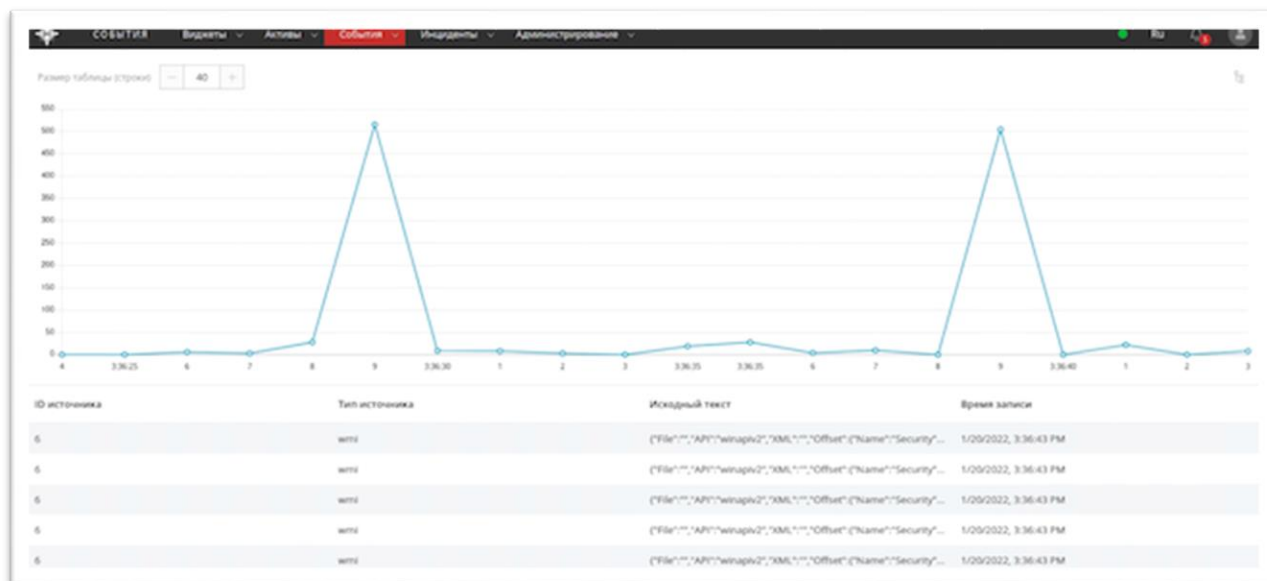


Рисунок 16 – События в настоящем времени

В карточке каждого события можно увидеть его исходное содержимое (рисунок 17).

