Учреждение образования

«Белорусский государственный технологический университет»

**Отчёт за практические занятия по предмету:**

Основы защиты информации

Выполнила:

Студентка 2 курса 1 группы ФИТ

Гринцевич Юлия Сергеевна

**2021г.**

# **Практическое занятие №1**

**Концепция национальной безопасности РБ**

**Цель работы:** Изучить концепцию национальной безопасности РБ.

**Ответы:**

1. **Что такое информационная безопасность?**

**Информационная безопасность** – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

**Информационная безопасность** – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

1. **Перечислить основные национальные интересы в информационной сфере?**

**Национальные интересы** - совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства, позволяющих обеспечивать конституционные права, свободы, высокое качество жизни граждан, независимость, территориальную целостность, суверенитет и устойчивое развитие Республики Беларусь;

Основные национальные интересы в информационной сфере:

* реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
* формирование и поступательное развитие информационного общества;
* равноправное участие Республики Беларусь в мировых информационных отношениях;
* преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
* эффективное информационное обеспечение государственной политики;
* обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

1. **Основные угрозы национальной безопасности, связанные с ИТ-сферой?**

**Источник угрозы национальной безопасности** - фактор или совокупность факторов, способных при определенных условиях привести к возникновению угрозы национальной безопасности;

**Угроза национальной безопасности -** потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь;

1)нарушение функционирования критически важных объектов информатизации;

2)деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

3)недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

4)снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;

1. **Назвать основные внутренние и внешние источники угроз национальной безопасности в информационной сфере?**

**Внутренние:**

1)зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах;

2)несоответствие качества национального контента мировому уровню;

3)недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

4)распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

5)рост преступности с использованием информационно-коммуникационных технологий;

6)недостаточная эффективность информационного обеспечения государственной политики;

7)несовершенство системы обеспечения безопасности критически важных объектов информатизации.

**Внешние:**

1)открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;

2)доминирование ведущих зарубежных государств в мировом информационном пространстве;

3)информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь;

4)нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

5)развитие технологий манипулирования информацией;

6)препятствование распространению национального контента Республики Беларусь за рубежом;

7)широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;

8)попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь;

1. **Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере?**

Нейтрализация внутренних источников угроз национальной безопасности обеспечивается путем принятия своевременных и действенных мер по устранению условий и предпосылок формирования политической и социально-экономической напряженности в обществе, практического воплощения принципов демократического социального правового государства, взаимной ответственности личности, общества и государства по обеспечению национальной безопасности.

**Вывод:** изучая концепцию национальной безопасности РБ были получены знания о национальной безопасности: основные положения и тенденции современного мира, национальные интересы, состояния национальной безопасности на современном этапе, основные угрозы, внутренние и внешние источники угроз национальной безопасности.

**Международные стандарты информационной безопасности**

**Ответы на вопросы:**

**2. Охарактеризуйте основные положения Оранжевой книги.**

В Оранжевой книге предложены три категории требований безопасности - политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены не посредственно на обеспечение безопасности информации, а два последних - на качество самих средств защиты.

1. Политика безопасности.

• Политика безопасности

Возможность осуществления субъектами доступа к объектам должна определяться на основе их идентификации и набора правил управления доступом.

• Метки

Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

2. Аудит.

• Идентификация и аутентификация

Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

• Регистрация и учет

Для определения степени ответственности пользователей за действия в системе все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективность его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

3. Корректность.

• Контроль корректности функционирования средств защиты

Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

•Непрерывность защиты

Все средства защиты (в т. ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

**4. Каковы основные положения Европейских критериев безопасности информационных технологий?**

Европейские критерии рассматривают следующие задачи средств информационной безопасности:

\*защита информации от несанкционированного доступа с целью обеспечение конфиденциальности;

\*обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;

\*обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

**5. Чем отличается «информационная система» и «продукт информационных технологий»?**

Система - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

Продукт – это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях. Угрозы безопасности системы носят вполне конкретный и реальный характер. Относительно угроз продукту можно лишь строить предположения. Разработчик может специфицировать условия, пригодные для функционирования продукта; дело покупателя обеспечить выполнение этих условий.

**7. Что такое Профиль защиты?**

**Профиль защиты** - это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, технологии разработки и квалификационному анализу.

**Профиль защиты** - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

**9. Опишите структуру общих критериев безопасности информационных технологий.**

Единые критерии регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов, используя схему из Федеральных критериев. Единые критерии предлагают достаточно сложный процесс разработки и квалификационного анализа ИТ-продуктов, требующий от потребителей и производителей составления и оформления весьма объемных и подробных нормативных документов.

