ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ

«**КОЛЛЕДЖ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ**

имени Героя Советского Союза М.Ф. Панова»

**КУРСОВАЯ РАБОТА**

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

По профессиональному модулю: ПМ.01. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

По междисциплинарному курсу: МДК 01.04. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Тема работы: «Обеспечение безопасности автоматизированной информационной системы организации»

Группа СОБ-213/19

|  |  |
| --- | --- |
| Студент Бурмистрова В.К. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ФИО | подпись  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Оценка |
| Преподаватель Грибаков С.Л. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ФИО | подпись |

Москва 2021

**СОДЕРЖАНИЕ**

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лит

Лист

Листов

2

43

ГБПОУ КСТ

СОБ-213/19

Обеспечение безопасности автоматизированной информационной системы организации

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Бурмистрова В.К.

Разраб.

Грибаков С.Л.

Пров.

Т. контр.

Н. контр.

Утв.

[ВВЕДЕНИЕ 4](#_Toc71897670)

[1. ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ 6](#_Toc71897671)

[2. ТРИ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ 8](#_Toc71897672)

[2.1. Неблагоприятная для предприятия экономическая политика государства. 8](#_Toc71897673)

[2.2. Действия иных хозяйствующих субъектов. 8](#_Toc71897674)

[2.3. Кризисные явления в мировой экономике. 11](#_Toc71897675)

[3. ИЗ ЧЕГО СОСТОИТ СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 12](#_Toc71897676)

[3.1. Система обеспечения информационной безопасности организации: комплексный подход к построению 12](#_Toc71897677)

[3.2. Рекомендаций разработчикам системы информационной безопасности 15](#_Toc71897678)

[3.3. Пять принципов системы обеспечения информационной безопасности организации 16](#_Toc71897679)

[4. СЛУЖБА БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ 18](#_Toc71897680)

[4.1 Чем занимается служба безопасности в организации 18](#_Toc71897681)

[5. КАКИЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ХОРОШИ 22](#_Toc71897682)

[6. РЕКОМЕНДАЦИИ ОТ ICC ПО ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ 29](#_Toc71897683)

[7. АНТИВИРУСНАЯ ЗАЩИТА KASPERSKY ENDPOINT SECURITY 11 30](#_Toc71897684)

[7.1. Kaspersky Anti-Spam. Защита от спама 30](#_Toc71897685)

[8. VIPNET ENDPOINT PROTECTION 32](#_Toc71897686)

[8.1 Персональный межсетевой экран ViPNet EPP 32](#_Toc71897687)

[8.2. Контроль приложений с помощью ViPNet EPP 33](#_Toc71897688)

[8.4. Предотвращение вторжений с помощью ViPNet EPP 37](#_Toc71897689)

[8.5. Слежение за антивирусом с помощью ViPNet EPP 38](#_Toc71897690)

[ЗАКЛЮЧЕНИЕ 40](#_Toc71897691)

[СПИСОК ЛИТЕРАТУРЫ 41](#_Toc71897692)

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

3

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

# **ВВЕДЕНИЕ**

Конфиденциальная для бизнеса информация входит в сферу повышенного интереса конкурирующих компаний. Для недобросовестных конкурентов, коррупционеров и других злоумышленников особый интерес представляет информация о составе менеджмента предприятий, их статусе и деятельности фирмы. Доступ к конфиденциальной информации и ее изменение могут нанести существенный урон финансовому положению компании. При этом, информационная утечка может быть даже частичной. В некоторых случаях даже обеспечение хищения 1/5 конфиденциальной информации может иметь критические последствия для финансовой безопасности. Причиной утечки информации, если отсутствует должное обеспечение информационной безопасности организации, могут быть различные случайности, вызванные неопытностью сотрудников.

Использование информационных систем в работе организаций предполагает необходимость использования множества программных систем, каждая из которых может обладать определенными уязвимостями в области информационной безопасности.

Задачи менеджмента информационной безопасности в настоящее время являются актуальными, так как позволяют обеспечить эффективную структуру управления системой защиты информации, своевременно выявлять недостатки существующей технологии, принимать меры по их устранению.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

4

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Рост количества используемых программ снижает общий уровень защищенности системы. Анализ системы на наличие уязвимостей позволяет выявлять недостатки в системе защиты информации, своевременно устраняя их. Поиск уязвимостей проводится с использованием специальных программ-сканеров уязвимостей.

Цель данной работы: выяснить, как обеспечить безопасность автоматизированной информационной системы организации.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

4

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Для достижения поставленной цели, необходимо выполнить следующие задачи:

* Узнать, что такое информационная безопасность, как защитить информацию;
* Исследовать угрозы информационной безопасности организации;
* Определить из чего состоит система информационной безопасности;
* Определить принципы системы обеспечения информационной безопасности организации;
* Узнать, чем занимается служба безопасности в организации;
* Рассмотреть, какие методы и средства обеспечения информационной безопасности организации хороши.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

5

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

**ТЕОРИТИЧЕСКАЯ ЧАСТЬ**

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

6

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

# **ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ**

Информационная безопасностьпредполагает обеспечение защиты данных от хищений или изменений как случайного, так и умышленного характера. Система обеспечения информационной безопасности организации – эффективный инструмент защиты интересов собственников и пользователей информации. Следует отметить, что ущерб может быть нанесен не только несанкционированным доступом к информации. Он может быть получен в результате поломки коммуникационного или информационного оборудования. Особенно актуальна эффективная организация обеспечения безопасности информационных банковских систем и учреждений открытого типа (учебные, социальные и др.).

Для того чтобы наладить должное обеспечение защиты информации следует иметь четкое представление об основных понятиях, целях и роли информационной безопасности.

Термин «безопасность информации» описывает ситуацию, исключающую доступ для просмотра, модерации и уничтожения данных субъектами без наличия соответствующих прав. Это понятие включает обеспечение защиты от утечки и кражи информации с помощью современных технологий и инновационных устройств.

Защита информациивключает полный комплекс мер по обеспечении целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права.

Целостность – понятие, определяющее сохранность качества информации и ее свойств.

Конфиденциальность предполагает обеспечение секретности данных и доступа к определенной информации отдельным пользователям.

