МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 (АТИТиМОТД)

ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ СЛУЖБОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ СПО

Магистерская диссертация
44.04.04 Профессиональное обучение по направлению
Управление информационной безопасностью в профессиональном образовании

Выполнила:
магистрант группы ОФ-209/210-2-1
Шамне Кирилл Андреевич
Научный руководитель:
зав.кафедрой АТИТиМОТД ППИ
к.т.н, доцент.
Руднев Валерий Валентинович

Проверка на объем заимствований:
72,2 % авторского текста

Работа рекомендована к защите
«24» мая 2018г.
зав. кафедрой АТИТиМОТД ППИ
к.т.н., доцент В.В.Руднев

Челябинск 2018

Оглавление

Введение

Современный уровень развития информационных технологий выдвигает на передний план новые требования к построению систем защиты информации и обеспечению информационной безопасности.

В России на протяжении длительного времени понятие информационной безопасности отождествлялось с обеспечением конфиденциальности информации, а наибольшее распространение получило применение технических средств защиты. Сегодня информация, будучи нематериальной по своей природе, становится предметом товарно-денежных отношений и объектом нормативно-правового регулирования. Перед государственными и коммерческими предприятиями и организациями все острее встает проблема не только обеспечения надежной защиты информации от несанкционированного ознакомления и распространения, но и поддержки стабильного доступа к информации и возможности эффективной работы с ней. Более того, Доктрина информационной безопасности Российской Федерации провозглашает «соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею» одной из составляющих национальных интересов в информационной сфере.

СИБ должна обеспечивать:

- конфиденциальность (защита информации от несанкционированного раскрытия или перехвата);
- целостность (достоверность и полноту информации и компьютерных программ);
- доступность (возможность получить пользователям информацию, в пределах своей компетенции).

С учетом зарубежного и отечественного опыта обеспечение

информационной безопасности осуществляется по следующим направлениям:

- правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

- организационная защита – это регламентация производственной деятельности и отношений исполнителей на нормативно-правовой основе,

исключить или ослабляющая нанесение ущерба;

- инженерно-техническая защита-это использование различных технических средств, которые предотвращают нанесение ущерба.

В связи с вышеизложенным сегодня при построении систем защиты информации все большее внимание уделяется установлению баланса между техническими средствами и законодательно-организационными мерами защиты. Преимущество получает комплексный подход к защите информации, который состоит в одновременном решении целого ряда разноплановых задач путем применения совокупности взаимосвязанных средств, методов и мероприятий.

Отечественная и зарубежная наука уделяет большое внимание информационной безопасности. Многие зарубежные социологи и политологи активно исследуют вопросы информационного противоборства и информационной безопасности. Среди наиболее известных трудов можно отметить работы Д.Альбертса, Г.С.Джоуэта, М.Либицки, Д.А.Мальтизи,

Р.Д.Маклорина, Р.Л.Пфальцграффа, А.Шафрански, Р.Х.Шульца, А.Эделыптейна и других, где рассматриваются различные аспекты влияния информации на политические, экономические, военные и культурные процессы в современных международных отношениях.

Научное осмысление различных аспектов информационной

безопасности активно проводились отечественными учеными

А.В.Возженикoвым, Ю.Ф.Нуждиным, Е.Н.Пасхиным, Е.Е.Перчук, А.И.Поздняковым, Г.Г.Почепцовым, А.А.Прохожевым, С.П.Расторгуевым,

А.А.Стрельцовым, Г.Л.Смоляным, Д.С.Черешкиным, А.С.Шийко, В.Н.Цыгичко и другими.

Рассмотрению проблем защиты личности от вредного информационного воздействия в современном мире посвящены работы Г.В.Грачева, Ю.А.Ермакова, В.Е.Лепского, И.К.Мельника, И.Н.Панарина и других исследователей.

Различным аспектам правовой защиты интересов личности в информационной сфере общества посвящены работы В.А.Анниковой, А.А.Антопольского, А.Л.Балыбердина, И.Л.Бачило, М.С.Григорьева, В.И.Кирина, О.А.Колобова, В.А.Копылова, В.Н.Ясенева, В.Н.Лопатина, Д.В.Огородова, В.Д.Попова, Ю.Г.Просвирина, А.А.Фатьянова.

Техническим аспектам защиты информации в информационных системах и сетях посвящены работы В.А.Герасименко, С.Н.Гриняева, М.П.Зегжды, В.Н.Лопатина, В.А.Никитова, Е.И.Орлова, Г.И.Савина.

Различным аспектам проблемы защиты информации посвящены работы Д.А.Андрианова, Н.А.Брусницына, В.Н.Кузнецова, Е.Ю.Митрохина,

С.З.Павленко, И.Н.Панарина, С.В.Рабовского, С.П.Расторгуева, А.В.Федорова, А.С.Шийко.

Анализ публикаций последних лет свидетельствует о необходимости выбора систем защиты информации, основанных на таком комплексном подходе, надежное функционирование которых невозможно без эффективного управления. Основные функции системы управления информационной безопасностью должны состоять в оценке степени критичности ситуации, связанной с нарушением информационной безопасности предприятия, организации, оценке уровня риска нарушения информационной безопасности и в поддержке принятия решения относительно действий в данной ситуации. Принятие решений в такой системе затруднено по ряду причин: не всегда возможно сформировать полное множество угроз информационной безопасности, количественно

оценить степень критичности возникшей ситуации, построить прогноз ее развития. Другими словами, основная проблема заключается в зачастую

неполных и неопределенных исходных данных о состоянии системы защиты информации, возможных угрозах, дестабилизирующих факторах.

Таким образом, тема исследования, направленная на решение данной проблемы, является актуальной и определяет цели, задачи и основные направления исследования.

Объектом исследования: Является система защиты информации (СЗИ) организации профессионального образования.

Предметом исследования: Программные средства защиты информации, обеспечивающие информационную безопасность организации профессионального образования

Цель исследования: Выявить наиболее эффективные и доступные программные средства защиты информации способствующие повышению уровня информационной безопасности в профессиональном образовании.

Для достижения поставленной цели необходимо решение следующих

задач:

- раскрыть понятия информация, информационная безопасность, информационная безопасность образовательной организации;

- выявить основные угрозы;

- проанализировать основные способы обеспечения информационной безопасности в организации;

- рассмотреть программные средства защиты информации;

- проанализировать программные средства защиты информации;

- выяснить, какие более доступны и надежны.

Гипотеза: Программные средства защиты информации играют

большую роль в обеспечении информационной безопасности образовательной организации.

Для решения поставленных задач и проверки выдвинутой гипотезы нами использованы теоретические и эмпирические методы исследования.

Задачи исследования:

- раскрыть понятия информация, информационная безопасность, информационная безопасность образовательной организации;

- выявить основные угрозы;

- проанализировать основные способы обеспечения информационной безопасности в организации;

- рассмотреть программные средства защиты информации;

- проанализировать программные средства защиты информации;

- выяснить, какие более доступны и надежны.

Для решения поставленных задач и проверки выдвинутой гипотезы нами использованы теоретические и эмпирические методы исследования. **Теоретические методы**: анализ научной, психолого-педагогической, методической, технической литературы, монографических и диссертационных работ, материалов и публикаций периодической печати по теме исследования, сравнение, аналогия. Теоретические методы в процессе организации исследования дополнялись **эмпирическими методами**: наблюдение, анализ программных средств.

Научная новизна:

-определено влияние на социальное и культурное развитие детей и подростков информационного влияния (ИВ) в сети Интернет;

-этот новый смысл концепции ИБУ, рассматривается как состояние защищенности основных интересов учащихся от угроз, создаваемых информации воздействуют на психику и социально-культурное развития детей разнообразными социальными субъектами и информационной средой общества, в том числе образовательной средой. Под основными интересами учащихся в данном контексте относится к реализации конституционного права на получение качественного образования, направленного на

формирование информационной культуры (ИК) студентов, их физического, духовного и интеллектуального развития, на обеспечение личной безопасности, на повышения качества и уровня жизни;

- разработана концепция ИБУ, включая понятийный аппарат проблемы, основные источники информационной опасности и виды угроз.

Теоретическая значимость исследования определяется расширением научных знаний в области информационной безопасности ОО.

Практическая значимость диссертации определяется тем, что ее результаты позволяют повысить степень защиты информации в ОО путем использования предложенных программных средств и рекомендаций по их применению при формировании системы информационной безопасности, направленной на снижение информационных рисков.

Структура работы:

Работа состоит из введения, трёх глав, заключения, список использованной литературы.

В первой главе рассматриваются основные понятия информационной безопасности, существующие угрозы информационной безопасности, средства защиты информации, программные средства защиты информации в ОО, алгоритмы работы и существующие уязвимости.

Вторая глава посвящена информационной безопасности ОО, комплексу программных средств защиты информации.

В третей главе проводится анализ программных средств информационной безопасности наиболее подходящих для СПО.

ГЛАВА 1 ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Информация. Информационная безопасность.

Информация это сведения об объектах и явлениях окружающей среды, их свойствах, параметрах и состоянии, которые воспринимают информационные системы в процессе жизнедеятельности и работы.

Под *информационной безопасностью* понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход

к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов,

связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Информационная безопасность многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только системный, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории:

обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность - возможность за разумное время получить требуемую информационную службу;

Целостность - актуальность и целостность информации, ее защита от разрушения и несанкционированного изменения;

Конфиденциальность – защита от несанкционированного доступа к информации. Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

В российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

- **информация** - сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

- **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

- **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

- **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации,

содержащейся в ее базах данных.

- **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

В статье 4 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. установление ограничений доступа к информации только федеральными законами;
3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. достоверность информации и своевременность ее предоставления;
7. неприкосновенность частной жизни, недопустимость сбора,

хранения, использования и распространения информации о частной жизни лица без его согласия;

8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий

перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся *информация* делится на информацию ограниченного доступа и общедоступную. К общедоступной информации относятся общеизвестные сведения и иная *информация, доступ* к которой не ограничен. В законе, определяется *информация*, к которой нельзя ограничить *доступ*, например, *информация* об окружающей среде или деятельности государственных органов. Оговаривается также, что *ограничение доступа* к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, *доступ* к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

1. информацию, свободно распространяемую;
2. информацию,предоставляемуюпосоглашениюлиц,

участвующих в соответствующих отношениях;

3. информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4. информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее *определение* защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2. соблюдение конфиденциальности информации ограниченного доступа;

3. реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2. своевременное обнаружение фактов несанкционированного доступа к информации;

3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5. возможность незамедлительного восстановления информации,

модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6. постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ "Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РФ и определяет *права* и обязанности его субъектов.

1.2. Основные угрозы безопасности информации.

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или повредиться. Компоненты автоматизированной информационной системы можно разделить на следующие группы:

Оборудование - это компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства - принтеры, контроллеры, кабели, линии связи, и т. д.);

Программное обеспечение - это приобретенные программы, исходные, объектные, загрузочные модули;

Операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;

Данные, хранимые временно и постоянно, на дисках, флэшках, печатные, архивы, системные журналы и т. д.;

Персонал. Пользователи, администраторы, разработчики и т. д.

Опасные воздействия на компьютерную информационную систему можно разделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным

воздействиям на всех этапах цикла жизни системы. Из причин случайных воздействия во время эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и аварий;
- неисправности и сбои оборудования;
- ошибки в программном обеспечении;

- ошибки в работе персонала;

- помехи в линиях связи с влиянием внешней среды.

Преднамеренные воздействия - это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник.

Можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя на уровне разработчика данной системы;

- нарушителем может быть как постороннее лицо, так и законный пользователь системы;

- преступнику известна информация о принципах работы системы;

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ. Несанкционированный доступ и использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов несанкционированного доступа, по которым можно осуществить хищение, изменение или уничтожение информации (Рис.1):

- Через человека

- Программа

- Через аппаратуру

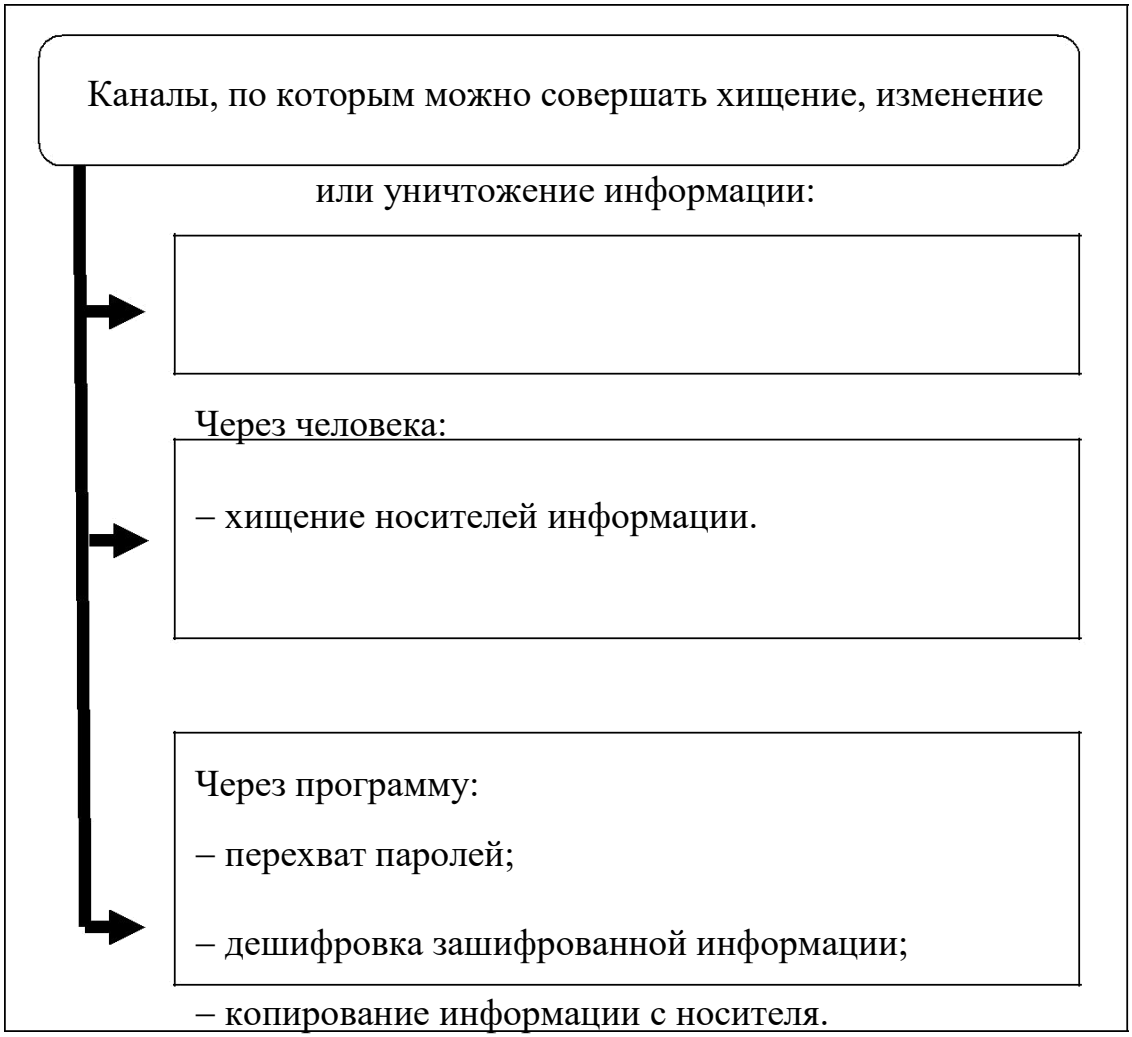

Рис. 1. Каналы для совершения хищения, изменения или уничтожения информации.

Особо следует остановиться на угрозах, которым могут подвергаться

компьютерные сети. Основной характеристикой любой компьютерной сети является то, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программ с помощью механизма сообщений. При этом сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характеризуется тем, что в отношении них принимают так называемых удаленных атак. Преступник может находиться за тысячи километров от атакуемого объекта, при этом нападению может быть не только конкретный компьютер, но и информация, передающаяся по сети каналов связи.

1.3. Обеспечение безопасности информации

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. *Законодательный* - это правила, нормы, стандарты и т. д.

Нормативно-правовая база определяет правила защиты информации:

• Ст. 16 закона от 27.07.2006 № 149-ФЗ "ОБ информации, информационных технологиях по защите информации".

В соответствии со статьей защита информации - принятие правовых, организационных и технических мер. Средства должны быть направлены на обеспечение защиты информации от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

• Ст. 9 Федерального закона № 149-ФЗ, пункт 5 изложить в следующей редакции "Сведения, полученные от граждан (физических лиц) при исполнении ими профессиональных обязанностей или организациями при осуществлении некоторых видов деятельности (профессиональная тайна), подлежит защите в случаях, если эти лица федеральными обязанности соблюдения такой информации. Такая обязанность возлагается трудового кодекса Российской Федерации (далее – таможенный кодекс), глава 14,

который определяет защиту персональных данных работника. В соответствии со статьей ТК РФ: "Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданскую или уголовную ответственность в соответствии с федеральным законом.

• Для развития этих положений в Российской федерации принят закон

№ 152-ФЗ РФ "О защите персональных данных». Его основной целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейные тайны. Статья 3

этого закона определяет: "Персональные данные - любая информация, касающаяся определенного или неопределенному на основании такой информации лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, положение, имущественного, другая информация"

• Закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию", в соответствии с которым содержание и графической информации, предназначенные для детей в дошкольных образовательных учреждениях, должны соответствовать содержанию и художественному проектирования информации для детей в этом возрасте. А также, в соответствии с Федеральным законом "Об основных гарантиях прав ребенка", образовательные учреждения обязаны

ограничиватьдоступучащихсякресурсамсетиИнтернет,

пропагандирующим насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение.

2. *Моральный и этический*. Всевозможные стандарты, несоблюдение которых ведет к падению престижа конкретного человека или целой организации.

3. *Административный*.Действияобщегохарактера,

предпринимаемые руководством организации.

4. *Физический*. Механические, электрические и электронно-

механические препятствия на возможных путях проникновения потенциальных нарушителей.

5. *Аппаратно - программный* (электронные устройства и специальные программы защиты информации).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Надежная система защиты должна соответствовать следующим принципам:

– Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.

– Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.

– Защита тем более эффективна, чем проще пользователю с ней работать.

– Возможность отключения в экстренных случаях.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать.

Под защитой должна находиться вся система обработки информации.

Разработчики системы защиты, не должны быть в числе тех, кого эта система будет контролировать.

Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.

Объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других.

Надежная система защиты должна быть полностью протестирована и согласована.

Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.

Система защиты должна разрабатываться, исходя из предположения, что пользователи будут совершать серьезные ошибки и, вообще, имеют наихудшие намерения.

Существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

1.4. Средства защиты информации.

Средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных

элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

- *Аппаратные (технические) средства.* Это различные по типу устройства (механические, электромеханические, электронные и др.),

которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, сторожа, защитная сигнализация и др. Вторую - генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны - недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

- *Программные средства* включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств -

универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки - ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств)

1.5. Программные средства защиты информации.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств -- универсальность, гибкость, надежность, простота установки, способность

к модификации и развитию. Недостатки -- ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Программные средства - это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения

Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Среди них можно выделить и подробнее рассмотреть следующие:

- средства архивации данных;
- антивирусные программы;
- криптографические средства;
- средства идентификации и аутентификации пользователей;
- средства управления доступом;
- протоколирование и аудит.

1.6. Анализ программных средств защиты информации

Средства архивации информации

Иногда резервные копии информации приходится выполнять при общей ограниченности ресурсов размещения данных, например владельцам персональных компьютеров. В этих случаях используют программную архивацию. Архивация это слияние нескольких файлов и даже каталогов в единый файл - архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов. Действие большинства средств архивации основано на использовании алгоритмов сжатия, предложенных в 80-х гг. Абрахамом Лемпелем и Якобом Зивом. Наиболее известны и популярны следующие архивные форматы:

- ZIP, ARJ для операционных систем DOS и Windows;
- TAR для операционной системы Unix;
- межплатформный формат JAR (Java ARchive);
- RAR (все время растет популярность этого формата, так как разработаны программы позволяющие использовать его в операционных системах DOS, Windows и Unix).

Пользователю следует лишь выбрать для себя подходящую программу, обеспечивающую работу с выбранным форматом, путем оценки ее характеристик - быстродействия, степени сжатия, совместимости с большим количеством форматов, удобности интерфейса, выбора операционной системы и т.д. Список таких программ очень велик - PKZIP, PKUNZIP, ARJ, RAR, WinZip, WinArj, ZipMagic, WinRar и много других.

Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware).

Антивирусные программы

Это программы разработанные для защиты информации от вирусов. Неискушенные пользователи обычно считают, что компьютерный вирус - это

специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять нежелательные различные действия на компьютере. Специалисты

по компьютерной вирусологии определяют, что обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и файлы, системные области компьютера

и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Следует отметить, что это условие не является достаточным, т.е. окончательным. Вот почему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому

“хорошие” файлы можно отличить от “вирусов”. Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Особую проблему представляют собой компьютерные вирусы. Это отдельный класс программ, направленных на нарушение работы системы и порчу данных. Среди вирусов выделяют ряд разновидностей. Некоторые из них постоянно находятся в памяти компьютера, некоторые производят деструктивные действия разовыми "ударами".

Существует так же целый класс программ, внешне вполне благопристойных, но на самом деле портящих систему. Такие программы называют "троянскими конями". Одним из основных свойств компьютерных вирусов является способность к "размножению" - т.е. самораспространению внутри компьютера и компьютерной сети.

С тех пор, как различные офисные прикладные программные средства получили возможность работать со специально для них написанными

программами (например, для Microsoft Office можно писать приложения на языке Visual Basic) появилась новая разновидность вредоносных программ –

Макро Вирусы. Вирусы этого типа распространяются вместе с обычными

файлами документов, и содержатся внутри них в качестве обычных подпрограмм.

С учетом мощного развития средств коммуникации и резко возросших объемов обмена данными проблема защиты от вирусов становится очень актуальной. Практически, с каждым полученным,

например, по электронной почте документом может быть получен макровирус, а каждая запущенная программа может (теоретически) заразить компьютер и сделать систему неработоспособной.

Поэтому среди систем безопасности важнейшим направлением является борьба с вирусами. Существует целый ряд средств, специально предназначенных для решения этой задачи. Некоторые из них запускаются в режиме сканирования и просматривают содержимое жестких дисков и оперативной памяти компьютера на предмет наличия вирусов. Некоторые же должны быть постоянно запущены и находиться в памяти компьютера. При этом они стараются следить за всеми выполняющимися задачами.

На рынке программного обеспечения наибольшую популярность завоевал пакет AVP, разработанный лабораторией антивирусных систем Касперского. Это универсальный продукт, имеющий версии под самые различные операционные системы. Также существуют следующие виды: Acronis AntiVirus, AhnLab Internet Security, AOL Virus Protection, ArcaVir, Ashampoo AntiMalware, Avast!, Avira AntiVir, A-square anti-malware, BitDefender, CA Antivirus, Clam Antivirus, Command Anti-Malware, Comodo Antivirus, Dr.Web, eScan Antivirus, F-Secure Anti-Virus, G-DATA Antivirus, Graugon Antivirus, IKARUS virus.utilities, Антивирус Касперского, McAfee VirusScan, Microsoft Security Essentials, Moon Secure AV, Multicore antivirus, NOD32, Norman Virus Control, Norton AntiVirus, Outpost Antivirus, Panda и т.д.

Способы обнаружения и удаления неизвестного вируса:

- Профилактика заражения компьютера;
- Восстановление пораженных объектов;

- Антивирусные программы.

Профилактика заражения компьютера

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Для того чтобы определить основные правила компьютерной гигиены, необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word. Пользователь зараженного макро - вирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д. Выводы - следует избегать контактов с подозрительными источниками информации и пользоваться только законными (лицензионными) программными продуктами.

Восстановление пораженных объектов

В большинстве случаев заражения вирусом процедура восстановления зараженных файлов и дисков сводится к запуску подходящего антивируса,

способного обезвредить систему. Если же вирус неизвестен ни одному антивирусу, то достаточно отослать зараженный файл фирмам-производителям антивирусов и через некоторое время (обычно - несколько дней или недель) получить лекарство - “update” против вируса. Если же время не ждет, то обезвреживание вируса придется произвести

самостоятельно. Для большинства пользователей необходимо иметь резервные копии своей информации.