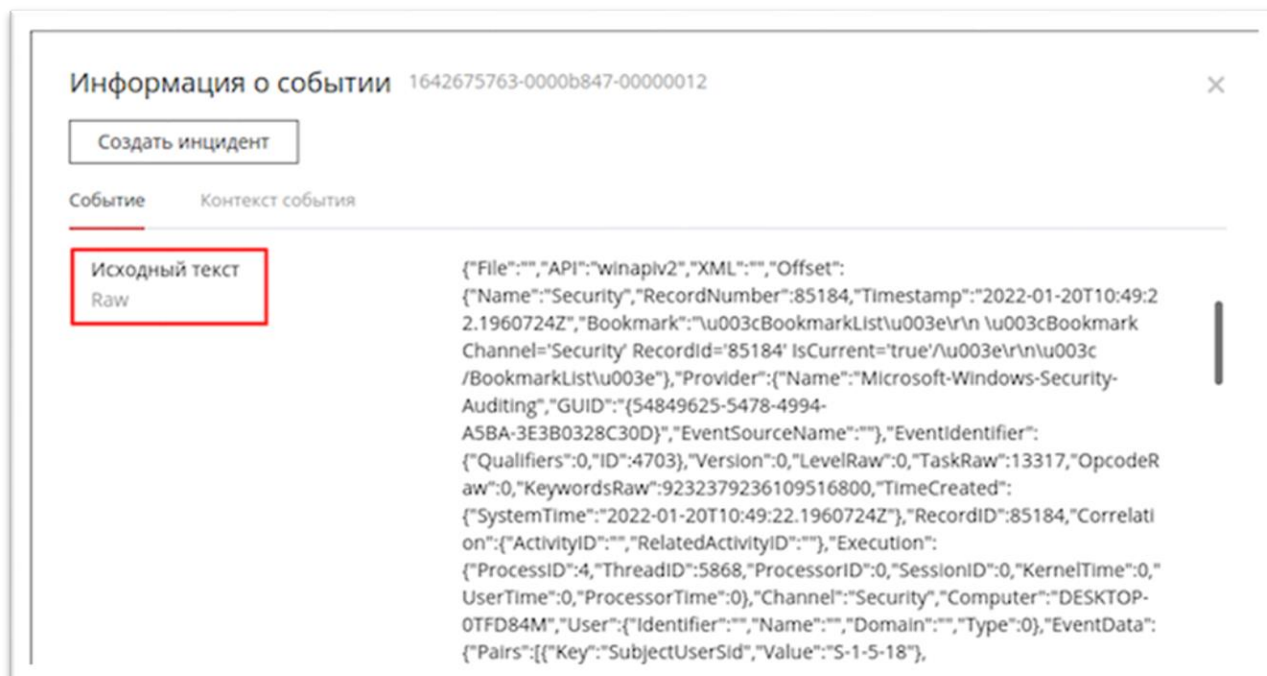


Рисунок 17 – Исходный текст события из Windows

Для KOMRAD Enterprise SIEM вендор выпускает пакеты экспертиз, доступные для пользователей, которые приобрели расширенную техническую

поддержку продукта. Пакеты экспертиз включают в себя фильтры событий и директивы корреляции. Готовые фильтры и директивы значительно облегчают внедрение и использование продукта.

Отечественная система централизованного управления событиями по информационной безопасности KOMRAD Enterprise SIEM предоставляет пользователям все функциональные возможности, которые необходимы для организации эффективного мониторинга. Решение предназначено для применения не только в компаниях среднего и крупного бизнеса, но и в государственных организациях. KOMRAD Enterprise SIEM отличается низкой ценой владения и доступен широкому кругу потребителей благодаря низким требованиям к вычислительным ресурсам, интуитивно понятному пользовательскому интерфейсу и наличию пакетов экспертиз.

Достоинства данного решения:

- Возможность подключения произвольных источников событий по распространённым протоколам.
- Удачное соотношение цены и качества продукта.
- Бессрочная лицензия.
- Низкие требования к аппаратному обеспечению.
- Наличие пакетов экспертиз.
- Наличие сертификата ФСТЭК России.
- Сертифицированная по требованиям Минобороны России по НДВ-2 версия для использования в информационных системах, в которых обрабатывается информация, отнесённая к государственной тайне.

2.2. Оценка эффективности предложенных рекомендаций по реализации эффективных методов управления информационной безопасностью ГБПОУ «Южно-Уральский государственный колледж» с помощью метода анализа дерева отказов

Для оценки эффективности предложенной SIEM системы сначала определим некоторые базовые понятия, которые будут использоваться в этой оценке. Привычные для специалистов по информационной безопасности свойства защищенности информационной системы применительно к системе управления событиями информационной безопасности могут быть выстроены в порядке убывания приоритетов следующим образом: доступность, целостность, конфиденциальность. В понятие надежности кроме указанных свойств защищенности, входят такие свойства, как безотказность, сохранность (устойчивость к воздействиям) и ремонтпригодность.

Безотказность – свойство системы непрерывно сохранять работоспособное состояние в течение некоторого времени (наработки). Под наработкой обычно понимается продолжительность времени работы системы или объем работы. Состоянием называется множество существенных свойств, которыми объект обладает в данный момент времени. Безотказность и доступность условно можно объединить в понятие минимизации простоев информационной системы, т.е. обеспечение непрерывности обслуживания системы.

Важнейшим понятием в теории надежности является понятие *отказа*. В информационной системе отказы происходят не всегда одинаково, различные способы отказа называются состояниями отказа. Состояния отказа отражают события ненадлежащего обслуживания. Применительно к системе под отказом будем понимать отрицательный результат аутентификации и соответственно состояние отказа в авторизации легального пользователя.

Работоспособное состояние – это такое состояние объекта, при котором множество существенных свойств в полном объеме отвечает заданным требованиям. Под *опасным отказом* будем понимать положительный результат прохождения процесса аутентификации злоумышленником.