Доступность – качество информации, определяющее ее быстрое и точное нахождение конкретными пользователями.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

7

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Цель защиты информации – минимизация ущерба вследствие нарушения требований целостности, конфиденциальности и доступности.

# **ТРИ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ**

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

8

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

### **2.1.** Неблагоприятная для предприятия экономическая политика государства.

Регулирование экономики государством с помощью манипуляций (определение валютного курса, учетная ставка, таможенные тарифы и налоги) является причиной многих противоречий на предприятиях в сфере производства, финансов и коммерции.

Большую опасность для обеспечения безопасности информации предприятия несут административные обязательства выхода на рынок, что приводит к насильственному сужению товарно-денежных отношений, нарушению законов со стороны государства и ограничению деятельности предприятия. Часто государство преувеличивает свою компетентность в финансовой и коммерческой сфере деятельности предприятия и необоснованно вмешивается в пространство информации этих сфер, а также посягает на собственность предприятия в различных формах.

Серьезную угрозу для обеспечения безопасности информации предприятия несут политические действия, направленные на ограничение или прекращение экономических связей. Санкции в экономике вызывают у обеих сторон недоверие к дальнейшей деятельности и подрывают коммерческие взаимоотношения. Все это ведет к дестабилизации экономических отношений, и не только на уровне государства.

### **2.2.** Действия иных хозяйствующих субъектов.

В данном случае риск обеспечению безопасности информации несет нездоровая конкуренция. Нездоровая или недобросовестная конкуренция имеет несколько понятий и по нормам международного права разделяется на три вида:

* Когда деятельность одной коммерческой структуры пытаются представить потребителю под видом другой;
* Дискредитирование репутации коммерческого предприятия путем распространения ложной информации;
* Неправомерное и некорректное использование торговых обозначений, вводящих потребителя в заблуждение.

В западных странах существуют законодательные акты по ведению недобросовестной конкуренции, фирменным наименованиям, товарным обозначениям и препятствованию обеспечению безопасности информации, нарушение которых ведет к определенной юридической ответственности. Также к ответственности приводят следующие неправомерные действия:

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

9

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* Подкуп или переманивание потребителей со стороны конкурента;
* Порядок обеспечения информационной безопасности организации нарушается путем разглашения коммерческих тайн, а также выяснения информации с помощью шпионажа, подкупа;
* Установление неравноправных и дискредитирующих условий, влияющих на обеспечение безопасности информации;
* Тайное создание картелей, сговор во время торгов с предоставлением коммерческой информации;
* Создание условий, ограничивающих возможность обеспечения безопасности информации;
* Преднамеренное снижение цен для подавления конкуренции;
* Копирование товаров, рекламы, услуг и других форм коммерческой деятельности и информации конкурента.

Имеются и другие аспекты, выявляющие недобросовестную конкуренцию. К ним относится экономическое подавление, которое выражается в разных формах – шантаж персонала, руководителей, компрометирующая информация, парализация деятельности предприятия и срыв сделок с помощью медиаканалов, коррупционных связей в госорганах.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

10

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Коммерческий и промышленный шпионаж, подрывающий основы обеспечения информационной безопасности организации, также входит под правовую юридическую ответственность, поскольку он подразумевает незаконное завладение секретной информацией конкурента с целью извлечения личной выгоды.

Та информация, которая предоставляется для широких масс по легальным каналам, не дает руководству предприятия полного ответа на интересующие вопросы о конкурентах. Поэтому, многие крупные предприятия, даже считая действия шпионажа неэтичными и неправомерными, все равно прибегают к мерам, противодействующим обеспечению безопасности информации. Шпионы, работающие на конкурирующем предприятии, часто прибегают к таким действиям, как прямое предложение служащему о предоставлении секретной информации, кража, подкуп и другие разные уловки. Многие действия по подрыву обеспечения безопасности информации облегчаются за счет появления на рынке различных подслушивающих устройств и других современных технических разработок, которые позволяют максимально качественно осуществлять коммерческий и промышленный шпионаж.

Для многих служащих конкурентной компании сумма, предложенная за шпионаж, предоставление секретной информации и нарушение обеспечения безопасности информации, в несколько раз превышает их ежемесячный доход, что является очень соблазнительным для обычного сотрудника. Поэтому, можно считать, что подписка о неразглашении не является полной гарантией обеспечения безопасности коммерческой информации.

Следующей формой недобросовестной конкуренции, направленной на препятствование обеспечению безопасности информации, считается физическое подавление в виде посягательства на жизнь и здоровье служащего компании.  В эту категорию входит:

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

11

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* Организация разбойных нападений на производственные, складские помещения и офисы с целью ограбления;
* Уничтожение, порча имущества и материальных ценностей путем взрыва, поджога или разрушения;
* Захват сотрудников в заложники или физическое устранение.

### **2.3. Кризисные явления в мировой экономике.**

Кризисы имеют особенность перетекать из одной страны в другую, используя каналы внешних экономических связей. Они также наносят ущерб обеспечению безопасности информации. Это следует учесть, определяя методы и средства обеспечения информационной безопасности организации.

Поэтапное интегрирование России в международную экономику способствует зависимости коммерческих предприятий страны от различных процессов, происходящих в мировой экономике (падение и рост цен на энергоносители, структурная перестройка и другие факторы). По степени внедрения национальной экономики в мировую экономическую структуру усиливается ее подверженность внешним факторам. Поэтому, современное производство в стремлении к увеличению прибыли, улучшению деятельности путем модернизации, повышению уровня обеспечения безопасности информации, стабильности обязательно должно обращать внимание на динамику потребительского спроса, политику государства и центральных банков, развитие научно-технического прогресса, на отношение конкурентов, мировую политику и хозяйственную деятельность.