Анализ антивирусных программ

Самыми популярными и эффективными антивирусными программами считаются антивирусные фаги (иначе эти программы называются сканерами или полифагами) и ревизоры (CRC сканеры). Часто обе приведенные разновидности объединяются в одну универсальную антивирусную программу, что значительно повышает ее мощность. Реже используют различного типа мониторы (блокировщики) и вакцины (иммунизаторы). Следует, однако, иметь в виду, что, в принципе, нельзя создать универсальное и абсолютно надежное средство борьбы со всеми существующими и будущими вирусами.

Программы-фаги. Принцип работы антивирусных программ-фагов (сканеров) основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски или, как их еще называют, некоторая постоянная последовательность кода, специфичная для конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Например, перебор всех возможных вариантов кода вирусов. Этот способ эффективно используется для детектирования полиморфных вирусов.

Во многих полифагах используются алгоритмы эвристического сканирования, т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие мягкого решения («возможно, заражен» или «не заражен») для каждого проверяемого объекта.

К достоинствам сканеров относится их универсальность, к недостаткам — низкая скорость сканирования, а также необходимость постоянного обновления антивирусных баз.

Принцип работы типичного алгоритма сканирования сводится к следующему. После загрузки с дискеты, на которой операционная система

гарантированно свободна от вируса, программа проверяет дерево каталогов диска, логическое имя которого указывается в виде параметра при запуске.

При нахождении *.exe или *.cot модуля проверяется его длина. Если длина модуля больше 4 Кбайт, в теле программы ищется сигнатура вируса по соответствующему смещению. Если вирус найден, восстанавливаются скрытые в теле вируса байты начала модуля, после чего длина файла уменьшается на длину вируса и вирус удаляется из зараженного модуля. После этого восстанавливаются исходные время и дата создания файла.

Программы-ревизоры. Они подсчитывают контрольные суммы для присутствующих на диске файлов и системных секторов. Эти суммы сохраняются в базе данных антивируса вместе с некоторой другой информацией: размерами файлов, датами их последней модификации и т.п. При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

Ревизоры, использующие антиСТЕЛС алгоритмы, являются довольно сильным оружием против вирусов: практически 100 % вирусов оказываются обнаруженными почти сразу после их появления в компьютере. Существенным недостатком таких средств борьбы с вирусами является то, что программы-ревизоры распознают наличие вируса в системе уже после его распространения. Кроме того, они не распознают вирусы в новых, только что полученных или записанных файлах, поскольку в их базах данных отсутствует информация об этих файлах. Периодически появляются вирусы, которые используют эту слабость ревизоров, заражая только вновь создаваемые файлы. Такие вирусы остаются невидимыми.

Программы-мониторы. Антивирусные мониторы — это резидентные программы, перехватывающие вирусоопасные ситуации и сообщающие об их возникновении. К вирусоопасным относятся вызовы на открытие для записи в выполняемых файлах, запись в загрузочные секторы дисков, попытки программ остаться резидентно. Иначе говоря, вызовы генерируются вирусами в моменты их размножения.

К достоинствам программ-мониторов относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения, что бывает очень полезно в случаях, когда давно известный вирус постоянно «выползает неизвестно откуда». К недостаткам относятся существование путей обхода защиты монитора и большое количество ложных срабатываний. Существуют аппаратные реализации некоторых функций мониторов, в том числе встроенные в BIOS. Однако, как и в случае с программными мониторами, такую защиту легко обойти прямой записью в порты контроллера диска, а запуск DOS утилиты FDISK немедленно вызывает ложное срабатывание защиты.

Программы-вакцины. Антивирусные вакцины (иммунизаторы) подразделяются на два типа: сообщающие о заражении и блокирующие заражение каким-либо типом вируса. Первые обычно записываются в конец файлов (по принципу файлового вируса), и при запуске файла каждый раз проверяют его на предмет обнаружения изменений. Недостаток у таких вакцин один, но он летален: абсолютная неспособность вакцины сообщить о заражении СТЕЛСвирусом. Поэтому такие иммунизаторы, как и мониторы, в настоящее время практически не используются.

Второй тип вакцин защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженными. Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске зараженной программы, вирус распознает вакцину как свою резидентскую копию и не активизируется. Такой тип вакцинации не может быть универсальным, поскольку при его помощи нельзя иммунизировать файлы от всех известных вирусов. Однако несмотря на это подобные программные средства в качестве полумеры могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет детектироваться антивирусными сканерами.

Антивирусные программные комплексы. В современных условиях лишь они могут обеспечить надежную защиту от вирусных программ, отличающихся большим разнообразием принципов построения и функционирования. Обычно современные антивирусные программные комплексы включают в свой состав монитор, сканер, ревизор и планировщик.

Планировщик используется для координации работы разных компонентов антивирусного пакета и планирования антивирусных мероприятий в вычислительной системе.

Вакцина вследствие своей естественной ограниченности использования низкой универсальности в настоящее время практически не применяется.

Назвать среди большого количества программ, лучший антивирусник невозможно, ведь критериев, которыми могут руководствоваться пользователи при выборе, множество. Несомненно одно - все решения заслуживают внимания пользователей и относятся к числу достойных.

Криптографические средства

Механизмами шифрования данных для обеспечения информационной безопасности общества является криптографическая защита информации посредством криптографического шифрования.

Криптографические методы защиты информации применяются для обработки, хранения и передачи информации на носителях и по сетям связи. Криптографическая защита информации при передаче данных на большие расстояния является единственно надежным способом шифрования.

Криптография - это наука, которая изучает и описывает модель информационной безопасности данных. Криптография открывает решения многих проблем информационной безопасности сети: аутентификация,

конфиденциальность, целостность и контроль взаимодействующих участников.

Термин *«Шифрование»* означает преобразование данных в форму, не читабельную для человека и программных комплексов без ключа

шифрования-расшифровки. Криптографические методы защиты информации дают средства информационной безопасности, поэтому она является частью концепции информационной безопасности.

Криптографическая защита информации (конфиденциальность).

Цели защиты информации в итоге сводятся к обеспечению конфиденциальности информации и защите информации в компьютерных системах в процессе передачи информации по сети между пользователями системы.

Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Важнейшим компонентом криптографического метода защиты информации является ключ, который отвечает за выбор преобразования и порядок его выполнения. Ключ - это некоторая последовательность символов, настраивающая шифрующий и дешифрующий алгоритм системы криптографической защиты информации. Каждое такое преобразование однозначно определяется ключом, который определяет криптографический алгоритм, обеспечивающий защиту информации и информационную безопасность информационной системы.

Один и тот же алгоритм криптографической защиты информации может работать в разных режимах, каждый из которых обладает определенными преимуществами и недостатками, влияющими на надежность информационной безопасности.

Основы информационной безопасности криптографии (Целостность данных)

Защита информации в локальных сетях и технологии защиты информации наряду с конфиденциальностью обязаны обеспечивать и целостность хранения информации. То есть, защита информации в

локальных сетях должна передавать данные таким образом, чтобы данные сохраняли неизменность в процессе передачи и хранения.

Для того чтобы информационная безопасность информации обеспечивала целостность хранения и передачи данных необходима разработка инструментов, обнаруживающих любые искажения исходных данных, для чего к исходной информации придается избыточность.

Информационная безопасность с криптографией решает вопрос целостности путем добавления некой контрольной суммы или проверочной комбинации для вычисления целостности данных. Таким образом, снова модель информационной безопасности является криптографической - зависящей от ключа. По оценке информационной безопасности, основанной на криптографии, зависимость возможности прочтения данных от секретного ключа является наиболее надежным инструментом и даже используется в системах информационной безопасности государства.

Как правило, аудит информационной безопасности предприятия, например, информационной безопасности банков, обращает особое внимание на вероятность успешно навязывать искаженную информацию, а криптографическая защита информации позволяет свести эту вероятность к ничтожно малому уровню. Подобная служба информационной безопасности данную вероятность называет мерой лимитостойкости шифра, или способностью зашифрованных данных противостоять атаке взломщика.

Идентификация и аутентификация пользователя

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс представления компьютерной системе, который включает две стадии:

- идентификацию - пользователь сообщает системе по ее запросу свое имя (идентификатор);

- аутентификацию - пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль).

Для проведения процедур идентификации и аутентификации пользователя необходимы:

- наличие соответствующего субъекта (модуля) аутентификации;
- наличие аутентифицирующего объекта, хранящего уникальную информацию для аутентификации пользователя.

Различают две формы представления объектов, аутентифицирующих пользователя:

- внешний аутентифицирующий объект, не принадлежащий системе;
- внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта.

Внешние объекты могут быть технически реализованы на различных носителях информации - магнитных дисках, пластиковых картах и т. п. Естественно, что внешняя и внутренняя формы представления аутентифицирующего объекта должны быть семантически тождественны.

Управление доступом защиты информации

Управление доступом как один из способов защиты информации - это способ защиты информации с помощью регулирования использования всех ресурсов системы (технических, программных средств, элементов баз данных).

Управление доступом включает следующие функции защиты:

- проверку полномочий, заключающуюся в проверке соответствия времени, ресурсов и процедур установленному регламенту;
- разрешение и создание условий работы в пределах (и только в пределах) установленного регламента;

- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (задержка работ, отключение, сигнализация) при попытках несанкционированных действий.

- идентификацию пользователей, персонала и ресурсов системы, причем под идентификацией понимается присвоение каждому объекту персонального идентификатора (имени, кода, пароля и т.п.)

  и опознание (установление подлинности) субъекта или объекта по предъявленному идентификатору;

Протоколирование и аудит

Под *протоколированием* понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Протоколирование требует для своей реализации здравого смысла. Какие события регистрировать? С какой степенью детализации? На подобные вопросы невозможно дать универсальные ответы. Необходимо следить за тем, чтобы, с одной стороны, достигались перечисленные выше

цели, а, с другой, расход ресурсов оставался в пределах допустимого. Слишком обширное или подробное протоколирование не только снижает производительность сервисов (что отрицательно сказывается на

доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Характерная особенность протоколирования и аудита – зависимость от других средств безопасности. Идентификация и аутентификация служат отправной точкой подотчетности пользователей, логическое управление доступом защищает конфиденциальность и целостность регистрационной информации. Возможно, для защиты привлекаются и криптографические методы.

Защита информации в КС от несанкционированного доступа

Для осуществления несанкционированного доступа злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав КС. Он осуществляет несанкционированный доступ, используя:

- знания о КС и умения работать с ней;
- сведения о системе защиты информации;
- сбои, отказы технических и программных средств;
- ошибки, небрежность обслуживающего персонала и пользователей.

Для защиты информации от несанкционированного доступа создается

система разграничения доступа к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа возможно только при сбоях и отказах КС, а также используя слабые места в комплексной системе защиты информации. Чтобы использовать слабости в системе защиты, злоумышленник должен знать о них.

Одним из путей добывания информации о недостатках системы защиты является изучение механизмов защиты. Злоумышленник может тестировать систему защиты путем непосредственного контакта с ней. В этом

случае велика вероятность обнаружения системой защиты попыток ее тестирования. В результате этого службой безопасности могут быть предприняты дополнительные меры защиты.

Гораздо более привлекательным для злоумышленника является другой подход. Сначала получается копия программного средства системы защиты или техническое средство защиты, а затем производится их исследование в лабораторных условиях. Кроме того, создание неучтенных копий на съемных носителях информации является одним из распространенных и удобных способов хищения информации. Этим способом осуществляется несанкционированное тиражирование программ. Скрытно получить техническое средство защиты для исследования гораздо сложнее, чем программное, и такая угроза блокируется средствами и методами обеспечивающими целостность технической структуры КС. Для блокирования несанкционированного исследования и копирования информации КС используется комплекс средств и мер защиты, которые объединяются в систему защиты от исследования и копирования информации. Таким образом, система разграничения доступа к информации

и система защиты информации могут рассматриваться как подсистемы системы защиты от несанкционированного доступа к информации.

Другие программные средства защиты информации

Межсетевые экраны (также называемые брандмауэрами или файрволами - от нем. Brandmauer, англ. firewall -- «противопожарная стена»).

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 (вирусы, 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.

Вывод по главе 1

Информация это ресурс, потеря и повреждение которого приводит к моральному или материальному ущербу. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Проблема информационной безопасности образовательной организации превращается в последнее время из гипотетической во вполне реальную. Количество угроз растет с каждым днем, изменяется нормативно-правовая база, соответственно реалиям времени должны изменяться и методы обеспечения информационной безопасности учебного процесса.

В современной ОО информация, информационная инфраструктура – один из главных компонентов учебного процесса. Учебные классы оснащаются компьютерной техникой и её качественное бесперебойное

функционирование существенно определяет качество полученных знаний, способствует формированию профессиональных компетенций учащихся.