Для формирования дерева отказов и дерева событий введем следующие предположения, основанные на опыте проектирования, построения и анализе функционирования ряда промышленных:

1. Основной поток заявок $\lambda_{л.п}$ на обслуживание системы поступает от легальных пользователей системы, при этом заявки не содержат ошибок, а система и ее элементы не имеют отказов.

2. Среди массы заявок от легальных пользователей имеется некоторая часть некорректно оформленных заявок $\lambda_{ош.л.п} \in \lambda_{л.п}$. из-за непреднамеренных ошибок.

3. Из числа заявок от легальных пользователей имеется некоторая часть заведомо ложных заявок $\lambda_{з.л.л.п} \in \lambda_{л.п}$. с целью выдать себя за пользователя с более привилегированными правами доступа. Таким образом, имеем соотношение: $\lambda_{ош.л.п} + \lambda_{ош.л.п} + \lambda_{з.л.л.п} = \lambda_{л.п}$.

4. В систему поступает некоторая часть заведомо ложных заявок от злоумышленников $\lambda_{з.л.зл}$, пытающихся выдать себя за легальных пользователей: $\lambda_{з.л.зл} \cap \lambda_{л.п}$.

Уточним ряд положений о работе системы:

1. Система состоит из серверной и клиентской частей, связанных устойчивым каналом (каналами) связи.

2. Серверная часть состоит из нескольких связанных защищенным образом серверов, отказоустойчивость ОУ которых (по SLA – Service Level Agreement, соглашение об уровне обслуживания) $OU \geq 99,95\%$. Системное, прикладное и специальное программное обеспечение – лицензионное, как правило, вовремя обновляется и обслуживается производителями.

3. Клиентская часть представлена в виде следующих модификаций: компьютер пользователя с необходимым набором программного обеспечения и аутентификационной информацией (АИ) пользователя логином и паролем.

Проведем анализ видов и последствий отказов согласно рекомендациям. Как известно, этот метод позволяет определить возможные причины отказа элементов системы и события, породившие отказ.

Составим дерево отказов системы в соответствии с пятиуровневой схемой. Верхний (первый) уровень – отказ системы. Второй уровень – отказ составных частей. Третий уровень – отказ элементов. Следующий уровень

определяет события, порождающие отказ. Пятый уровень определяет виды воздействий, приводящих к отказу информационной системы.

Построение всего дерева отказов в виде графа событий и последствий представляет собой трудночитаемый рисунок с множеством мелких значков и надписей. Поэтому выделим наиболее существенные виды отказов системы, не пропуская, по возможности, наиболее критичные с точки зрения безопасности и надежности. Рассмотрим некоторые отказы системы, связанные с событиями, породившими отказ, в процедурах регистрации и хранения (таблица 2).

Таблица 2 – Примеры дерева отказов ГБПОУ «ЮУГК»

Уровень системы	Отказ системы	Отказ системы	Опасный отказ системы (в процедуре регистрации)	Опасный отказ системы (в процедуре хранения)
Уровень составных частей	Отказ в регистрации пользователю	Отказ в регистрации пользователю	Злоумышленник к зарегистрирован под видом легального пользователя	Злоумышленник владеет АИ легального пользователя
Уровень элементов	Отказ в приеме АИ	Отказ в результате проверки АИ	Проверки АИ не выявили обмана	Потеря конфиденциальности АИ
События, порождающие отказ	Неполный набор представленных пользователем АИ	В базах данных не найдена АИ представленных пользователем	Поддельные документы на имя легального пользователя	Нарушение условий хранения АИ
Виды воздействия	Ошибка пользователя	Вирусная атака	Атака класса «маскарад»	Хищение и копирование АИ

Сформированное таким образом дерево отказов позволяет более четко идентифицировать вероятные события, которые могут привести к нарушениям информационной безопасности при работе системы. Рассмотрение отказов является одной из важных подготовительных процедур для идентификации рисков нарушения безопасности функционирования системы. Следующей процедурой является формирование модели дерева событий, где необходимо

выделить наиболее вероятные опасные события и оценить частоту их реализации.

Существует вероятность ошибки первого рода (система не авторизовала легального пользователя). Рассмотрим возможные причины такого события:

- 1) пользователь неверно ввел свою АИ
- 2) перегрузка системы ввиду большого числа одновременных заявок и/или время ожидания превысило некий порог ожидания;
- 3) отказ клиентской части (аппаратный или программный сбой);
- 4) отказ канала связи (аппаратный и/или программный);
- 5) отказ серверной части.