# **ИЗ ЧЕГО СОСТОИТ СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

12

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Система безопасности обеспечивается работой таких подразделений, как:

1. Компьютерная безопасность. Работа этого подразделения основана на принятии технологических и административных мер, которые обеспечивают качественную работу всех аппаратных компьютерных систем, что позволяет создать единый, целостный, доступный и конфиденциальный ресурс.
2. Безопасность данных - это защита информации от халатных, случайных, неавторизированных или умышленных разглашений данных или взлома системы.
3. Безопасное программное обеспечение - это целый комплекс прикладных и общецелевых программных средств, направленных на обеспечение безопасной работы всех систем и безопасную обработку данных.
4. Безопасность коммуникаций обеспечивается за счет аутентификации систем телекоммуникаций, предотвращающих доступность информации неавторизированным лицам, которая может быть выдана на телекоммуникационный запрос.

### **3.1.** Система обеспечения информационной безопасности организации: комплексный подход к построению

Система безопасности потенциальных и реальных угроз непостоянна, поскольку те могут появляться, исчезать, уменьшаться или нарастать. Все участники отношений в процессе обеспечения безопасности информации, будь то человек, государство, предприятие или регион, представляют собой многоцелевые сложные системы, для которых трудно определить уровень необходимой безопасности.

На основании этого система обеспечения информационной безопасности организации рассматривается как целый комплекс принятых управленческих решений, направленных на выявление и предотвращение внешних и внутренних угроз. Эффективность принятых мер основывается на определении таких факторов, как степень и характер угрозы, аналитическая оценка кризисной ситуации и рассматривание других неблагоприятных моментов, представляющих опасность для развития предприятия и достижения поставленных целей. Обеспечение информационной безопасности организации базируется на принятии таких мер, как:

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

13

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

1. Анализ потенциальных и реальных ситуаций, представляющих угрозу безопасности информации предприятия;
2. Оценка характера угроз безопасности информации;
3. Принятие и комплексное распределение мер для определения угрозы;
4. Реализация принятых мер по предотвращению угрозы.

Основная цель обеспечения комплексной системы безопасности информации для защиты предприятия, это:

* Создать благоприятные условия для нормального функционирования в условиях нестабильной среды;
* Обеспечить защиту собственной безопасности;
* Возможность на законную защиту собственных интересов от противоправных действий конкурентов;
* Обеспечить сотруднику сохранностью жизни и здоровья.
* Предотвращать возможность материального и финансового хищения, искажения, разглашения и утечки конфиденциальной информации, растраты, производственные нарушения, уничтожение имущества и обеспечить нормальную производственную деятельность.

Качественная безопасность информации для специалистов - это система мер, которая обеспечивает:

* Защиту от противоправных действий;

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

14

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* Соблюдение законов во избежание правового наказания и наложения санкций;
* Защиту от криминальных действий конкурентов;
* Защиту от недобросовестности сотрудников.

Эти меры применяются в следующих сферах:

* Производственной (для сбережения материальных ценностей);
* Коммерческой (для оценки партнерских отношений и правовой защиты личных интересов);
* Информационной (для определения ценности полученной информации, ее дальнейшего использования и передачи, как дополнительный способ от хищения);
* Для обеспечения предприятия квалифицированными кадрами.

Обеспечение безопасности информации любого коммерческого предприятия основывается на следующих критериях:

* Соблюдение конфиденциальности и защита интеллектуальной собственности;
* Предоставление физической охраны для персонала предприятия;
* Защита и сохранность имущественных ценностей.

При создавшейся за последние годы на отечественном рынке обстановке рассчитывать на качественную защиту личных и жизненно важных интересов можно только при условии:

* Организации процесса, ориентированного на лишение какой-либо возможности в получении конкурентом ценной информации о намерениях предприятия, о торговых и производственных возможностях, способствующих развитие и осуществление поставленных предприятием целей и задач;

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

15

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* Привлечение к процессу по защите и безопасности всего персонала, а не только службы безопасности.

### **3.2. Рекомендаций разработчикам системы информационной безопасности**

1. Все используемые средства для защиты должны быть доступными для пользователей и простыми для технического обслуживания.
2. Каждого пользователя нужно обеспечить минимальными привилегиями, необходимыми для выполнения конкретной работы.
3. Система защиты должна быть автономной.
4. Необходимо предусмотреть возможность отключения защитных механизмов в ситуациях, когда они являются помехой для выполнения работ.
5. Разработчики системы безопасности должны учитывать максимальную степень враждебности окружения, то есть предполагать самые наихудшие намерения со стороны злоумышленников и возможность обойти все защитные механизмы.
6. Наличие и место расположение защитных механизмов должно быть конфиденциальной информацией.

Организация обеспечения безопасности информационных банковских систем основывается на тех же принципах защиты и предполагает постоянную модернизацию защитных функций, поскольку эта сфера постоянно развивается и совершенствуется. Казалось бы, еще недавно созданные новые защитные системы со временем становятся уязвимыми и недейственными, вероятность их взлома с каждым годом возрастает.

### **3.3. Пять принципов системы обеспечения информационной безопасности организации**

Принцип комплексности**.** При создании защитных систем необходимо предполагать вероятность возникновения всех возможных угроз для каждой организации, включая каналы закрытого доступа и используемые для них средства защиты. Применение средств защиты должно совпадать с вероятными видами угроз и функционировать как комплексная система защиты, технически дополняя друг друга. Комплексные методы и средства обеспечения информационной безопасности организации являются сложной системой взаимосвязанных между собой процессов.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

16

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Принцип эшелонирования представляет собой порядок обеспечения информационной безопасности организации, при котором все рубежи защитной системы будут состоять из последовательно расположенных зон безопасности, самая важная из которых будет находиться внутри всей системы.

Принцип надежности (равнопрочности). Стандарт организации обеспечения информационной безопасности должен касаться всех зон безопасности. Все они должны быть равнопрочными, то есть иметь одинаковую степень надежной защиты с вероятностью реальной угрозы.

Принцип разумной достаточности предполагает разумное применение защитных средств с приемлемым уровнем безопасности без фанатизма создания абсолютной защиты. Обеспечение организации высокоэффективной защитной системой предполагает большие материальные затраты, поэтому к выбору систем безопасности нужно подходить рационально. Стоимость защитной системы не должна превышать размер возможного ущерба и затраты на ее функционирование и обслуживание.