Вот поэтому-то обеспечение информационной безопасности учебного процесса, в том числе непрерывного функционирования компьютерных и информационных ресурсов, является весьма важной для его качества.

Для обеспечения информационной безопасности используются различние средства защиты информации.

Основные направления использования программной защиты информации:

- защита информации от НСД,
- защита программ от копирования,
- защита информации от разрушения,
- защита информации от вирусов,
- защита программ от вирусов,
- программная защита каналов связи.

По каждому из данных направлений имеется большое количество качественных программных продуктов, распространяемых на рынке.

Но для осуществления информационной безопасности образовательного учреждения требуется программа, которая будет включать в себя целый комплекс защиты и множество подконтрольных программ.

ГЛАВА 2.ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ (ОО)

2.1 Информационная безопасность образовательных организаций

Учитывая изложенное, под информационной безопасностью ОО следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Построение системы информационной безопасности в школе происходит следующим образом. На первом этапе определяется, что подлежит защите. На втором этапе выявляются возможные каналы утечки информации и определяются возможные угрозы информационным системам. Далее вырабатываются меры по защите информации и технологических систем. На основе выработанных мер

защиты разрабатываются нормативно-правовые документы, регламентирующие информационную безопасность. В последующем организуется контроль за соблюдением установленных правил. При таком подходе система информационной безопасности будет направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию. В целях обеспечения информационной безопасности и ее организации, на основании законодательных документов, в ОО следует разрабатывать соответствующие нормативно-правовые акты. Правовые нормы обеспечения информационной безопасности в конкретном

ОО фиксируются в учредительных, организационных и функциональных документах. Требования обеспечения информационной безопасности отражаются в уставе (учредительном договоре) в виде следующих положений:

- ОО имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных учащихся,

работников ОО, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз;

- ОО обязано обеспечить сохранность конфиденциальной информации. Такие требования дают право администрации ОО:

- назначить ответственного за обеспечение информационной безопасности;

- издаватьнормативныеираспорядительныедокументы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- включать требования по обеспечению информационной безопасности в коллективный договор;

- включать требования по защите информации в договоры по всем видам деятельности; разрабатывать перечень сведений конфиденциального характера;

- требовать защиты интересов ОО со стороны государственных и судебных инстанций.

К организационным и функциональным документам следует отнести:

- приказ руководителя ОО о назначении ответственного за обеспечение информационной безопасности;

- должностные обязанности ответственного за обеспечение информационной безопасности;

- перечень защищаемых информационных ресурсов и баз данных;

- инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников ОО.

Данный перечень документов не является исчерпывающим. В зависимости от особенностей, специфики и характера ОО он может быть

расширен и дополнен. Кроме того, должен быть определен порядок допуска сотрудников ОО к информации.

Такой допуск предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и ОО об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

- инструктаж работника специалистом по информационной безопасности; - контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

Как показала практика, при проверке организации системы информационной безопасности, как правило, отмечаются следующие недостатки:

- отсутствует перечень сведений, составляющий конфиденциальную информацию;

- отсутствуют должностные обязанности ответственного за информационную безопасность;

- не соблюдается порядок учета носителей информации конфиденциального характера;

- нарушен порядок делопроизводства.

Самым серьезным недостатком в организации информационной безопасности является отсутствие взаимопонимания между теми, кто обеспечивает информационную безопасность, и теми, кто пользуется данной информацией. Нередко пользователи информации нарушают порядок обращения с ней и не соблюдают требования нормативно-правовых документов, регламентирующих информационную безопасность. Решение данной проблемы возможно только при соблюдении принципов

информационной безопасности, постоянной требовательности по соблюдению конфиденциальности со стороны руководителя ОО.

С учетом этих недостатков для обеспечения информационной безопасности в ОО требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности ОО;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета в классе информатики ОО;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и учащихся ОО;
- учет всех носителей конфиденциальной информации.

Реализация данного комплекса мер вносит кардинальные изменения в организацию работы с информацией в ОО, а также делопроизводства, в т. ч. и по вопросам безопасности.

При таком подходе, основными составными задачами делопроизводства станут: документирование информации, учет документов, организация документооборота, обеспечение надежного хранения документов, своевременное их уничтожение, проверка наличия хранящихся документов, контроль за своевременным и правильным их исполнением. Необходимо помнить, что не на всяком документе имеется гриф "Для служебного пользования" ("Ограниченного пользования"), однако это не означает, что такой документ не представляет никакой ценности. Не бывает важных или не очень важных документов. Самый малозначительный, на первый взгляд документ, при определенных обстоятельствах может оказаться чрезвычайно важным. Организация вышеперечисленных мероприятий позволит избежать непредвиденных ситуаций, путаницы и неразберихи. Следует отметить, что при организации делопроизводства необходимо выявить и учесть все возможные каналы утечки информации. Наиболее характерными каналами утечки информации для ОО могут стать разглашение, хищение и несанкционированный доступ. Учитывая эти аспекты, систему организации делопроизводства можно представить в следующем виде:

– учет всей документации ОО, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

– регистрация и учет всех входящих (исходящих) документов ОО в

специальном журнале информации о дате получения (отправления)

документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

– регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

– особый режим уничтожения документов. Уничтожать документы можно с помощью уничтожителя бумаг, или сжиганием. В обязательном порядке нужно составлять об этом акт, подписываемый комиссией, назначенной приказом руководителя ОО.

Для облегчения контроля все документы следует разделить на две группы: для общего пользования и для служебного пользования (ограниченного пользования). Документам каждой категории необходимо присвоить свой гриф. Это можно сделать при помощи штампов, специальных отметок или цветового выделения (для общего пользования – зеленый цвет, для служебного – красный). При присвоении соответствующего грифа соблюдаются определенные правила, которые необходимо учитывать в своей работе: ответственность за присвоение соответствующего грифа несет исполнитель документа, а субъектом оценки его присвоения является руководитель ОУ; ценность информации определяется с помощью таких критериев, как полезность, своевременность, актуальность, достоверность, конфиденциальность; информация подлежит защите при условии, что доступ к ней закрыт на законном основании. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила: Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах.

Для создания безопасной информационной системы в ОО можно принять меры:

- Обеспечить защиту компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.)

- Установить строгий контроль за электронной почтой, обеспечить постоянный контроль за входящей и исходящей корреспонденции.

- Использовать контент-фильтры для фильтрации сайтов по их содержимому.

Одна сумма всех этих мероприятий, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Специалисты, которые имеют отношение к системе защиты, должны быть в полной мере представить себе принципы ее функционирования и в случае возникновения сложной ситуации адекватно реагировать. Под защитой должна находиться вся система обработки информации.

Лица, занимающиеся обеспечением информационной безопасности, должны нести ответственность.

Надежная система защиты должна быть полностью протестирована и совместима. Защита становится более эффективной и гибкой, если она допускает изменение их параметров со стороны администратора.

2.2 Меры информационной защиты образовательной организации СПО.

Борьба с различными видами атак на информационную безопасность должна вестись на пяти уровнях, причем работа должна носить комплексный

характер. Существует ряд методических разработок, которые позволят построить защиту образовательного учреждения на необходимом уровне.

Нормативно-правовой способ защиты информационной безопасности.

В России принята «Национальная стратегия действий в интересах детей», определяющая степень угроз и меры защиты их безопасности.

Действия по ограничению агрессивного воздействия на сознание ребенка должны стать основными. На втором месте должно оказаться обеспечение безопасности баз данных.

Защита информации опирается на действующие в этой сфере законы, определяющие отдельные ее массивы как подлежащие защите. Они выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна). Порядок защиты персональных данных определяется в том числе федеральным законом «Об информации», Трудовым кодексом. Они и Гражданский кодекс помогают разработать методику для обеспечения защиты сведений, относящихся к коммерческой тайне. Кроме законов необходимо выделить действующие в этой сфере ГОСТы, определяющие порядок защиты данных, и применяемые в этих целях методики и аппаратные средства.

Морально-этические средства обеспечения информационной безопасности.

В образовательной сфере большую роль играет система морально-этических ценностей. На ней должна основываться система мер, защищающих подростка от травмирующей, этически некорректной, незаконной информации. В целях защиты от пропаганды необходимо применять нормы закона «О защите прав ребенка», определяющие его права на защиту от сведений, которые могут причинить моральную травму.

Необходимо создавать перечни документов, программ и иных источников, которые могут травмировать психику детей, в целях недопущения их

проникновения на территорию учебного заведения. Это станет одной из основ информационной безопасности.

Административно-организационные меры.

Этот комплекс мер целиком построен на создании внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями. Это внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни сведений, не подлежащих передаче. Дополнительно должен быть разработан регламент, определяющий порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и документов.

Кроме того, эти методики должны определять порядок доступа детей к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов неоднозначного характера от доступа ребенка, запрет на пользование собственными носителями информации. Должно быть предусмотрено использование системы родительского контроля над ресурсами сети Интернет.

Физические меры.

За данную систему мер и ее внедрение должно отвечать руководство образовательного учреждения и сотрудники IT-подразделений. Перекладывать организацию мер физической защиты компьютерной сети и носителей на сотрудников наемных охранных подразделений недопустимо. Среди физических мер должна быть предусмотрена пропускная система защиты в помещения, содержащие носители информации, организация контроля доступа посетителей, установления различных степеней допуска. Кроме того, к мерам физической защиты может быть отнесено обязательное копирование значимой информации на диски компьютеров, не имеющих

доступа к сети Интернет. Обязательно не только установление паролей, но и их регулярная замена.

Технические меры.

Комплексную систему защиты всего периметра компьютерной сети должны обеспечивать специализированные программные продукты, например, DLP-системы и SIEM-системы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними. Для тех учебных заведений, бюджет которых не позволяет внедрение профессиональных систем, необходимо использование разрешенных и рекомендуемых программных мер защиты, в частности антивирусов.

Электронная почта, к которой имеют доступ сотрудники и учащиеся, должна быть контролируема. Оптимально также ввести полный запрет на копирование любой информации с жестких дисков компьютеров образовательного учреждения.

Кроме того, должно быть предусмотрено программное обеспечение, ограничивающее доступ ребенка на определенные сайты (контент-фильтры).

Все меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности. Желательно привлечение к этой проблеме родителей учеников, в ряде случаев они помогут провести аудит мер безопасности и порекомендовать современные решения. Кроме того, на родителей должны быть возложены обязанности и по ограничению информации, которую ребенок может получить дома. Необходимо просматривать страницы, посещаемые ребенком. На основании анализа его поиска можно вносить изменения в перечень сайтов, доступ к которым ограничен с компьютеров, установленных в учебном заведении.

2.3 SIEM-системы

SIEM является составляющей SOC, поэтому играет важную роль в информационной безопасности.

SOC (Security Operation Center) – это центр управления событиями ИБ, представляет собой комплекс процессов и программно-аппаратных средств, предназначенный для централизованного сбора и анализа информации о

событиях и инцидентах ИБ, поступающих из различных источников ИТ-инфраструктуры, и своевременное реагирование на них.

SIEM-системы, как и многие другие продукты появились в результате эволюционного развития и последующего слияния систем SEM и SIM.

SEM (Security Event Management) - системы действуют в режиме приближённом к реальному времени. Для этого им требуется: автоматический мониторинг событий, их сбор, корреляция, генерация предупреждающих сообщений.

SIM (Security Information Management) - системы, в свою очередь, анализируют накопленную информацию со стороны статистики, различных отклонений от «нормального поведения» и т.д.

Когда же возможности SIM и SEM объединяются в рамках одного продукта, говорят о SIEM-системах. Исходя из этого, можно дать «литературный» перевод аббревиатуры SIEM – система сбора и корреляции событий.

Важно понимать, что SIEM-системы в качестве самостоятельного (standalone) решения не предназначены и не способны предотвращать инциденты нарушения информационной безопасности. Их сущность заложена в их названии: анализ информации, поступающей из различных источников (DLP, IDS, антивирусы, межсетевые экраны и т.д.), и дальнейшее выявление отклонений от норм по заданным критериям. Тем не менее, «плюсов» вполне достаточно.

Перед системой SIEM ставятся следующие задачи:

- Консолидация и хранение журналов событий от различных источников.

- Предоставление инструментов для анализа событий и разбора инцидентов.
- Корреляция и обработка событий по правилам.
- Автоматическое оповещение и инцидент-менеджмент.

Перейдём к рассмотрению принципов работы SIEM-систем.