Также существует вероятность ошибки второго рода, когда система признала АИ правильной и авторизовала злоумышленника под именем легального пользователя.

На основе анализа опыта построения и эксплуатации ряда промышленных информационных систем практикующих специалистов выделим ряд вероятных опасных событий и оценим влияние SIEM системы.

RNE_i , $i = 1, n$. Перечислим эти события и приведем грубую оценку частоты их реализации для двух состояний информационной системы: без применения двухфакторной аутентификации и после реализации таковой.

RNE_1 . Целенаправленные действия злоумышленника при регистрации. *Регистрация* – одна из самых ответственных операций процессов аутентификации, существенно влияющая на безопасность, надежность и в конечном счете на доверие работы системы. Данную угрозу обозначают как «маскарад» при регистрации. Средняя частота такого события для государственных систем по оценке располагается в достаточно широких пределах: 10^{-7} – 10^{-5} в год. При применении SIEM системы частота снижается до нижнего предела.

RNE_2 . Злоумышленник для доступа к интересующим его информационным ресурсам может воспользоваться уязвимостями системы. Это опасное событие имеет вероятность осуществиться. Будем называть это

событие «уязвимости СИА» и оценим частоту в пределах 10^{-5} – 10^{-3} . При применении SIEM системы частота снижается до нижнего предела.

РНЕ3. Этот тип вероятного опасного события может быть связан с действиями инсайдера. Помочь злоумышленнику пройти все рубежи может легальный пользователь. Еще больше возможностей у администратора. Кратко назовем это событие «помощь инсайдера». Средние оценки частоты: 10^{-6} – 10^{-4} . При применении SIEM системы частота снижается до нижнего предела.

РНЕ4. Завладение злоумышленником АИ легального пользователя. Это может быть кража, клонирование, подсмотренный пароль, перехваченный PIN-код. При применении SIEM системы частота снижается до нижнего предела.

РНЕ5. Атака «вход по принуждению» встречается все реже и реже: 10^{-7} – 10^{-5} . При применении SIEM системы частота снижается до нижнего предела.

РНЕ6. Ошибки и/или целенаправленные действия злоумышленника при смене пароля, замене цифрового сертификата доступа или сценарии «забыл дома смарт-карту». Коротко назовем этот тип «смена АИ» и оценим частоту в пределах 10^{-5} – 10^{-3} . При применении SIEM системы частота снижается до нижнего предела.

РНЕ7. Данный тип связан с ошибками валидации. Под валидацией будем понимать процесс проверки действительности сертификата доступа и цепочки сертификатов, для парольной защиты это процедура сличения хешей паролей (присланного претендентом и зарегистрированного в базе данных учетных записей). Короткое название – «ошибки валидации». При применении SIEM системы частота снижается до нижнего предела.

РНЕ8. Ошибки в принятии решения «свой–чужой». Процедура производится на серверах, вероятная частота подобного события 10^{-7} – 10^{-5} . При применении SIEM системы частота снижается до нижнего предела.

РНЕ9. Имитация доверяющей стороны. Особенно актуален такой тип ВОС при предоставлении Web –доступа, который становится все более

распространенным. Фишинг (подмена сайта) является одним из актуальных ВОС, оценки частоты колеблются в пределах 10^{-4} – 10^{-2} . При применении SIEM системы частота снижается до нижнего предела.

PHE10. Подмена доверенной стороны или объекта (spoofing), оценим частоту 10^{-6} – 10^{-4} . При применении SIEM системы частота снижается до нижнего предела.

PHE11. Риск добровольной передачи персонального средства ИА другому пользователю. Частоту можно оценить в пределах 10^{-4} – 10^{-2} . При применении SIEM системы частота снижается до нижнего предела.

PHE12. Воздействие вредоносного программного обеспечения, вероятность заражения рабочих мест определяется политикой безопасности организации, в среднем может быть оценена как 10^{-4} – 10^{-2} . При применении SIEM системы частота снижается до нижнего предела.

Таким образом, анализируя влияние SIEM системы на вероятность реализации рисков ИБ можем отметить, что вероятность их появления снижается в 12 типовых случаях, что свидетельствует о повышении уровня защищенности информационных ресурсов. Проведенное исследование подтвердило выдвинутую гипотезу.