Принцип непрерывности. Работа всех систем безопасности должна быть круглосуточной и непрерывной.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

17

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

# **СЛУЖБА БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ**

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

18

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Служба безопасности – одна из важнейших структурных единиц любого современного предприятия, отвечающая за обеспечение безопасности проведения производственных и прочих внутренних процессов от несанкционированных посягательств.

Цель создания службы безопасности – обеспечение для предприятия условий защищенности от криминальной конкуренции – деятельности социальных организаций или физических лиц, направленной на получение односторонних преимуществ в бизнесе и основанной на нарушениях законодательства, деловой этики, наносящий экономический или иной ущерб цивилизованному бизнесу.

### **4.1 Чем занимается служба безопасности в организации**

В целом деятельность службы безопасности на предприятии может иметь одну из форм:

* Может входить в структуру организации и финансироваться за ее счет.
* Может существовать как отдельное коммерческое или государственное предприятие и работать в организации по договору с целью обеспечения безопасности отдельных объектов.

Служба безопасности, входящая в состав предприятия, может иметь форму многофункциональной структуры, обеспечивающей полную безопасность предприятия. Обычно, такая форма службы безопасности присуща крупным финансовым компаниям со стабильной экономической ситуацией. Это инвестиционные фонды, коммерческие банки, финансово-промышленные группы - все, кто может использовать собственные технические средства и персонал.

Служба безопасности как отдельная коммерческая организация, которая предоставляет услуги в сфере безопасности и защиты, может оказывать как комплексные, так и отдельные услуги. Она может полностью обеспечить организацию системы охраны или выполнять конкретные задания: определять, где установлены подслушивающие устройства; сопровождать транзитные перевозки; предоставлять личную охрану и другие услуги. К этой категории можно отнести частные сыскные и охранные агентства и некоторые государственные организации.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

19

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Для многих предприятий намного выгоднее пользоваться услугами коммерческой службы безопасности, чем содержать собственную охранную структуру.

Основы обеспечения информационной безопасности организации базируются на таких функциональных направлениях, как:

1. Своевременная организация безопасности по предотвращению угроз для жизненно важных интересов организации со стороны криминальных лиц или конкурентов. В этом случае для обеспечения защиты используются такие методы информации, как деловая разведка и аналитическое прогнозирование ситуации.
2. Принятие мер по предотвращению внедрения агентуры и установки технических устройств с целью получения конфиденциальной информации и коммерческой тайны предприятия. Основными средствами защиты здесь являются строгий пропускной режим, бдительность охранной службы и применение технических защитных устройств.
3. Обеспечение личной охраны руководству и персоналу организации. Основными критериями для этого вида охраны являются организация предупреждающих мер, опыт и профессионализм охранника, системный подход к обеспечению безопасности.

На структуру и организацию системы безопасности оказывают влияние такие факторы, как:

* Масштабность и уровень производственной деятельности организации, количество служащих и возможности для технического развития;
* Позиция предприятия на рынке – темпы его развития в отрасли, динамика продаж и процентный охват рынка, зоны стратегического влияния, конкурентная способность товаров и услуг;
* Уровень финансовой рентабельности, платежеспособность, деловая активность и привлекательность для инвестиционных вложений;

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

20

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* Наличие объектов и субъектов для специальной охраны – обладатели коммерческой или государственной тайны, взрывоопасные и пожароопасные участки, экологически вредное производство;
* Присутствие криминальной среды.

**Служба безопасности может состоять из типового набора услуг:**

Первое направление – юридическая защита предпринимательской деятельности, которая представляет собой юридически грамотное оформление обязанностей, прав и условий для ведения деятельности (прав собственности на патент, лицензию, имущество, ведение бухгалтерской документации, регистрационных документов, соглашений, арендных договоров, уставов и другой документации). Реализация и внедрение данной защиты для безопасности предпринимательской деятельности очевидна, поскольку нормативно-правовая база в данных условиях нестабильна и требует определенной юридической защиты.

Второе направление – физическая безопасность участников предпринимательской деятельности. В данном случае участниками или субъектами предпринимательской деятельности могут быть не только предприниматели, но и используемые ими ресурсы – материальные, финансовые, информационные.

Безопасность интеллектуальных ресурсов также входит в эту категорию. Это обслуживающий персонал, работники предприятия, акционеры.

Третье направление – информационно-коммерческая безопасность, которая представляет собой защиту информационных ресурсов предпринимателя и его интеллектуальной собственности.

Четвертое направление – охрана и безопасность персонала и людей, работающих на предприятии. Это соблюдение техники безопасности, охраны труда, экологии, санитарии, деловых взаимоотношений, личной безопасности работников.

На основании данной информации можно сделать вывод, что универсального или идеального метода защиты на сегодняшний день не существует, хотя потребность в качественной безопасности очевидна, а в некоторых случаях – критически необходима.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

21

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

# **КАКИЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ХОРОШИ**

Для обеспечения защиты информации используются следующие методы:

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

22

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

1)Препятствие. Метод представляет собой использование физической силы с целью защиты информации от преступных действий злоумышленников с помощью запрета на доступ к информационным носителям и аппаратуре.

2)Управление доступом – метод, который основан на использовании регулирующих ресурсов автоматизированной системы, предотвращающих доступ к информационным носителям. Управление доступом осуществляется с помощью таких функций, как:

* Идентификация личности пользователя, работающего персонала и систем информационных ресурсов такими мерами, как присвоение каждому пользователю и объекту личного идентификатора;
* Аутентификация, которая устанавливает принадлежность субъекта или объекта к заявленному им идентификатору;
* Проверка соответствия полномочий, которая заключается в установлении точного времени суток, дня недели и ресурсов для проведения запланированных регламентом процедур;
* Доступ для проведения работ установленных регламентом и создание необходимых условий для их проведения;
* Регистрация в виде письменного протоколирования обращений к доступу защитных ресурсов;
* Реагирование на попытку несанкционированных действий в виде шумовой сигнализации, отключения, отказа в запросе и в задержке работ.

3) Маскировка – метод криптографического закрытия, защищающий доступ к информации в автоматизированной системе.