В теории всё просто: система собирает информацию, анализирует «на лету» (и генерирует предупреждающее сообщение), складывает в базы данных, анализирует поведение на основании предыдущих наблюдений (и генерирует предупреждающее сообщение).

На практике схема реализуется с помощью соответствующих компонентов:

- Агенты (сбор данных из различных источников);
- Серверы-коллекторы (аккумуляция информации, поступившей от агентов);
- Сервер баз данных (хранение информации);
- Сервер корреляции (анализ информации).

Входной информацией для SIEM-систем может служить практически любая информация. Главное – правильно её подать. Как уже было сказано выше, сбор данных может осуществляться с помощью специальных агентов, которые представляют собой программу, которая локально собирает журналы событий и по возможности передает их на сервер. Для «вычитки» того или иного источника данных агент использует коллекторы - библиотеки для понимания конкретного журнала событий или системы. Коллекторы играют важную роль, так как разные источники могут именовать одно и то же событие по-своему. Например, Firewall одного производителя может записывать в отчёт deny, другого discard, третьего drop, хотя событие одно и тоже. Коллекторы помогают привести все эти события к общему знаменателю.

Если же для источника нет соответствующего коллектора, события можно попробовать отправлять как SYSLOG (при условии, что источник умеет это делать). Однако и здесь можно столкнуться с «проблемой синонимов» и необходимостью писать дополнительный обработчик для приведения данных в единый формат.

Также информацию можно собирать удалённо при помощи соединения по протоколам NetBIOS, RPC, TFTP, FTP. Однако в этом случае

может возникнуть проблема с нагрузкой на сеть, так как часть систем позволяет передавать только журнал целиком, а не «свежие» записи.

SIEM-системы могут использовать следующие источники информации:

- Access Control, Authentication. Применяются для мониторинга контроля доступа к информационным системам и использования привилегий.
- DLP-системы. Сведения о попытках инсайдерских утечек, нарушении прав доступа.
- IDS/IPS-системы. Несут данные о сетевых атаках, изменениях конфигурации и доступа к устройствам.
- Антивирусные приложения. Генерируют события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном коде.
- Журналы событий серверов и рабочих станций. Применяются для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности.
- Межсетевые экраны. Сведения об атаках, вредоносном ПО и прочем. Сетевое активное оборудование. Используется для контроля доступа, учета сетевого трафика.
- Сканеры уязвимостей. Данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостей, поставка инвентаризационных данных и топологической структуры.
- Системы инвентаризации и asset-management. Поставляют данные для контроля активов в инфраструктуре и выявления новых.
- Системы веб-фильтрации. Предоставляют данные о посещении

сотрудниками подозрительных или запрещенных веб-сайтов.

Получив информацию, система может её проанализировать. В основе анализа лежит практически «чистая» математика и статистика. Но отправной

точкой служат задаваемые вручную правила. К примеру, однократное событие «login failed» ничего не значит, в то время как три и более таких события от одной учетной записи уже могут свидетельствовать о попытках подбора пароля.

В простейшем случае в SIEM-системах правила представлены в формате RBR (Rule Based Reasoning) и содержат набор условий, триггеры, счетчики, сценарий действий.

- сетевые атаки во внутреннем и внешнем периметрах;
- вирусные эпидемии или отдельные вирусные заражения;
- попытки несанкционированного доступа к конфиденциальной информации;
- мошенничество;
- ошибки и сбои в работе информационных систем;
- уязвимости;
- ошибки конфигураций в средствах защиты и информационных системах;
- целевые атаки (APT).

2.4. Анализ программного комплекса защиты информации для образовательной организации СПО.

Рынок SIEM-систем сложился довольно давно. На нем представлены технические решения различных производителей. Все они

отличаются по архитектуре, возможностям масштабирования, полноте функционала, спектру решаемых прикладных ИБ-задач. Большая часть этих решений пошла по пути развития систем сбора и централизованного хранения событий с различных устройств (Log Management). Со временем появились корреляция событий и выявление инцидентов. На данный момент каждый производитель старается дополнить функционал SIEM вспомогательными

функциями, такими как управление уязвимостями, рисками, поиск аномалий в сетевых протоколах, формирование списков зараженных IP-адресов и т.д. Для выявления наиболее оптимальной системы, было решино сравнить функционал ряда SIEM-систем, чтобы дать обобщенное представление об их возможностях. При подготовке списка сравниваемых решений, в том числе опирались на отчеты международных аналитических агентств, в первую очередь – компании Gartner , а также на популярность решений на российском рынке. (Для анализа «способности реализации» аналитики Gartner принимают во внимание семь критериев, связанных с опытом клиента при использовании продукта или сервиса. Эта оценка включает простоту установки, использования, администрирования и масштабирования, стабильность работы и последующую сервисную поддержку. Для сбора информации аналитики проводят интервью с потребителями услуг поставщиков, а также собирают отзывы клиентов Gartner, которые пользовались SIEM-системами. По шкале «полнота видения» оценивается способность организации понимать потребности клиента и воплощать это в своих продуктах и сервисах.)

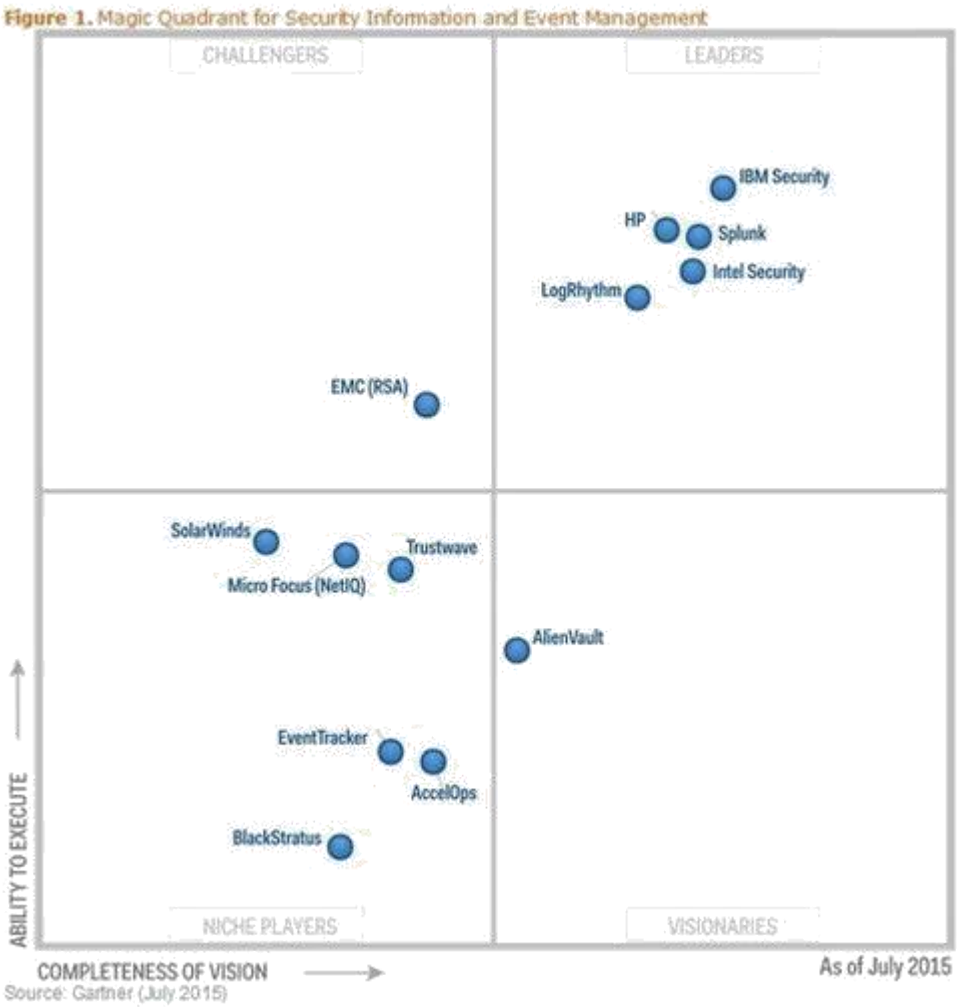

Рис. 2. Gartner Magic Quadrant for Security Information and Event Management, July 20

Основными функциями SIEM являются корреляция событий и выявление инцидентов информационной безопасности. Ввиду малой распространенности на рынке России и СНГ таких продуктов, как Splunk и LogRhythm, мы решили не рассматривать эти платформы в нашей статье.

По моему мнению, среди отечественных решений наиболее перспективной является платформа Positive Technologies. Несмотря на то, что платформа основана на Open Source, компания способна развивать свое решение самостоятельно.

Таким образом, в список сравниваемых нами решений попали:

- HP ArcSight
- IBM QRadar

- Intel Security McAfee ESM
- RSA Security Analytics
- Positive Technologies MaxPatrol SIEM

Так как все компании разные, ожидания от SIEM-систем у них различны (мы говорим о компаниях X и Y из первой статьи нашего номера), соответственно, разнятся и приоритеты в части функциональных возможностей. Поэтому мы вводим весовую модель для определения оптимальной платформы для компаний X и Y, где значение 5 – это максимально важный критерий для организации, а 1 – соответственно, наоборот.

1. Поддержка источников событий (5)
2. Сбор событий (8)
3. Корреляция (10)
4. Поиск данных и аналитика (9)
5. Визуализация и отчетность (5 и 5 соответственно)
6. Оповещение и приоритизация (5 и 5 соответственно)
7. Общие настройки и предустановленный функционал (5 и 3 соответственно)
8. Масштабируемость, отказоустойчивость и хранение (8, 5 и 7 соответственно)
9. Мониторинг компонентов системы и внутренний аудит (3)
10. Удобство использования (10)
11. Наличие сертификатов соответствия ФСТЭК (2)
12. Дополнительные модули системы (5)

Для оценки степени выполнения критериев сравнения мы ввели следующие виды оценок: 0 – критерий не выполняется; 1 – критерий выполняется частично; 2 – критерий полностью выполняется. Далее мы разбираем каждый блок. Результат тестирования по первому блоку – поддержка источников событий – представлен в табл. 1

		PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analytics**	**McAfee ESM**
Критерий	**Параметры**	**Оценки**				
Поддержка источников событий	Количество поддерживаемых источников событий	1	2	2	1	1
	Качество парсинга событий	1	1	2	1	1
	Частота обновлений коннекторов/парсеров событий	2	2	2	1	1
	Возможность автообновления парсеров событий	1	2	0	2	2
	Возможность подключения нестандартных источников *(упоминание о количестве поддерживаемых*	2	2	2	2	2

	транспортов)					
	Автообнаруже-ние источников событий (автоматическое заведение источников событий при получении логов по syslog)	2	2	2	2	2

Табл. 1 Поддержка источников событий.

PT MaxPatrol SIEM. Количество поддерживаемых источников постоянно растет. Известные поддерживаемые источники – Syslog, Windows

Event Log, Windows File log, Windows WMI log, NetFlow, ODBC Log, Checkpoint LEA, SNMP Traps, SSH File Log, Telnet File Log. Max Patrol SIEM

– новый продукт на рынке SIEM, он не дотягивает до гигантов индустрии по количеству поддерживаемых систем, но очень динамично развивается.

Российские корни вендора могут дать продукту поддержку отечественных источников событий, отсутствующих во всех его западных конкурентах. Для разработки правил нормализации используется SDK, собственный язык программирования позволяет гибко нормализовать практически любое событие. Автообнаружение источников событий в системе присутствует, база источников периодически пополняется

IBM QRadar. Платформой поддерживается более 300 стандартных источников событий. Полноценная категоризация определена для большей части основных событий аудита, но довольно часто встречаются и события без категории. Качество парсинга обусловлено и используемой схемой хранения событий, включающей небольшое количество наиболее критичных полей. Обновления коннекторов/парсеров событий выпускаются вендором по мере выхода исправлений и дополнений. Присутствует автообновление парсеров событий. Для подключения нестандартных источников могут применяться часто используемые транспорты. Разработка собственных парсеров происходит по большей части в основном интерфейсе продукта, для описания событий используется regex.