Выводы по второй главе

Во второй главе были предложены административно-организационные и технические мероприятия. Предполагается обновить локальные акты ГБПОУ «ЮУГК» и дать ознакомиться всем сотрудникам, имеющим доступ к персональным данным.

В качестве инженерно-технических методов, организация может приобрести специализированное решение для управления ИБ.

Сотрудники организации должны участвовать в различных аспектах программы информационной безопасности и обладать соответствующими навыками и знаниями. Необходимый уровень профессионализма сотрудников может быть достигнут с помощью тренингов, проводить которые могут как специалисты организации, так и внешние консультанты.

Компетентность пользователей является обязательным условием для успешного обеспечения информационной безопасности, а также позволяет гарантировать, что средства контроля работают должным образом. Пользователи не могут следовать политике, которую они не знают или не понимают. Не зная о рисках, связанных с информационными ресурсами организации, они не могут видеть необходимости исполнения политики, разработанной с целью уменьшения рисков.

Должно проходить непрерывное обучение пользователей и других сотрудников на примере рисков и соответствующих политик. Для этого можно воспользоваться курсами повышения квалификации в области информационной безопасности, которые проводит региональный учебно-научный центр «Информационная безопасность» Южно-Уральского государственного университета.

Обработать вручную большое количество инцидентов нарушений ИБ и выявить инциденты невозможно. Для этого предложено использовать специализированные решения SIEM (Security Information and Event Management) для автоматизации данных процессов.

Для ГБПОУ «ЮУГК» было выбрано решение «KOMRAD Enterprise SIEM». Это гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации. Она позволяет осуществлять централизованный сбор событий ИБ, выявлять инциденты ИБ и оперативно на них реагировать. Применение комплекса позволяет эффективно выполнять требования, предъявляемые регуляторами к защите персональных данных, к обеспечению безопасности государственных информационных систем и контролю критической информационной инфраструктуры предприятия. КОМРАД позволяет отправлять данные о событиях и инцидентах ИБ во внешние системы.

Отечественная система централизованного управления событиями по информационной безопасности KOMRAD Enterprise SIEM предоставляет пользователям все функциональные возможности, которые необходимы для организации эффективного мониторинга. Решение предназначено для применения не только в компаниях среднего и крупного бизнеса, но и в государственных организациях. KOMRAD Enterprise SIEM отличается низкой ценой владения и доступен широкому кругу потребителей благодаря низким требованиям к вычислительным ресурсам, интуитивно понятному пользовательскому интерфейсу и наличию пакетов экспертиз.

Для оценки эффективности предложенной SIEM системы предлагается воспользоваться методом «дерево отказов». Выделим наиболее существенные виды отказов системы, не пропуская, по возможности, наиболее критичные с точки зрения безопасности и надежности. Анализируя влияние SIEM системы на вероятность реализации рисков ИБ можем отметить, что вероятность их появления снижается в 12 типовых случаях, что свидетельствует о повышении уровня защищенности информационных ресурсов. Проведенное исследование подтвердило выдвинутую гипотезу.

ЗАКЛЮЧЕНИЕ

В ходе выполнения магистерской диссертации, была раскрыта гипотеза исследования, заключающаяся в предположении о повышении эффективности мер управления информационной безопасностью образовательной организации при реализации эффективных методов управления ИБ.

В рамках этой гипотезы были решены поставленные задачи:

1. раскрыта сущность и содержание методов управления информационной безопасностью.

2. изучен объект защиты-ГБПОУ «Южно-Уральский государственный колледж», его структуру, информационные ресурсы и информационные потоки колледжа; проанализировать методы управления информационной безопасностью в ГБПОУ ЮУГК; выявить уязвимости в системе защиты информации.

3. разработаны рекомендации по реализации эффективных методов управления информационной безопасностью колледжа ГБПОУ «Южно-Уральский государственный колледж».

4. проведена оценка предложенных рекомендаций по реализации эффективных методов управления информационной безопасностью колледжа ГБПОУ «Южно-Уральский государственный колледж».

В первой главе исследования проанализированы сущность и содержание методов управления информационной безопасности образовательной организации. Описаны методы и средства защиты используемые в ГБПОУ «ЮУГК» к ним относятся правовые, организационно-технические, административно-технические, физические методы.

Во второй главе отражены результаты реализации эффективных методов управления информационной безопасностью ГБПОУ «ЮУГК».