4) Регламентация – метод информационной защиты, при котором доступ к хранению и передаче данных при несанкционированном запросе сводится к минимуму.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

23

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

5) Принуждение – это метод, который вынуждает пользователей при доступе к закрытой информации соблюдать определенные правила. Нарушение установленного протокола приводит к штрафным санкциям, административной и уголовной ответственности.

6) Побуждение – метод, который основан на этических и моральных нормах, накладывающих запрет на использование запрещенной информации, и побуждает соблюдать установленные правила.

Все перечисленные методы защиты направленны на обеспечение максимальной безопасности всей информационной системы организации и осуществляются с помощью разных защитных механизмов, создание которых основано на таких средствах, как:

1. Физические средства защиты используются в качестве внешней охраны для наблюдения за территорией объекта и защиты автоматизированной информационной системы в виде специальных устройств.

Вместе с обычными механическими системами, для работы которого необходимо участие человека, параллельно внедряются и электронные полностью автоматизированные системы физической защиты. С помощью электронной системы проводится территориальная защита объекта, организовывается пропускной режим, охрана помещений, наблюдение, пожарная безопасность и сигнализационные устройства.

Самая элементарная система электронной защиты состоит из датчиков, сигналы которых обрабатываются микропроцессорами, электронных ключей, биометрических устройств для идентификации человека и других интеллектуальных систем.

Защита оборудования, входящего в общую автоматизированную систему информационной безопасности, и переносных устройств (магнитных лент или флешек) осуществляется с помощью таких механизмов, как:

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

24

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* Замковые системы (механические, радиоуправляемые, кодовые, с микропроцессором), которые устанавливаются на сейфы, двери, ставни, системные блоки и другие устройства;
* Микровыключатели, с помощью которых фиксируется открывание и закрывание окон и дверей;
* Инерционные датчики, которые используются в электросети, телефонных проводах, телекоммуникационных антеннах;
* Наклейки из специальной фольги приклеивают на приборы, документы, системные блоки, узлы, что служит для них защитой от выноса за территорию организации или помещения. Любая попытка выноса документов или устройств с защитной наклейкой через пропускные устройства будет оповещена сигналом тревоги.
* Металлические шкафы и специальные сейфы, служащие для установки отдельных устройств информационной автоматизированной системы – фалов-серверов, принтеров и переносных информационных носителей.

Доступ информации через электромагнитные каналы ограничивают с помощью экранизирующих и поглощающих устройств и материалов:

* В помещениях, где установлены элементы автоматизированной информационной системы. Для защиты проводится экранирование всех поверхностей в помещении – пола, стен и потолка с помощью металлизированных обоев, токопроводящей штукатурки и эмали, фольги, проволочной сетки, многослойных стальных или алюминиевых листов, специальной пластмассы, токопроводящего кирпича и других материалов.
* Оконные проемы закрывают шторами с металлической нитью или покрывают стекла токопроводящим составом;
* На все отверстия в помещениях устанавливают металлические сетки с системой заземления или соединяют с настенной экранировкой;

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

25

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* Вентиляционные каналы комплектуют с магнитными ловушками, блокирующими распространение радиоволн.

В качестве защиты для блоков и узлов автоматизированной системы применяют:

* Экранированный кабель, который можно монтировать между блоками, стояками, внутри и снаружи стен;
* Эластичные экранированные соединители или разъемы, сетевые фильтры для блокировки электромагнитных излучений;
* Провода, дроссели, наконечники, конденсаторы и другие устройства с помехоподавляющим действием;
* На трубах системы водопроводной и газовой сети устанавливают диэлектрические разделительные вставки, разрывающие электромагнитные цепи.

В местах ввода сети с переменным напряжением устанавливают электронные отслеживатели, контролирующие электропитание. При любых повреждениях шнура происходит кодирование и включение сигнала тревоги. Запись последующих событий происходит после активации телевизионной камеры.

Для выявления подслушивающих устройств наиболее эффективным считается обследование с помощью рентгена. Но, с точки зрения технических и организационных мероприятий, рентгеновское обследование самое затратное.

Использование различных шумовых генераторных устройств, защищающих информацию в компьютерах от хищения, методом снятия излучений с дисплея неблагоприятно воздействует на здоровье человека. В результате происходят такие нарушения, как облысение, головные боли, снижение аппетита, поэтому данный способ защиты используется на практике крайне редко.

2. Аппаратные средства защиты– это все виды электронных и электромеханических устройств, встроенных в блоки информационной автоматизированной системы, которые представлены как самостоятельные устройства, соединенные с этими блоками.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

26

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Основная их функция - это обеспечение внутренней защиты соединительных элементов и систем в вычислительной технике – периферийного оборудования, терминалов, линий связи, процессоров и других устройств.

Обеспечение безопасности информации с помощью аппаратных средств включает:

* Обеспечение запрета неавторизированного доступа удаленных пользователей и АИС (автоматизированная информационная система);
* Обеспечение надежной защиты файловых систем архивов и баз данных при отключениях или некорректной работе АИС;
* Обеспечение защиты программ и приложений.

Вышеперечисленные задачи обеспечения безопасности информации обеспечивают аппаратные средства и технологии контроля доступа (идентификация, регистрация, определение полномочий пользователя).

Обеспечение безопасности особо важной информации может осуществляться с использованием уникальных носителей с особыми свойствами, которые предотвращают считывание данных.

3. Программные средства защиты входят в состав ПО (программного обеспечения), АИС или являются элементами аппаратных систем защиты. Такие средства осуществляют обеспечение безопасности информации путем реализации логических и интеллектуальных защитных функций и относятся к наиболее популярным инструментам защиты. Это объясняется их доступной ценой, универсальностью, простотой внедрения и возможностью доработки под конкретную организацию или отдельного пользователя. В то же время, обеспечение безопасности информации с помощью ПО является наиболее уязвимым местом АИС организаций.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

27

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Программные защитные средства, способные решать следующие задачи по обеспечению безопасности информации:

* Обеспечение контроля входа в АИС и загрузки баз данных при помощи уникальных идентификаторов (логин, пароль, код и др.);
* Обеспечение ограничения доступа пользователей к определенным компонентам АИС и ее внешним ресурсам;
* Защита ПО, обеспечивающего выполнение процессов для определенного пользователя от посторонних субъектов;
* Обеспечение безопасности потоков конфиденциальных данных;
* Безопасность информации от воздействия вирусного ПО;
* Уничтожение остаточных данных конфиденциального характера в открытых после введения паролей файлах в оперативной памяти;
* Формирование протоколов об уничтожении и стирании остаточных конфиденциальных данных;
* Обеспечение целостности данных путем внедрения избыточной информации;
* Автоматическое обеспечение безопасности работы пользователей АИС на основе данных протоколирования информации с последующей подготовкой отчетов в регистрационном журнале системы.