HP ArcSight. Платформой поддерживается более 300 стандартных источников событий. Все события категоризированы, и их имена определены. Помимо этого, коннекторы многих систем включают в себя несколько вариантов парсеров, что позволяет выбрать наиболее подходящий под конкретные цели алгоритм обработки аудита. Обновления коннекторов/парсеров событий выпускаются вендором по мере выхода исправлений и дополнений – 2–3 раза в квартал. Возможность

автообновления парсеров событий отсутствует. Вендор заверяет, что это сделано намеренно, поскольку автообновление в производственной среде

может привести к изменению корреляционной логики. У многих заказчиков на корреляционную логику завязаны SLA, эскалации, документооборот – здесь важно, чтобы все изменения SIEM-системы проходили контролируемым образом. Кроме того, наличие подключения SIEM-системы

к сети Интернет создает определенные риски. Для подключения нестандартных источников могут применяться часто используемые транспорты. Механизм разработки коннекторов, реализованный в ArcSight,

является одним из самых мощных и гибких. Он позволяет не только разложить событие по определённым полям, но и с помощью множества встроенных функций изменять эти значения, а также реализовывать логические операции, основываясь на значениях определённых токенов. Коннектор представляет собой текстовый файл определённого формата, для описания событий используется regex. Для разработки также существует несколько графических утилит.

RSA Security Analytics. Поддерживается большое количество разнородных систем. Более 250 поддерживаемых стандартных источников событий. Для парсинга в платформу заложена многоуровневая модель обработки события. Есть проблемы с опознанием систем по событиям. При разборе событий возникают проблемы с кириллицей. Нет регулярности в выходе обновлений коннекторов/парсеров. Обновления выходят в зависимости от популярности подключаемого нестандартного источника. Поддерживается автообновление парсеров событий. Для разработки коннекторов используется модуль прошлого SIEM от RSA – enVision. Парсер представляет собой текстовый файл XML-формата. Как приемник RSA enVision, RSA SA использует многие его парсеры. Платформой поддерживаются следующие виды транспортов: AWS, Checkpoint, File Collection, Netflow Collection, ODBC, SDEE, SNMP, VMware, Windows, Legacy Windows и NetApp. Присутствует автообнаружение источников событий.

McAfee ESM. Решение поддерживает большое количество разнородных источников событий (более 400 систем: WMI, Syslog, SCP, FTP, HTTP(S), ODBC/MSSQL, OPsec, CEF, MEF). Обработка событий выполняется корректно. Но отсутствует механизм траблшутинга парсинга событий. Например, для аудита СУБД очень сложно разобраться, почему может не осуществляться парсинг событий. Обновления коннекторов выходят регулярно и доступны сразу для всего модельного ряда. Поддерживается автообнаружение источников событий. Поддерживается создание собственных парсеров событий. Разработка происходит в основном интерфейсе продукта, для описания событий используется regex. Сбор событий Результаты тестирования решений по критериям блока «Сбор событий» представлены в табл. 2.

		PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analytics**	**McAfee ESM**
Крите-рий	**Параметры**	**Оценки**				
Сбор событий	Нормализация (перевод записей лог-журналов в единый стандартный вид)	1	1	2	2	1
	Агрегация (объединение одинаковых событий)	1	1	2	2	1
	Фильтрация (запись					

	событий, удовлетворяющих определенным условиям)	2	1	2	2	2
	Контроль целостности данных	0	2	2	1	1
	Возможность сбора, хранения, работы по raw-событиям	2	2	2	2	2

	Возможность хранения данных в течение разного периода времени, разделения данных на физическом и логическом уровне	1	2	2	1	2
	Маскирование данных при сборе\отображении в консоли	0	2	2	0	0
	Возможность мониторинга сетевого трафика (в том числе до 7-го уровня)	0	2	1	2	1

Табл. 2. Сбор событий.

PT MaxPatrol SIEM. Присутствуют механизмы нормализации, агрегации и фильтрации событий. Нормализация производится только для определённых типов событий. Поддерживается возможность сбора, хранения и работы по raw-событиям. Отсутствует маскирование данных при сборе/отображении в консоли. Платформой поддерживается мониторинг

сетевого трафика вплоть до 7-го уровня модели OSI при помощи дополнительного модуля MaxPatrol X Network Traffic.

IBM QRadar. Схема нормализации имеет 19 полей. Встречается много событий, которые плохо нормализуются. Агрегация присутствует, но она не настраиваемая. Также поддерживается фильтрация, но отфильтрованные события учитываются в лицензионном ограничении. Обеспечиваются маскирование данных и мониторинг сетевого трафика вплоть до 7-го уровня модели OSI.

HP ArcSight. Схема нормализации имеет более 200 полей. События хорошо нормализуются. Присутствует возможность гибкой настройки

параметров агрегации. Поддерживается маскирование данных. Мониторинг NetFlow до 7-го уровня модели OSI осуществляется путем интеграции HP ArcSight и HP Tipping Point. Включение передачи событий из Tipping Point в ArcSight поддерживается решением по умолчанию и осуществляется одним действием в интерфейсе управления.

RSA Security Analytics. Поддерживаются нормализация, агрегация и фильтрация событий. Для контроля целостности данных требуется использование дополнительного модуля Archiver. Работа по raw-событиям гораздо медленнее по сравнению с конкурентами. Возможность хранения данных в течение разного периода времени, их разделения на физическом и логическом уровне также требует использования дополнительного модуля Archiver. Отсутствует маскирование данных. Мониторинг сетевого трафика вплоть до 7-го уровня модели OSI осуществляется с помощью модуля Packet Decoder.

McAfee ESM. Процесс нормализации приводит все события в формат MEF (McAfee Event Format). Осуществляется категоризация событий. Агрегация присутствует. Есть ограничения по агрегации – максимум 3 значения, по которым можно ее выполнить. Параметры агрегации можно переопределить. Разбор сетевого трафика на уровне приложений осуществляется путем интеграции с решением IPS от McAfee.

Корреляция

Результаты тестирования решений по критериям блока «Корреляция» представлены в табл. 3.

		PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analitycs**	**McAfee ESM**
Критерий	**Параметры**	**Оценки**				

Корреляция	Базовая корреляция	2	2	2	2	2

	Поведенческий анализ	0	2	2	2	1
	Обогащение данных из других систем	2	2	2	2	2
	Историческая корреляция	1	2	2	0	2

Табл. 3. Корреляция

PT MaxPatrol SIEM. Реализованы механизмы real-time корреляции событий. Отсутствуют механизмы для проведения поведенческого анализа. Поддерживается обогащение данных в пределах платформы MaxPatrol X. Проведение корреляции исторических данных планируется реализовать в следующих релизах.

IBM QRadar. Реализованы механизмы real-time корреляции событий, есть возможность провести поведенческий анализ, осуществляется обогащение данных из других систем, поддерживается корреляция исторических данных.

HP ArcSight. В продукте реализован один из наиболее гибко настраиваемых корреляционных механизмов. Возможно обогащение собираемых данных из сторонних систем на уровнях сбора (в коннекторе) и обработки (на менеджере). Историческая корреляция ограничена возможностью ручной проверки правила на исторических данных определённого временного интервала. Генерация корреляционных событий при этом не происходит.

RSA Security Analytics. В ядре системы заложен достаточно слабый корреляционный функционал, для полноценной корреляции возможно

использование дополнительного модуля ESA. Функционал исторической корреляции в платформе отсутствует.

McAfee ESM. Реализованы механизмы real-time корреляции событий. При проведении поведенческого анализа есть возможность просмотреть два

наложенных графика – статистику по событиям за предыдущий период и текущую статистику (онлайн). Для работы с историческими данными необходимо использовать компонент McAfee Advanced Correlation Engine (ACE). Этот модуль может выполнять и историческую корреляцию, но в один момент времени он может работать только в одном из режимов (real-time или исторической корреляции).

Поиск данных и аналитика.

Результаты тестирования решений по критериям блока «Поиск данных и аналитика» представлены в табл. 4.

		PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analitycs**	**McAfee ESM**
Критерий	**Параметры**	**Оценки**				
Поиск данных и аналитика	Возможности по поиску событий	2	2	2	2	2
	Возможность группировки событий	2	2	2	2	2
	Возможности Drilldown по полям	2	1	2	2	2
	Google Like Search	2	2	2	1	2
	Скорость работы	1	2	2	2	2

	интерфейса					
	Возможность применения активного воздействия	0	2	2	2	2
	Использование встроенных средств диагностики компонентов системы и создание своих	1	2	2	2	1

Табл. 4. Поиск данных и аналитика.

PT MaxPatrol SIEM. Поддерживается поиск по событиям. Присутствует возможность группировки событий, Drilldown по полям и применения активного воздействия. Поддерживается механизм Google Like Search. Скорость работы интерфейса в боевой системе средняя. В качестве средств диагностики компонентов системы используются файлы журналов компонентов. События аудита работы самой системы не попадают в основной поток событий SIEM. Есть возможность активного воздействия средствами самой платформы (сканирование), а также выполнения скриптов.

IBM QRadar. Поддерживаются поиск по событиям и группировка событий. Drilldown по полям осуществляется в несколько действий. Присутствует механизм Google Like Search. Скорость работы интерфейса высока с учетом выполнения аппаратных требований. События аудита работы самой системы являются частью основного потока событий SIEM. Существуют преднастроенные правила, реагирующие на критичные события диагностики внутренних компонентов. Присутствует возможность создания своих правил. Поддерживается возможность выполнения скриптов.

HP ArcSight. Поддерживаются поиск по событиям и группировка событий. Drilldown по полям осуществляется в несколько действий, есть возможность создания нескольких различных Drilldown для одного Dashboard. Механизм Google Like Search реализован только в web-интерфейсах продукта. Скорость работы интерфейса высока с учетом выполнения аппаратных требований. События аудита работы самой системы являются частью основного потока событий SIEM. Существуют преднастроенные правила, реагирующие на критичные события диагностики внутренних компонентов. Присутствует возможность создания своих правил. Также есть возможность выполнения команд на некоторых продуктах HP (а также некоторых других вендоров), кастомных скриптов (на менеджере или коннекторах).

RSA Security Analytics. Поддерживаются поиск по событиям и группировка событий. Drilldown по полям осуществляется в несколько

действий. Механизм Google Like Search доступен при использовании дополнительного модуля Warehouse. Скорость работы интерфейса высокая с учетом выполнения аппаратных требований. Существуют встроенные средства диагностики компонентов системы.

McAfee ESM. На практике встречаются ситуации, когда скорость работы интерфейса падает: например, при выборке по небольшому промежутку данных, которые были зафиксированы более 3 месяцев назад. Создание собственного dashboard и поиск по нему приводят к задержкам. Есть предположение, что индексируется только строго определенные значения (SRC IP, DST IP и т.п.). Соответственно, поиск по другим значениям занимает длительное время. Присутствуют средства диагностики компонентов системы, но зачастую нужно обращаться к вендору, т.к. штатная диагностика обычно говорит о том, что события не поступают, ресивер не доступен и т.п.

Визуализация и отчетность

Результаты тестирования решений по критериям блока «Визуализация и отчетность» представлены в табл. 5.

		PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analitycs**	**McAfee ESM**
Критерий	**Параметры**	**Оценки**				
Визуализация	Типы графического представления	1	1	2	2	2
	Поля графического представления	2	1	2	0	2
	Возможности					

	кастомизации графических панелей	1	1	2	2	2
Отчетность	Возможность перемещения графических панелей	0	2	2	2	2
	Наличие русского интерфейса	2	2	2	0	0
	Форматы	1	2	2	2	2

	отчетов					
	Возможность запуска отчетов за большие промежутки времени	1	2	2	2	2
	Поддержка создания отчетов по заданному расписанию	1	2	2	2	2
	Возможность переименования полей отчетов	1	2	2	2	2

Табл. 5. Визуализация и отчетность.

PT MaxPatrol SIEM. Доступны гистограммы и графики, а также таблицы и отчеты. Интерфейс русифицирован. Есть встроенные отчеты, формат, поля, промежутки времени, но для их кастомизации необходимо использовать SDK.

IBM QRadar. По умолчанию доступны 9 типов графического представления. Существуют некоторые ограничения в кастомизации графических панелей. Интерфейс русифицирован. Отчеты могут быть экспортированы в файлы следующих форматов: MS Excel, RTF, PDF, XML, HTML.

HP ArcSight. Доступны более 20 типов графического представления. В качестве полей графического представления используются Data Monitor, Dashboard, Query Viewer. Русифицированный интерфейс решения доступен с

февраля 2015 года. Отчеты могут быть экспортированы в следующие форматы: MS Excel, RTF, PDF, CSV, HTML.

RSA Security Analytics. Доступны более 5 типов графического представления. В качестве полей графического представления используются Dashboard, System Stats. Русский интерфейс отсутствует. Отчеты могут быть экспортированы в следующие форматы: MS Excel, RTF, PDF, CSV, HTML.