Для оценки эффективности предложенной SIEM системы предлагается воспользоваться методом «дерево отказов». Выделим наиболее существенные виды отказов системы, не пропуская, по возможности, наиболее критичные с

точки зрения безопасности и надежности. Анализируя влияние SIEM системы на вероятность реализации рисков ИБ можем отметить, что вероятность их появления снижается в 12 типовых случаях, что свидетельствует о повышении уровня защищенности информационных ресурсов. Проведенное исследование подтвердило выдвинутую гипотезу.

Основные положения и результаты работы докладывались и обсуждались на научно-практических конференциях и были отражены в работе:

1. Ахметшин Д.Р. Обеспечение кибербезопасности в условиях дистанционного обучения на примере ГБПОУ «Южно - Уральский государственный колледж»/ О. А. Черяева, А. Р. Халиуллин, Д. Р. Ахметшин // Инновационные проекты и программы в психологии, педагогике и образовании: сборник статей по итогам Международной научно-практической конференции, Екатеринбург, 29 сентября 2021 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2021. – С. 103-107.

Практическая значимость результатов, полученных в данной магистерской диссертации, заключается в том, что они могут использоваться в качестве базы исследовательской, аналитической и проектной деятельности авторов, изучающих тему методов управления информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Александрова, А.В. Информационная безопасность и конституционные права личности/ А. В. Александрова, Е. И. Образумов // Наука. Общество. Государство. — 2021. — № 1. — С. 63-70.
2. Ахметшин, Д. Р. Обеспечение кибербезопасности в условиях дистанционного обучения на примере ГБПОУ «Южно - Уральский государственный колледж»/ Д. Р. Ахметшин, А. Р. Халиуллин, О.А. Черяева // Инновационные проекты и программы в психологии, педагогике и образовании: сборник статей по итогам Международной научно-практической конференции, Екатеринбург, 29 сентября 2021 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2021. – С. 103-107.
3. Базелюк, Н. Г. Методы управления информационной безопасностью в организации/ Н. Г. Базелюк, А. В. Степанов // Евразийский союз ученых. – 2015. – № 4-13(13). – С. 65-67
4. Баранова, Е.К. Основы информационной безопасности: учебник/ Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019. — 202 с.
5. Белим, С.В. Проблемы построения политики безопасности при объединении информационных систем/ С. В. Белим, С. Ю. Белим // Математические структуры и моделирование. — 2018. — № 3. - С. 126-131
6. Белов, Е.Б. Основы информационной безопасности: учебное пособие для вузов/ Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2016. – 544 с.
7. Белякова, Е.Г. Информационная культура и информационная безопасность школьников/ Е. Г. Белякова, Э. В. Загвязинская, А. И. Березенцева // Образование и наука. — 2017. — № 8. — С. 147-162.

8. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учеб. пособие/ В.В. Бондарев. — Москва: Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.
9. Гафнер, В. В. Информационная безопасность: учебное пособие/ В.В. Гафнер. - Рн/Д: Феникс, 2017. - 324 с.
10. Гельруд, Я.Д. Управление безопасностью подготовки кадров к работе с информационными и коммуникационными технологиями в информационном обществе/ Я.Д. Гельруд, С.А. Богатенков // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. — 2016. — № 3. — С. 40-51.
11. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.
12. Государственная дума Федерального собрания Российской Федерации седьмого созыва Комитет по образованию и науке решение от 20 февраля 2018 года N 40-5 Развитие информатизации системы образования. Совершенствование законодательства в области электронного обучения и дистанционных образовательных технологий [Электронный ресурс]: URL: <https://docs.cntd.ru/document/556985932> (дата обращения: 30.05.2022)
13. Грачева, Е.А. Информационная безопасность/ Е. А. Грачева // The Newman in Foreign Policy. — 2020. — № 54 (98) Vol. 3. — С. 57-59.
14. Гришина Н.В. Основы информационной безопасности предприятия: учебное пособие/ Н.В. Гришина. - Инфра-М., 2019. – 216 с.
15. Гульятеева, Т. А. Основы информационной безопасности: учебное пособие/ Т. А. Гульятеева. — Новосибирск: НГТУ, 2018. — 79 с.
16. Гуцин, А. Н. Личностно-ориентированные информационные системы: учебное пособие / А. Н. Гуцин. — Санкт-Петербург: БГТУ «Военмех» им. Д.Ф. Устинова, 2012. — 120 с.
17. Жарникова, Ю. С. Угрозы информационной безопасности образовательного учреждения / Ю. С. Жарникова. — Текст: непосредственный