Большинство современных ОС (операционных систем) содержат программные решения для обеспечения блокировки повторного доступа к информации. При отсутствии таких средств могут использоваться различные коммерческие ПО. Внедрение избыточных данных направлено на обеспечение контроля случайных ошибок. Это может реализовываться через использование контрольных сумм или обеспечение кодирования устойчивого к помехам.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

28

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Для обеспечения безопасности особо важной информации используется метод хранения данных с использованием системы сигнатур. В качестве сигнатуры может применяться система, включающая сочетание защитного байта с его размером, временем изменения и именем. При любом обращении к этому файлу система анализирует сочетание информации с оригиналом.

Необходимо уточнить, что надежное обеспечение безопасности информации возможно только при использовании шифрования данных.

# **РЕКОМЕНДАЦИИ ОТ ICC ПО ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ**

В современных условиях интеллектуальная собственность (ИС) имеет особую ценность не только для бизнеса, но и для всей государственной и международной экономики. Обеспечение защиты информации, торговых марок, авторских прав и других объектов ИС способствует успешному развитию и получению стабильных доходов. Все чаще внедряются технологии по использованию компаниями ИС других владельцев, которая включает весь цикл от разработки и производства продукта до его реализации, предоставления услуг и обеспечения работы технологических процессов.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

29

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Международная торговая палата (МТП) инициировала разработку рекомендаций по обеспечению безопасности ИС в рамках проекта «Бизнес в борьбе с контрафактом и пиратством» («Business Action to Stop Counterfeiting and Piracy» - «BASCAP»). Основываясь на опыте различных компаний, данные рекомендации предлагают практические мероприятия по оценке уровня безопасности информации, авторских прав и других объектов ИС, способствующие обеспечению защиты интеллектуальных прав. Внедрение таких рекомендаций способствует повышению эффективности преодоления рисков, которые связаны с контрафактом и пиратством.

Документ, разработанный МТП, направлен на обеспечение руководителей всевозможных направлений работы с ИС эффективным инструментом по разработке, внедрению и внутрикорпоративному использованию интеллектуальных прав. Он включает технологии формирования систем обеспечения взаимодействия с посредниками и другими субъектами, использующими разработки в сфере ИС. Большая часть рекомендаций включает описание существующих наработок в данной сфере с практическими примерами и советами по конкретным типам интеллектуальных прав.

**ПРАКТИЧЕСКАЯ ЧАСТЬ**

# **АНТИВИРУСНАЯ ЗАЩИТА KASPERSKY ENDPOINT SECURITY 11**

Антивирусная защита Kaspersky Endpoint Security, продукт "Лаборатории Касперского", для бизнеса применяется с целью защитить от червей и троянских программ, а также сложных атак с использованием ботнетов и лжеантивирусов, так же антивирус блокирует клавиатурных шпионов, рекламных программ, целевого фишинга, руткита и атак типа «человек посередине». Блокируется реклама и сбор данных, осуществляемый на посещаемых сайтах.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

30

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Так же данный продукт защищает сервер, администратор использует службы предоставления отчетности о работе программного обеспечения. Сюда входят отчеты о запрещенных программах, шифровании данных, работе компонента «контроля программ».

Благодаря функции контроля устройств, администратор определил доступ пользователей к установленным или подключенным устройствам к рабочей станции (жесткие диски, принтеры, веб-камеры). Это обеспечивает защиту от заражения при подключении внешних устройств и предотвращает потерю или утечку данных.

### **7.1. Kaspersky Anti-Spam. Защита от спама**

Злоумышленники часто используют спам в качестве основного канала распространения вредоносного программного обеспечения. Для борьбы со спамом предприятие, анализ защищенности которого проводится в данной курсовой работе, использует модуль Kaspersky Anti-Spam - продукт «Лаборатории Касперского».

С помощью данного предприятия корпоративная почта предприятия защищена от спама. Сервис быстро реагирует на новые спамерские рассылки и блокирует их, чтобы сотрудник не перешел по фишинговой ссылке и не занес в корпоративную сеть вирус.

Основа Kaspersky Anti-Spam - интеллектуальная технология SpamTest, которая обеспечивает: нечеткое (то есть срабатывающее и при неполном совпадении) сравнение проверяемого письма с образцами - письмами, ранее идентифицированными как спам; выявление в тексте письма фраз, характерных для спама; обнаружение картинок, ранее использованных в спамерских письмах. Кроме перечисленных выше критериев для идентификации спама используются и формальные параметры, в числе которых:

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

31

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* «черные» и «белые» списки, которые может вести пользователь,
* различные особенности заголовков почтового сообщения, характерные для спама, - например, признаки фальсификации адреса отправителя,
* приемы, применяемые спамерами для обмана почтовых фильтров, - случайные последовательности, замена и удвоение букв, текст белым по белому и другие,
* проверка не только текста самого письма, но и вложенных файлов в форматах plain text, HTML, MS Word, RTF и других.

При приеме почты Kaspersky Anti-Spam производит анализ поступающей корреспонденции. При обнаружении спама письмо помечается специальной меткой [!! SPAM] в поле «Тема» и помещается в папку «Удаленные». Письма, распознанные как не спам, ничем не помечаются и обрабатываются почтовой программой в соответствии с установленными правилами. Если программа не уверена, что письмо спамерское, то ставится метка [?? Probable Spam] и письмо помещается в папку "Входящие" для принятия пользователем окончательного решения. Кроме этого, программой используются еще два вида меток: [OBSCENE] - для писем с непристойным содержанием и [FORMAL] - для автоматически генерируемых писем, например, писем от почтовых роботов.