McAfee ESM. Доступны следующие типы графического представления: табличное, pie chart, bar chart, графики, граф коммуникаций

на основе анализа NetFlow. Русский интерфейс отсутствует. Отчеты могут быть экспортированы в следующие форматы: PDF, CSV, HTML. Присутствует возможность запуска отчетов за большие промежутки времени.

Оповещение и приоритизация.

Результаты тестирования решений по критериям блока «Оповещение и приоритизация» представлены в табл. 6.

		PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analitycs**	**McAfee ESM**
Критерии	**Параметры**	**Оценки**				
Оповещение	Возможности по оповещению о возникающих событиях	1	2	2	2	2
	Возможность кастомизации параметров оповещения	0	1	2	2	2
	Возможные способы	1	2	2	2	2
	Гибкость настройки	1	2	2	2	1
Приоритизация	Возможность автоматического определения серьезности	1	2	2	2	2

	выявленного события					
	Возможность кастомизации	1	0	2	2	1
	Возможность объединения событий по параметрам инцидента	0	2	2	2	2

Табл. 6. Оповещение и приоритизация.

PT MaxPatrol SIEM. Отсутствует применение активного воздействия и реакции на оповещение. Невозможно провести кастомизацию параметров оповещения. В качестве возможных способов оповещения доступен только SMTP. Низкая гибкость настройки. Кастомизация приоритизации событий

доступна при использовании SDK. Отсутствует возможность объединения событий по параметрам инцидента.

IBM QRadar. Применение активного воздействия и реакции на оповещение доступно только для ряда продуктов IBM. При кастомизации параметров оповещения невозможно использовать переменные. Доступны следующие способы оповещения: E-mail, Syslog, Console. Отсутствует кастомизация приоритизации событий.

HP ArcSight. Доступно применение активного воздействия, реакции на оповещение (нативные процедуры для некоторых продуктов HP, в других продуктах это возможно посредством выполнения скриптов) и кастомизации параметров оповещения. Возможные способы оповещения: E-mail, SMS, консоль, выполнение команд в ОС хоста менеджера или коннектора. Есть возможность кастомизации и приоритизации событий.

RSA Security Analytics. Доступно применение активного воздействия и реакции на оповещение, а также кастомизации параметров оповещения. Возможные способы оповещения: SMTP, SNMP. Есть возможность кастомизации приоритизации событий.

McAfee ESM. Доступны способы оповещения начиная с оповещения по электронной почте и запуска внешней команды (скрипта) на указанном устройстве и заканчивая полноценной интеграцией на уровне API с продуктами McAfee Network Security Platform (IPS/IDS решение), всеми агентскими продуктами McAfee (от антивируса до защиты БД) на уровне запуска специализированных команд и переназначения политик на агенте, а также со сканером уязвимости McAfee Vulnerability Manager (запуск сканирования напрямую из консоли SIEM).

Общие настройки и предустановленный функционал.

Результаты тестирования решений по критериям блока «Общие настройки и предустановленный функционал» представлены в табл. 7.

		PT SIEM	IBM QRadar	HP ArcSight	RSA Security Analitycs	McAfee ESM
Критерии	**Параметры**	**Оценки**				
Оповещение	Поддержка интеграции с LDAP, AD для обеспечения аутентификации	0	2	2	2	2
	Наличие Workflow и функций системы управления инцидентами	1	1	2	2	2
	Оддержка интеграции с третьими Workflow-системами	0	1	2	1	2
	Возможности по разграничению доступа	2	2	2	2	2
	Возможности по разграничению доступа	2	2	2	2	2
	Поддержка интеграции с третьими Workflow-системами	0	1	2	1	2
	Возможности по разграничению	2	2	2	2	2

	доступа					
	Возможность настройки парольной политики	0	1	2	2	2
	Защита канала при взаимодействии компонентов системы	2	2	2	2	1
	Наличие предустановленных правил корреляции	1	2	2	2	2
Приоритизаци	Наличие предустановленных графических панелей (Dashboards)	1	2	2	2	2
	Наличие предустановленных отчетов	2	2	2	2	2

Табл. 7. Общие настройки и предустановленный функционал.

PT MaxPatrol SIEM. Отсутствует интеграция с LDAP и AD для обеспечения аутентификации, но данный функционал вендор обещает реализовать в 12-м релизе своей платформы. Для разграничения доступа между пользователями доступна ролевая модель. Присутствуют встроенные корреляционные правила, графические панели и отчёты. Реализован базовый функционал управления инцидентами.

IBM QRadar. Поддерживается аутентификация пользователей в различных LDAP. Существует встроенный функционал Workflow.

Поддерживается интеграция со сторонними Workflow-системами (ограниченная по поддерживаемым операциям). Встроено большое количество предустановленных корреляционных ресурсов, отчётов и графических панелей.

HP ArcSight. Поддерживается аутентификация пользователей в различных LDAP. Реализован встроенный функционал Workflow с гибкими возможностями кастомизации. Поддерживается интеграция со сторонними Workflow-системами. Встроено большое количество предустановленных корреляционных ресурсов, отчётов и графических панелей.

RSA Security Analytics. Поддерживается аутентификация пользователей в различных LDAP. Существует встроенный функционал Workflow, поддерживается интеграция со сторонними системами. Встроено большое количество предустановленных корреляционных ресурсов, отчётов и графических панелей.

McAfee ESM. Поддерживается аутентификация пользователей в различных LDAP. Осуществляется интеграция с Remedy на уровне подключения по API; любая внешняя система уровня Service Desk интегрируется на уровне шаблонных сообщений SMTP для автоматического заведения инцидентов. Встроено большое количество предустановленных корреляционных ресурсов, отчётов и графических панелей.

Масштабирование, отказоустойчивость и хранение.

Результаты тестирования решений по критериям блока «Масштабирование, отказоустойчивость и хранение» представлены в табл. 8.

		PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analitycs**	**McAfee ESM**
Критерии	**Параметры**	**Оценки**				
Масштабируемость	Ограничения по количеству обрабатываемых событий в секунду	1	2	2	1	1
	Возможность распределения задач сбора и обработки событий по компонентам системы	2	2	2	2	2
	Возможность установки компонентов в различных форм-факторах	2	2	2	2	2
	Возможность увеличения мощности ядра системы	2	2	2	2	2

	Возможности по разграничению доступа	2	2	2	2	2
	Возможность развития системы за счет добавления дополнительных компонентов	2	2	2	2	2
	Возможности по резервированию ядра системы	0	2	2	2	2
	Возможности по резервированию компонентов сбора событий	0	2	2	2	2
	Обеспечение непрерывности сбора событий	0	2	2	1	1
	Автоматическое резервирование	0	2	2	0	2

	конфигурации системы					
Приоритизаци	Возможность восстановления конфигурации после сбоев	0	2	2	1	2
	Автоматическое резервирование базы данных	0	2	2	0	2
	Возможность восстановления базы данных после сбоев	0	2	2	0	2
Храднение	Эффективность хранения (сжатие данных)	1	2	2	1	2
	Возможность подключения внешних массивов для хранения архивных данных	1	2	2	2	2

Табл. 8. Масштабирование, отказоустойчивость и хранение.

PT MaxPatrol SIEM. Ограничением по количеству обрабатываемых событий в секунду является порог в 30 000 (максимальная инсталляция, по информации от вендора). Отсутствует возможность резервирования компонентов системы и реализации отказоустойчивой конфигурации. Хранение событий осуществляется в исходном и нормализованном виде.

Осуществляется сжатие данных до 30%. Для хранения событий используется MongoDB. Существует возможность интеграции с внешними массивами для хранения архивных данных.

IBM QRadar. Ограничением по количеству обрабатываемых событий в секунду является порог в 1 200 000 (максимальная инсталляция, по информации от вендора). Есть возможность реализации конфигурации High Availability. Осуществляется резервирование всех компонентов системы, вплоть до ядра. Сжатие данных при хранении происходит в соотношении 1 к 10. Для хранения событий используются Ariel.

HP ArcSight. Ограничением по количеству обрабатываемых событий в секунду является порог в 1 500 000 (максимальная инсталляция, по информации от вендора). Есть возможность реализации конфигурации High Availability. Осуществляется резервирование всех компонентов системы, вплоть до ядра. Сжатие данных при хранении происходит в соотношении 1 к

10. Для хранения событий используются CORR-Engine.

RSA Security Analytics. Ограничением по количеству обрабатываемых событий в секунду является порог в 20 000 (максимальная инсталляция, по информации от вендора). Есть возможность реализации конфигурации High Availability. Осуществляется резервирование всех компонентов системы, вплоть до ядра. Сжатие данных при хранении происходит в соотношении 1 к

10. Для хранения событий используется RAW/Meta и в случае с Warehouse –

McAfee ESM. Ограничением по количеству обрабатываемых событий

в секунду является порог в 300 000 (максимальная инсталляция, по информации от вендора). Возможность увеличения мощности ядра и компонентов системы доступна для виртуальных комплексов. В случае ПАК требуется приобретение новой платформы. Есть возможность реализации конфигурации High Availability. Осуществляется резервирование всех компонентов системы, вплоть до ядра. Для хранения событий используется собственная внутренняя база данных.

Результаты тестирования по оставшимся блокам приведены в табл. 9.

		PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analitycs**	**McAfee ESM**
Критерии	**Параметры**	**Оценки**				

Мониторинг компонентов системы и внутренний аудит	Доступность ядра системы	2	2	2	2	2
	Доступность компонентов сбора событий	2	2	2	2	2
Удобство использования	Доступность источников событий	2	2	2	2	2
Наличие	Внутренний аудит	0	2	2	0	2

сертификатов	системы					
соответствия ФСТЭК	Централизованное управление компонентами системы из единой консоли	2	2	2	2	2
	Автоматическое обновление набора предустановленных правил и отчетов	1	2	0	2	2
	Качество поддержки производителя	1	2	2	1	2
	Замена вышедших из строя компонентов	1	2	2	1	1
	Наличие сертификатов НДВ 4 и ТУ	1	1	1	2	2
	Управление уязвимостями	2	2	0	2	2
Приоритизаци	Управление рисками	0	2	0	0	2
	Обнаружение аномальных действий пользователей	0	2	2	2	2
	Мониторинг действий пользователей	2	0	2	2	2
Дополнительные	Расследование	2	2	1	2	2

модули системы	инцидентов					
	Репутационные сервисы	0	2	2	2	2

Табл. 9. Результаты тестирования по оставшимся блокам.

Выводы по второй главе.

Итак, по результатам тестирования решений мы получили оценки, которые представлены в табл. 10 и 11.

	PT SIEM	**IBM QRadar**	**HP ArcSight**	**RSA Security Analytics**	**McAfee ESM**
Название блока	**Оценки**				
Поддержка источников событий	3,5	4,3	3,8	3,5	3,5
Сбор событий	3,4	5,6	6,5	5,6	4,7
Корреляция	5,0	7,5	7,5	5,5	6,8

Поиск данных и аналитика	6,2	7,3	8,0	7,3	7,3
Визуализация	2,2	2,3	3,6	2,2	3,2
Отчетность	2,5	5,0	5,0	5,0	5,0
Оповещение	1,2	2,7	3,0	3,0	2,7
Приоритизация	1,3	3,0	4,0	4,0	4,0
Общие настройки	1,0	1,8	2,3	2,2	2,3
Предустановленный функционал	3,3	5,0	5,0	5,0	5,0
Мониторинг компонентов системы и внутренний аудит	2,1	2,7	2,7	2,1	2,7
Масштабируемость	5,6	5,9	5,9	5,6	5,9
Отказоустойчивость	0,0	4,4	4,4	1,8	4,4
Хранение	1,6	3,3	3,3	2,3	3,3
Удобство использования	5,3	8,5	6,5	6,3	7,5
Наличие сертификатов соответствия ФСТЭК	0,8	0,8	0,8	1,6	1,6
Дополнительные модули системы	2,3	3,2	2,4	3,5	4,0
Итого:	47,4	73,2	74,7	66,5	73,8

Табл. 10. Результаты для образовательных организаций СПО.

HP ArcSight раньше других продуктов нашего обзора появился на рынке SIEM-решений России, потому успел завоевать немало поклонников и противников. Продукт HP поддерживает широкий перечень разнообразных

источников событий, выполняя нормализацию на очень высоком уровне. Он имеет наиболее широкие возможности тонкой отладки, кастомизации и действительно мощный корреляционный функционал. На ArcSight уже построено множество SOC в различных сферах деятельности. Платой за мощь и гибкость являются сложность первичного изучения продукта, его высокая стоимость и небольшое количество квалифицированных российских специалистов, умеющих работать с решением.