// Молодой ученый. — 2017. — № 11.2 (145.2). — С. 60-63. — URL: <https://moluch.ru/archive/145/40613/> (дата обращения: 30.05.2022)

18. Жидко, Е.А. Информационная безопасность предприятия как необходимый фактор организации управления безопасностью труда / Е.А. Жидко, В.С. Муштенко // Научный вестник Воронежского государственного архитектурно-строительного университета. Серия: Высокие технологии. Экология. — 2014. — № 1. — С. 223-228.

19. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите/ С.В. Запечников, Н. Г. Милославская. — М.: ГЛТ, 2017. — 536 с.

20. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях/ С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

21. Ильченко, Л.М. Расчет рисков информационной безопасности телекоммуникационного предприятия/ Л.М. Ильченко, Е.К. Брагина, И.Э. Егоров, С.И. Зайцев // Открытое образование, 2018. — С. 61-70.

22. Информационная безопасность образовательных учреждений [Электронный ресурс]: URL: <https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/> (дата обращения 13.03.2022)

23. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие/ В. Я. Ищейнов, М. В. Мещатунян. — 2-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 216 с.

24. Киреева, Н. В. Аудит информационной безопасности: методические указания/ Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара: ПГУТИ, 2019. — 21 с.

25. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления: монография / И.С. Клименко. — Москва: ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI

10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1137902> (дата обращения: 23.05.2022). – Режим доступа: по подписке.

26. Коджешау, М.А. Технологии и алгоритмы информационной безопасности / М.А. Коджешау // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2017. — № 2. — С. 129-135.

27. Конкин, Ю. В. Основы информационной безопасности: учебное пособие/ Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань: РГРТУ, 2021. — 96 с.

28. Конкин, Ю. В. Основы информационной безопасности: учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань: РГРТУ, 2021. — 96 с.

29. Конституция Российской Федерации [Электронный ресурс]: (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2021) URL: <http://www.consultant.ru/> (дата обращения 23.11.2021)

30. Крыжановский, А. В. Информационная безопасность: методические указания / А. В. Крыжановский, И. С. Поздняк. — Самара: ПГУТИ, 2018. — 38 с.

31. Леонтьев, А. С. Защита информации: учебное пособие / А. С. Леонтьев. — Москва: РТУ МИРЭА, 2021. — 79 с.

32. Логинова, А.О. Обзор нормативно-правовых источников и практик управления инцидентами информационной безопасности/ А. О. Логинова // Вестник СибГУТИ. — 2021. — № 1. — С. 50-59.

33. Лучинкина, А.И. Информационно-психологическая безопасность образовательной среды / А.И. Лучинкина // Научное мнение. — 2018. — № 1. — С. 73-78.

34. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации/ А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.
35. Маслова, М.А. Анализ и определение рисков информационной безопасности / М. А. Маслова // Научный результат. Информационные технологии. — 2019. — № 1. — С. 31-37. — ISSN 2518-1092.
36. Метод оценки экономической эффективности подразделения по защите информации [Электронный ресурс]: URL: <https://lib.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii> (дата обращения 23.11.2020)
37. Минин, А.Я. Информационная безопасность в образовании/ А.Я. Минин // Наука и школа. — 2017. — № 1. — С. 29-36.
38. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие/ А. В. Моргунов. — Новосибирск: НГТУ, 2019. — 83 с.
39. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие/ А. В. Моргунов. — Новосибирск: НГТУ, 2019. — 83 с.
40. Мызникова, Т. А. Основы информационной безопасности: учебное пособие / Т. А. Мызникова. — Омск: ОмГУПС, 2017. — 82 с.
41. Нормативное обеспечение эксплуатации средств защиты информации: учебное пособие/ А. В. Красов, И. И. Лившиц, Д. В. Юркин [и др.]. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 67 с.
42. Обеспечение информационной безопасности организации [Электронный ресурс]: URL: <https://iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/> (дата обращения 13.03.2022). — Текст: электронный
43. Поздняк, И. С. Управление информационной безопасностью: методические указания/ И. С. Поздняк, И. С. Макаров. — Самара: ПГУТИ, 2019. — 43 с.