# **VIPNET ENDPOINT PROTECTION**

ViPNet EndPoint Protection - система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия. Основными модулями системы являются - персональный межсетевой экран, система обнаружения и предотвращения вторжений, а также контроль запуска приложений на основе чёрных и белых списков.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

32

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Решение сочетает:

* проверенные в действии технологии обнаружения вторжений, дополненные настраиваемым модулем предотвращения вторжений,
* модуль межсетевого экранирования с фильтрацией пакетов для непрерывной защиты рабочих станций от сетевых атак,
* модуль контроля приложений, который работает на базе черных и белых списков программного обеспечения. Он разграничивает доступ приложений к файлам, реестру ОС Windows, процессам и параметрам командной строки, предотвращает установку и запуск вредоносного программного обеспечения.

### **8.1 Персональный межсетевой экран ViPNet EPP**

Межсетевой экран ViPNet EndPoint Protection делает возможной фильтрацию входящего и исходящего трафика, идущего через систему. Межсетевой экран использует набор ''правил'' для проверки сетевых пакетов при их входе или выходе через сетевое соединение, он или позволяет прохождение трафика или блокирует его. Правила межсетевого экрана могут проверять одну или более характеристик пакетов, включая, но не ограничиваясь типом протокола, адресом хоста источника или назначения и портом источника или назначения.

Прежде всего, на предприятии активированы безопасные протоколы управления SSH и HTTPS. Небезопасные протоколы, такие как TELNET, HTTP и т.д., отключены.

Так же установлен определенный диапазон ip-адресов, который может получать сетевые пакеты. IP-адреса не входящие в данный диапазон, будут блокироваться межсетевым экраном. Данный инцидент будет зафиксирован в журнале.

### **8.2. Контроль приложений с помощью ViPNet EPP**

Контроль приложений ViPNet EPP Агент управляет установкой и запуском приложений на защищаемом узле, а также доступом приложение к объектам ОС Windows: файлам, реестру, процессам, параметрам командной строки. Контроль приложений ViPNet EPP Агент реализован модулем Application Control.

Сотрудникам компаний разрешается использование приложений из белого списка, такие как: внутреннее корпоративное приложение, браузер с ограниченным набором страниц и стандартные приложения windows. Остальные приложения входят в черный список. Доступ к таким приложениям строго ограничен, все попытки открыть или установить программное обеспечение из черного списка на компьютер сотрудника будут фиксироваться в журнале событий, и помечаться специальным маркером: .

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

33

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Само приложение будет заблокировано. Так же у сотрудников есть права на операции с файлом. У каждого сотрудника есть определенный уровень доступа к файлам. Некоторые файлы сотрудники могут только просматривать, а в некоторых файлах могут изменять содержимое и удалять их. На рисунке 3 проиллюстрирована система работы контроля приложений.



Рис. 1 Схема работы контроля приложений ViPNet EPP Агент

**8.3. Обнаружение и предотвращение вторжений с помощью ViPNet EPP**

Обнаружение и предотвращение вторжений ViPNet EPP Агент реализовано двумя модулями:

* HIDS — обеспечивает обнаружение вторжений сигнатурным и эвристическим методами.
* HIPS — обеспечивает блокирование сетевых вторжений, выявленных правилами обнаружения сетевых.

С целью обнаружения вторжений в непрерывном режиме модуль HIDS всегда активен. Остановить работу модуля HIDS невозможно

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

34

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Для обнаружения вторжений на предприятии используется сразу два метода: сигнатурный метод и эвристический. Делается это для того, чтобы получать полную информацию о выявленных событиях информационной безопасности.

Сигнатурный метод основывается на выявлении в потоке данных такой последовательности, которая определена как признак вторжения (атаки), например, сообщения об ошибках, записанные в журнал приложения.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

35

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Эвристический метод основывается на том, что заранее известно, какое поведение на защищаемом узле является стандартным. Поведение, отличающееся от стандартного, считается аномальным. Эвристический метод применяется на предприятии для выявления аномалий сетевого трафика и поведения пользователей.

Схема обнаружения событий информационной безопасности нашего предприятия на сетевом уровне изображена на рисунке 4.



Рис. 2 Схема обнаружения событий информационной безопасности на сетевом уровне

На первом этапе злоумышленник получил удаленный доступ к одному из защищаемых узлов и запустил троянскую программу. На втором этапе при анализе трафика с помощью правил обнаружения сетевых атак выявлена активность троянской программы — сетевая атака. 3 этап - событие сетевой атаки регистрируется в журналах событий ViPNet EPP Агент и ViPNet EPP Сервер.

Обнаружение событий информационной безопасности на локальном уровне можно проиллюстрировать схемой изображено на рисунке 5.



Рис. 3 Обнаружение событий информационной безопасности на локальном уровне

На первом этапе злоумышленник получил удаленный доступ к защищаемому узлу и изменил записи в реестре ОС Windows, затем на втором этапе с помощью декодера обнаружено изменение в реестре. Третий этап - с помощью правила анализа определено, какие именно изменения произошли в реестре: ключи, разделы, параметры. И 4 этап, заключающий - событие изменения реестра зарегистрируется в журналах событий ViPNet EPP Агент и ViPNet EPP Сервер.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

36

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

Таким образом, на основе правил HIDS ViPNet EPP Агент анализирует трафик, а также изменения на защищаемых узлах. При срабатывании правил HIDS регистрируется событие информационной безопасности, содержащее сведения о сетевой атаке или зафиксированном отклонении.

С помощью эвристического метода происходит постоянный мониторинг поведения системы защищаемого узла предприятия и сетевого трафика в режиме, приближенном к реальному времени. Поведение системы и ее элементов не должно отклоняться от ожидаемых значений, задаваемых в критериях обнаружения аномалий. Все случаи отклонения от ожидаемого поведения фиксируются в журналах.