Задачи защиты - базовое понятие Единых критериев, выражающее потребность потребителей ИТ-продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

Проект защиты - специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования.

Общие критерии состоят из 3-х частей:

1. Введение и общая модель.

2. Функциональные требования безопасности.

3. Требования доверия к безопасности.

**10. Опишите технологию применения общих критериев безопасности информационных технологий.**

Каталог функциональных классов:

• аудит,

• связь (подтверждение приёма/передачи информации),

• криптографическая поддержка,

• защита данных пользователя (конфиденциальность, целостность, доступность),

• идентификация и аутентификация,

• управление безопасностью,

• приватность (конфиденциальность работы в системе),

• надежность средств защиты,

• контроль за использованием ресурсов,

• контроль доступа к объекту оценки,

• доверенный маршрут/канал (прямое взаимодействие).

Требования уверенности в безопасности (адекватности)

• управление проектом,

• дистрибуция,

• разработка,

• документация,

• процесс разработки,

• тестирование,

• анализ защиты.

«Единые критерии» содержат совокупность предопределённых оценочных уровней уверенности в безопасности, составленных из компонентов семейств требований уверенности в безопасности. Эти уровни предназначены:

• для достижения совместимости с исходными критериями;

• для обеспечения потребителя пакетами компонентов общего назначения.

**11. Каковы тенденции развития международной нормативной базы в области информационной безопасности?**

Основное назначение международных стандартов -это создание на межгосударственном уровне единой основы для разработки новых и совершенствования действующих систем качества. Сотрудничество в области стандартизации направлено на приведение в соответствие национальной системы стандартизации с международной. Международные стандарты не имеют статуса обязательных для всех стран-участниц. Любая страна мира вправе применять или не применять их. Решение вопроса о применении международного стандарта связано в основном со степенью участия страны в международном разделении труда.

Первые версии стандартов создавались в основном исходя из нужд обороны и были нацелены на обеспечение секретности информации. С развитием средств вычислительной техники и телекоммуникаций возникла потребность создания новых стандартов, отражающих особенности современного уровня информационных технологий.

# **Практическое занятие №2**

**Тема: «Решение задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа»**

**Цель:** научится решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

**Теоретическое введение:**

все методы защиты информации по характеру проводимых действий можно разделить на законодательные, организационные, технические, комплексные.

Е0− положительный эффект (экономический, политический, технический и т.д.

∆E− на такую величину несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования.

E− эффективность функционирования объекта с учетом воздействия несанкционированного доступа.

Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа: 𝐸=𝐸0−∆𝐸

∆𝐸3− снижение эффективности функционирования объекта при наличии средств защиты

K− это коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта; возрастающая.

Таким образом, для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид:

**Задание на выполнение:**

Решить задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа в соответствии с вариантом.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 6 | 12000 | 11000 | 6 | 300 |

Исходные данные: E0 =12000(руб.) E =11000(руб.) K=6 C=300(руб.).

Рассчитаем ∆E: ∆𝐸=𝐸0−𝐸=12000-11000=1000(руб.)

Находим значение относительной эффективности функционирования по формуле:



Относительная эффективность = 1-(1000/12000)=0,92

Вычислим коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта по формуле:



Получим коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта равный 1000/6=166,67 (руб.)

Находим эффективность функционирования по формуле:



Получим 12000-166,67= 11833,33 (руб.)

Найдём относительную эффективность функционирования по формуле:



Получим 1 - ( 1000 / 6 / 12000 ) = 0,99

В том случае, если эффективность функционирования имеет стоимостное значение, то вычисляем по формуле:



Получим 12000 – ( 1000 / 6 ) - 300 = 11533,33

**Вывод:** В итоге получим прибыль 11533,33 – 11000 = 533,33 (руб.);

В результате проведения лабораторной работы был приобретён опыт решения задач для создания средств защиты информации. На данных, полученных в результате работы, строится система для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

# **Практическое занятие №3**

**Разработка политики информационной безопасности завода**

**Цель работы**: Разработать проект политики информационной безопасности бизнес-компании.

**Введение**

Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры, будь то государственное учреждение или частное предприятие.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса об разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, Конституции, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, таких, как ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных.

Безопасность информационной инфраструктуры компании подразумевает защиту от случайных или умышленных действий, которые могут нанести вред владельцам данных или их пользователям. Действия лиц, несущих ответственность за эту сферу, должны быть направлены на создание защиты, препятствующей утечкам данных, а не борьбу с их последствиями. Но при этом важно сохранять простой доступ к информации тем людям, которые на законных основаниях пользуются базами данных.