IBM QRadar оказался на российском рынке немного позже и на тот момент явно отставал от ArcSight по корреляционному функционалу, но зато имел гораздо более простой и понятный интерфейс. За это время его

корреляционные возможности значительно возросли, но пока не дотягивают до возможностей ArcSight. У продукта появилось много нового, передового функционала, благодаря которому он оказался на лидирующих позициях отчёта Гартнера. QRadar имеет отличные возможности горизонтальной масштабируемости, присутствует функционал анализа сетевых потоков, а также возможность интеграции с множеством дополнительных модулей от IBM. Возможности тонкой отладки и кастомизации ограничены.

В McAfee ESM в первую очередь благодаря единому API реализована наиболее тесная интеграция со всей продуктовой линейкой производителя,

что позволяет организовать 2-стороннюю связь практически со всей инфраструктурой безопасности (построенной на McAfee). В продукте реализован довольно удобный и понятный web-интерфейс, позволяющий

быстро изменять представления данных при расследовании. Корреляционный функционал, реализованный в компоненте ERC, не отличается высокой гибкостью настройки. Существует также ACE – отдельное устройство, поддерживающее как real-time, так и историческую корреляцию и реализующее risk-based корреляцию. Возможности тонкой отладки и кастомизации ограничены.

Продукт RSA Security Analytics появился на российском рынке SIEM сравнительно недавно, он вобрал в себя опыт прошлого SIEM вендора (EnVision) и возможности приобретённого ими NetWitness. Основная концепция продукта основана на более тесном включении информации о сетевых потоках в стандартную логику работы SIEM. Продукт имеет удобный и понятный web-интерфейс, что облегчает его изучение. Корреляционный функционал ограничен, существует дополнительный корреляционный модуль. Продукт позиционируется вендором как решение для больших инсталляций, этому способствуют его богатая модульная структура и интеграция с высокоуровневыми продуктами RSA (Archer,

ECAT, RSA Security Operations Management). Возможности тонкой отладки и кастомизации ограничены.

PT SIEM: российские вендоры только начинают свой путь на рынке SIEM-решений, и этот продукт имеет все шансы прочно закрепиться на внутреннем рынке благодаря позициям вендора и тенденциям к импортозамещению. Продукт активно развивается, и ещё слишком рано сравнивать его с гигантами индустрии, но несмотря на это, даже текущая версия выглядит жизнеспособной. В ней уже реализована большая часть функционала современных SIEM-решений. Основной продукт вендора – хорошо зарекомендовавший себя MaxPatrol, следовательно, интеграция SIEM-системы с функционалом управления уязвимостями и аудита систем максимальна.

Исходя из результатов тестирования, я хочу сделать следующие выводы: для образовательной организации СПО наиболее оптимальными являются решения от компаний McAfee и IBM. Они подходят для тонкой настройкой системы и обладают специфической гибкость платформы для реализации основных функций SOC.

Заключение

Использование современных технологий управления информацией на основе связанных между собой систем управления базами данных, позволяет осуществлять подобные операции в автоматическом режиме. Вмешательство человека требуется только на этапах ввода исходной информации и формирования запроса на предоставление информации. В настоящее время,

невозможно построить универсальную систему информационной безопасности, такую как SOC, которая вмещала бы в себя все существующие на сегодняшний день возможности и функции управления информацией. В этом случае правильнее использовать лишь SIEM систему, и на её базе организовать единое операционное пространство, для способности интегрировать различные программные компоненты и виды данных. К рассматриваемым видам данных следует отнести: бумажные документы, файлы данных различных форматов, электронные документы, аудио и видео материалы, базы данных, приложения для работы с электронными документами, информационные ресурсы Интернет и другие. В частности, всякая информационная система, для которой определены механизмы автоматического входа-выхода, также может рассматриваться как информационный ресурс. Каждое учебное заведение имеет свои особенности

и механизмы управления, которые необходимо учитывать при создании системы.

В ходе данной работы рассмотрены основные нормативные документы, регулирующие правовые отношения в области защиты информации, приведены сведения о возможных угрозах безопасности информационной системе, в том числе подробно приведена и рассмотрена характеристика угроз несанкционированного доступа. При рассмотрении угроз, особое внимание уделялось классификации нарушителей безопасности, поскольку они выполняют доминирующую роль в нарушении безопасности информационной системе.

Особое внимание уделено основным компонентам для построения защищённой информационной системы. Подробно рассмотрены организация хранения информации в базе данных, классификация программного обеспечения и основные средства защиты локальной сети, приведены организационные меры защиты.

Единого рецепта, обеспечивающего 100% гарантии сохранности данных и надёжной работы сети, не существует. Однако создание комплексной, продуманной концепции безопасности, учитывающей специфику задач конкретной организации, поможет свести риск потери ценнейшей информации к минимуму.

Практически любую информацию можно защитить, если пользователь пожелает это сделать, сохранив ее таким образом. В скором будущем компьютеры заменят многие привычные сейчас вещи, следовательно, нам придется доверить компьютеру самое сокровенное, которое человек никогда

в жизни не доверит другому человеку, поэтому потребуется более надежная защита информации, такая, что тайны человека смогут лишь узнать, в крайнем случае, после его смерти. Человечество надеется, что компьютер станет другом, которому можно будет сказать все, зная, что он никогда сам не раскроет их тайны.

Обеспечение информационной безопасности достигается только при комплексном использовании всех средств защиты информации -

организационные, физические, социально-психологические мероприятия и программном - технические средства защиты. Исходя из проделанной работы можно сделать вывод, что программные средства защиты информации играют большую роль в обеспечении информационной безопасности образовательной организации.

Список использованной литературы

1. Административное право /под ред. Л.Л. Попова. М.: Юристъ - 703 с.

2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

3. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник/Под ред. Б.Н. Топорнина. СПб.: Издательство "Юридический центр Пресс", 2001. С. 436-438.

4. Белов Е.Б. Основы информационной безопасности. Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. -М.: Горячая линия - Телеком, 2006. - 544с

5. Бекетов Н. Информационная безопасность развития государства // Информационные ресурсы России, № 6, 2004. -С.: 32-35;

6. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.

7. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации СПб, Питер 2002- 464 с.

8. Галатенко В.А. Стандарты информационной безопасности: курс лекций. Учебное пособие. - 2-ое издание. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2009. - 264 с.

9. Гаврилов Э.П. Коммерческая тайна и результаты интеллектуальной деятельности // Патенты и лицензии. 2002. N 4. С.19-23

10. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с

11. Городов О.А. Информация как объект гражданского права //Правоведение. 2001. N 5. С.80 – 82

12. Гражданское право /под ред. Е.А.Суханова. М.: Волтерс Клувер, 2004 - 734 с.

13. Дозорцев В.А. Интеллектуальные права. Понятие. Система. Задачи кодификации. М.: НОРМА, 2003. - 400 с.

14. Дозорцев В.А. Понятие исключительного права // Юридический мир. 2000. N 3. С.4-11; N 6. С.25-35.

15. Доктрина информационной безопасности Российской Федерации утверждена Президентом РФ 9 сентября 2000 г. N Пр-1895 (РГ, 2000, N 187)

16. Даль В. Толковый словарь живого великорусского языка. Т. 1. М., 1989. С. 67.

17. Домарев В.В. Энциклопедия безопасности информационных технологий. Методология создания систем защиты информации. Киев.: ООО "ТИД "ДС", 2001

18. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.

19. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ, 2013. - 239 с.

20. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография. / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ, 2015. - 239 с.

21. Запечинков, С.В. Информационная безопасность открытых систем в 2-х томах т.1 / С.В. Запечинков. - М.: ГЛТ, 2006. - 536 с.

22. Запечинков, С.В. Информационная безопасность открытых систем в 2-х томах т.2 / С.В. Запечинков. - М.: ГЛТ, 2008. - 558 с.

23. 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, 2006. - 536 с.

24. 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, 2008. - 558 с.

25. Запечников, С.В. Информационная безопасность открытых систем. Том 1. Угрозы, уязвимости, атаки и подходы к защите: Учебник для вузов. /

С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ , 2006. - 536 с.

26. Запечников, С.В. Информационная безопасность открытых систем. Том 2. Средства защиты в сетях: Учебник для вузов. / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ , 2008. - 558 с.

27. Зверева Е.А. Информация как объект неимущественных гражданских прав //Право и экономика. 2003. N 9. С.28-33

28. Информатика /под ред. С.В.Симоновича. СПб, Питер 2001- 400 с.

29. Каймин В.А. Информатика и дистанционное образование - М.: НОРМА-ИНФРА-М, 2002 - 432 с.

30. Каймин В.А. Информатика. М.: ИНФРА-М, 2002 - 328 с.

31. Кирмайер М. Информационные технологии. СПб.: Питер, 2003 - 443 с.

32. Копылов В.А. Информационное право Российской Федерации. М.: Инфра-М, 2006 - 400 с.

33. Конотопов, М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2013. - 136 с.

34. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. - М .: Академия, 2006. - 256 с.

35. Лапчик М.П. Методика преподавания информатики: учеб. Пособие для студ. Пед. Вузов. /М.П. Лапчик, И.Р. Семакин, Е.К. Хеннер; под общей редакцией М.П. Лапчика. - М.: Издательский центр Академия, 2001. - 624

с.Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. - М.: ГЛТ, 2004. - 280 с.

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

С Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М.: Флинта, 2013. - 448 с.

- Моисеев А.М. Проблемы и пути совершенствования внутришкольного управления. Пособие для руководителей образовательных учреждений. Тамбов: ТОИПКРО. 2002. 331 с.

- Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

- Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

- Педагогика /под ред. А.А. Радугина. М.: Центр, 2001 - 272 с.

- Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации. М.Финансы и статистика, 2002 - 512 с.

- Роберт И. Современные информационные технологии в образовании: дидактические проблемы; перспективы использования.- М: Школа-Пресс, 2001 -292 с.

- Рогаткин Д.В. Службы примирения в системе школьного самоуправления // Вестник восстановительной юстиции». 2002. № 4. С. 12-30.

- Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. Защита информации - компьютерных системах и сетях. М: "Радио и связь", 1999 – 178 с.

Селевко Г.К. Современные образовательные технологии.- М: Народное образование, 2002 -255 с.

Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И., Основы организационного обеспечения информационной безопасности объектов информатизации // Гелиос АРВ, 2008 г., 192 с

Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010. - 277 с.

Семененко, В.А. Информационная безопасность / В.А. Семененко. -

М.: МГИУ, 2011. - 277 с.

- Тихонов В.А., Райх В.В., Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты // Гелиос АРВ, 2009г., 528 с

- Хорев П.Б. Методы и средства защиты информации в компьютерных системах:Учеб.пособие для студ. высш. учеб. заведений/Павел Борисович Хорев.–М.:Издательский центр «Академия», 2005.–256с.
- Чашников Л.А. Современные модели информационно-

аналитического обеспечения школьного управления // Вопросы психологии. 1993. № 9. С.36-57. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» //СПС Гарант

Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2010. - 336 с.

Чупрасова В.И. Современные технологии в образовании. Владивосток: Издательский дом «ДВР», 2004 - 154 с.

Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

Шаньгин, В.Ф. Информационная безопасность и защита информации - В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с

Шубинский М.И. Информационная безопасность для работников бюджетной сферы: учеб. пособие / НИУ ИТМО. - СПб., 2012.

Шафеева Е.Ю. Шубинский М.И. Основы безопасности жизне деятельности в сети Интернет (ОБЖИ): метод, пособие / МПСС. СПб., 2010.

Ярочкин В.И., Информационная безопасность: учебник для студентов вузов// -М.: Академический проект; Гаудеамус, 2-е изд., 2009 г., 544 с

Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 с.

Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. - М.: Академический проект, 2008. - 544 с.

https://dic.academic.ru/dic.nsf/ruwiki/746671

https://docviewer.yandex.ru/view/287874887

- http://www.jetinfo.ru/stati/sravnenie-siem-reshenij-dlya-postroeniya-soc
- http://www.itsec.ru/articles2/Inf_security/novye-podhody-pri-postroenii-soc-(security-operations-center)
- http://www.jetinfo.ru/stati/samyj-bezopasnyj-soc
- https://www.securitylab.ru/blog/personal/Business_without_danger/157117.php
- https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/
- https://searchinform.ru/products/siem/sravnenie-siem-sistem/
- https://www.securitylab.ru/blog/personal/Morning/325014.php
- http://siem.su/compare_SIEM_systems.php