### **8.4. Предотвращение вторжений с помощью ViPNet EPP**

Для блокировки сетевой активности, которая была выявлена правилами HIDS (правилами обнаружения сетевых атак) применяются правила предотвращения вторжений (правила HIPS). Как только срабатывает правило HIDS, также срабатывает соответствующее ему правило HIPS, которое создает блокирующий сетевой фильтр HIPS персонального межсетевого экрана ViPNet EPP Агент. Предотвращение вторжений на сетевом уровне нашего предприятия можно проиллюстрировано на рисунке 4.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

37

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата



Рис. 4 Предотвращение вторжений на сетевом уровне

Первый этап: Злоумышленник получил удаленный доступ к одному из защищаемых узлов и запустил троянскую программу. На втором этапе при анализе трафика с помощью правил обнаружения сетевых атак выявлена активность троянской программы — сетевая атака. На третьем этапе соответствующее правило предотвращения вторжений создает блокирующий сетевой фильтр. На 4 этапе персональный межсетевой экран ViPNet EPP Агент блокирует сетевую атаку (разрывает сетевое соединение) с помощью блокирующего сетевого фильтра. Заключающий этап, пятый - обытие сетевой атаки регистрируется в журналах событий ViPNet EPP Агент и ViPNet EPP Сервер.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

38

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

### **8.5. Слежение за антивирусом с помощью ViPNet EPP**

ViPNet EPP Агент может следить за работой антивирусов Kaspersky Endpoint Security 11 для Windows или Dr.Web Desktop Security Suite 11 для Windows.

Так как на нашем предприятии используется Kaspersky Endpoint Security 11, данная функция ViPNet EPP используется и выполняет следующие функции:

* каждые 30 секунд проверяется статус антивируса:
  1. если антивирус работает — режим работы персонального межсетевого экрана ViPNet EPP Агент не изменяется,
  2. если антивирус остановлен или отсутствует. В этом случае персональный межсетевой экран ViPNet EPP Агент переключается в режим «Полная блокировка трафика», весь сетевой трафик защищаемого узла, кроме трафика между ViPNet EPP Агент и ViPNet EPP Сервер, блокируется,
  3. при обнаружении работающего антивируса, персональный межсетевой экран ViPNet EPP Агент автоматически переключается в режим, установленный до включения функции слежения за антивирусом, при условии, что режим полной блокировки трафика не был установлен пользователем вручную,
* проверяются события журнала антивируса в разделе «Журналы приложений и служб» просмотра событий ОС Windows.

Если же антивирус обнаружил вредоносный объект, то персональный межсетевой экран ViPNet EPP Агент переключается в режим «Полная блокировка трафика» — весь сетевой трафик защищаемого узла, кроме трафика между ViPNet EPP Агент и ViPNet EPP Сервер, блокируется. Чтобы разблокировать трафик, необходимо переключить режим персонального межсетевого экрана вручную, или через назначение новой версии базы правил.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

39

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

# **ЗАКЛЮЧЕНИЕ**

В процессе курсовой работы были выполнены следующие задачи:

* Изучено, что такое информационная безопасность, как защитить информацию;
* Исследованы угрозы информационной безопасности организации;
* Определено из чего состоит система информационной безопасности, а также принципы системы обеспечения информационной безопасности организации;
* Изучено, что такое служба безопасности в организации;

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

40

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

* Обследовано, какие методы и средства обеспечения информационной безопасности организации хороши;
* Рассмотрены рекомендации от ICC по защите информации в организации.

Так же были рассмотрены программы для обеспечения информационной безопасности, такие как:

* Kaspersky Endpoint Security
* VIPNet Endpoint Protection

Цель курсовой работы достигнута.

# **СПИСОК ЛИТЕРАТУРЫ**

1.Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 c.

2.Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – М: Риор, 2017. - 400 c.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

41

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

3. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2019 -132 с.

4. Бубнов А.А. Техническая защита информации в объектах информаци-онной инфраструктуры: учеб. пособие для студ. учреждений сред. проф. образования/ А.А. Белов, В.Н. Пржегорлинский, К.Ю. Фомина – М.: Издательский центр «Академия», 2019. – 272с

5. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 c.

6. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 c.

7. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2017. - 159 c.

8. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 c.

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

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

11. Кузнецова, А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. - М.: Русайнс, 2017. - 64 c.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

42

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

12. Малюк, А.А. Информационная безопасность: концептуальные и мето-дологические основы защиты информации: А.А. Малюк. — М.: ГЛТ, 2016. — 280 c.

13. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 c.

14. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 c.

15. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

16. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Издательство «Горячая линия – Телеком» 2017 г. - 424 с.

17. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017. - 257 с.

18. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 c.

19. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 c.

20. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 c.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

42

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата

**СПИСОК ЭЛЕКТРОННЫХ РЕСУРСОВ**

1. <https://www.smart-soft.ru/blog/zaschita_informatsii_v_avtomatizirovannyh_sistemah/#:~:text>= ­— защита информации, объекты информации
2. <https://searchinform.ru/services/outsource-ib/zaschita-informatsii/v-informatsionnykh-sistemakh/v-avtomatizirovannykh-informatsionnykh-sistemakh/> — методы защиты информации
3. <https://userplay.info/help/instrukcii-manualy/?page=13>— инструкции и мануалы для работы с Secret Net Studio.
4. <https://www.securitycode.ru/products/secre-net-studio/> —— Код Безопасности. Secret Net Studio.
5. <https://www.securitycode.ru/upload/iblock/b4b/Руководство%20администратора.%20Настройка%20и%20эксплуатация.%20Локальная%20защита.pdf> — руководство администратора по Secret Net Studio.
6. <https://www.kaspersky.ru/small-to-medium-business-security/anti-spam> — Kaspersky Anti-Spam.
7. <https://infotecs.ru/downloads/documentacii/vipnet-endpoint-protection.html?arrFilter_93=2277291455&set_filter=Y> — документация   
   ViPNet EndPoint Protection.
8. <https://www.ixbt.com/soft/kaspersky-antispam.shtml> — обзор системы защиты от спама Kaspersky Anti-Spam.

Инв. № подп

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Лист

43

КР.10.02.05.2021.03.ПЗ

Лит

№ докум.

Изм.

Подп.

Дата