44. Поздняк, И. С. Экспертные системы оценки информационной безопасности: методические указания/ И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара: ПГУТИ, 2019. — 23 с.

45. Поликарпов, А. В. Социально-философские аспекты проблемы информационной безопасности России: дис. ... канд. философ. наук. - М., 2000.- Режим доступа: <https://www.dissercat.com/content/sotsialno-filosofskie-aspekty-problemy-informatsionnoi-bezopasnosti-rossii>

46. Полякова А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для академического бакалавриата и магистратуры: для студентов высших учебных заведений, обучающихся по юридическим направлениям и специальностям/ под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2017. — 324 с.

47. Постановление Правительства Российской Федерации № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» URL: <http://base.garant.ru/70252506/> (дата обращения 23.11.2020)

48. Привалов, А.Н. Методологические подходы к организации безопасной информационно-образовательной среды вуза/ А. Н. Привалов, Ю. И. Богатырева, В. А. Романов // Образование и наука. — 2017. — № 4. — С. 169-183.

49. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты». URL: <https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/471-informatsionnoe-pismo-fstek-rossii-2> (дата обращения 23.11.2021)

50. Прокудин, Дмитрий Евгеньевич. Информационные технологии в образовании и их роль в формировании техногенной культуры: диссертация ... доктора философских наук: 24.00.01 / Прокудин Дмитрий Евгеньевич; [Место защиты: Санкт-Петербургский государственный университет]. - Санкт-Петербург, 2012. - 336 с.

51. Пугин, В. В. Защита информации в компьютерных информационных системах: учебное пособие/ В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара: ПГУТИ, 2018. — 119 с.
52. Резниченко, М.Г. Профессиональная успешность специалистов в сфере информационной безопасности/ М. Г. Резниченко, Е. А. Помельникова // Вестник Самарского университета. История, педагогика, филология. — 2019. — № 3. — С. 82-88.
53. Риск-модели информационной безопасности: учебное пособие / А. А. Корниенко, С. В. Корниенко, А. П. Глухов, М. Л. Глухарев. — Санкт-Петербург: ПГУПС, 2021. — 79 с.
54. Санжаров, А.С. Методы оценки исследований информационной безопасности и компьютерных угроз / А.С. Санжаров, Ж.Т. Баранова // Известия Кыргызского государственного технического университета им. И.Раззакова. — 2018. — № 46. — С. 296-301.
55. Секлетова, Н. Н. Анализ рынка информационных систем и технологий: учебное пособие / Н. Н. Секлетова, А. С. Тучкова, О. И. Захарова. — Самара: ПГУТИ, 2018. — 215 с.
56. Серова А.Г. Анализ эффективности системы управления информационной безопасностью государственного учреждения. Экономика и управление. 2017;(6):71-74.
57. Скулябина, О. В. Системный анализ в информационной безопасности: учебное пособие/ О. В. Скулябина, С. Ю. Страхов. — Санкт-Петербург: БГТУ «Военмех» им. Д.Ф. Устинова, 2021. — 50 с.
58. Соколова, А.А. Информационно-образовательная среда и безопасность современной личности / А. А. Соколова, С. Н. Соколова, О. В. Пчелина // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. — 2020. — № 2. — С. 89-93.
59. Угрозы информации <https://siblec.ru/telekommunikatsii/osnovy-informatsionnoj-bezopasnosti-v-telekommunikatsiyakh/10-ugrozy-informatsii>

60. Управление информационной безопасностью в мире <http://lib.itsec.ru/articles2/research/upravlenie-informacionnoi-bezopasnostu-v-mire> Обеспечение информационной безопасности организации [Электронный ресурс]: URL: <https://iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/> (дата обращения 13.03.2022). – Текст: электронный
61. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». – Москва: Легион, 2022. – 144 с.
62. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – Москва: Омега-Л, 2022. – 96 с.
63. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». – Москва: Гросс-Медиа, 2022. – 16 с.
64. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации». – Москва: Норматика, 2022. – 144 с.
65. Шахворостов, Г.И. Актуальные направления совершенствования административного управления системой обеспечения информационной безопасности субъекта российской федерации: проблемы и предложения / Г. И. Шахворостов, А. И. Кустов, В. С. Самсонов, М. А. Жданов // Регион: системы, экономика, управление. — 2022. — № 1. — С. 28-35.