**Общие положения**

Цели и задачи

Концептуальная схема информационной безопасности предприятия направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

- разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;

- выявление, оценка и прогнозирование угроз информационной безопасности;

- организация технической защиты информации, участие в проектировании систем защиты;

- проведение периодического контроля состояния ИБ, учет и анализ результатов с выработкой решений по устранению уязвимостей и нарушений;

- контроль за использованием закрытых каналов связи и ключей с цифровыми подписями;

- организация плановых проверок режима защиты, и разработка соответствующей документации, анализ результатов, расследование нарушений;

- разработка и осуществление мероприятий по защите персональных данных;

- организация взаимодействия со всеми структурами, участвующими в их обработке, выполнение требований законодательства к информационным системам персональных данных, контроль действий операторов, отвечающих за их обработку.

**Структура организации**

Под организационной структурой управления предприятием понимается состав отделов, служб и подразделений в аппарате управления, системная их организация, характер соподчиненности и подчиненности друг другу и высшему органу управления, а также набор координационных и информационных связей, порядок распределения функций управления по различным уровням и подразделениям.

Директор является исполнительным органом организационной структуры. Директор предприятия осуществляет также контролирующую функцию, т.е. он подписывает и утверждает документы, договора и сделки с другими организациями, а также контракты о приёме на работу.

В организации разработаны положения о структурных подразделениях и должностные инструкции. Каждое подразделение взаимосвязано с другими подразделениями и выполняет свою функцию. Например, отдел кадров занимается вопросами формирования и развития стабильного трудового коллектива, созданием благоприятного социально-психологического климата, осуществляет эффективную кадровую политику, оказывает методическую помощь руководителям подразделений по проблемам управления персоналом. Является самостоятельным структурным подразделением и подчиняется непосредственно директору организации.

Во главе завода традиционно стоит **директор**. По каждому крупному направлению работы – у директора и других сотрудников некоторых должностей есть заместители – главный бухгалтер, главный инженер.

**Главный бухгалтер** непосредственно подчиняется директору предприятия и принимает участие в производственных, технических совещаниях.

Непосредственно главному бухгалтеру подчиняется **планово-экономический отдел**

В планово-экономическом отделе осуществляется разработка направлений перспективного развития предприятия, а также планирование объема, ассортимента и качества продукции, разрабатывается и утверждается годовой план экономического и социального развития.

**Главный инженер** организует обучение и повышение квалификации рабочих и инженерно-технических работников.

Является первым заместителем директора организации и несет ответственность за результаты и эффективность производственной деятельности.



Производственная структура предприятия – это состав и соотношение его внутренних звеньев: цехов отделов, лабораторий и других компонентов, составляющих единый хозяйственный объект; определяется размером предприятия, отраслью производства, уровнем технологии и специализации предприятия.

**Оценка рисков**

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

*– по аспекту информационной безопасности, на который направлены угрозы:*

а) угрозы конфиденциальности (неправомерный доступ к информации);

б) угрозы целостности (неправомерное изменение данных);

в) угрозыдоступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы);

*– по степени преднамеренности действий:*

а) случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия);

б) преднамеренные (умышленные действия, например, шпионаж и диверсии);

*– по расположению источника угроз:*

а) внутренние (источники угроз располагаются внутри системы);

б) внешние (источники угроз находятся вне системы);

*– по размерам наносимого ущерба:*

а) общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);

б) локальные (причинение вреда отдельным частям объекта безопасности);

в) частные (причинение вреда отдельным свойствам элементов объекта безопасности);

*– по степени воздействия на информационную систему:*

а) пассивные (структура и содержание системы не изменяются);

б) активные (структура и содержание системы подвергается изменениям).

Основными угрозами ИБ АСУ ТП (автоматизированным системам управления технологическим процессом) являются:

*– несанкционированное вмешательство в управление технологическими процессами;*

*– нарушение функционирования АСУ ТП или ее отдельных элементов;*

*– несанкционированный доступ к информации, хранимой в базах данных* *АСУ ТП и передаваемой по каналам передачи данных.*

В результате реализации угроз ИБ могут быть нарушены:

*– целостность (утрата, уничтожение, модификация) информации;*

*– доступность (блокирование) информации и отдельных элементов АСУ ТП;*

*– конфиденциальность (утечка, перехват, съем, копирование, хищение, разглашение) информации.*

Обеспечение ИБ АСУ ТП осуществляется по следующим направлениям, реализуемым организационно-техническими мерами защиты.

Физическая защита, включая:

– защиту технических средств обработки, хранения и передачи информации;

– защиту зданий, сооружений и помещений.

Защита при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов, включая:

– защиту от вредоносного ПО;

– резервирование серверов, сетевого оборудования, средств защиты и каналов передачи данных;

– обеспечение безопасности сетевой инфраструктуры;

– защиту программного обеспечения;

– регистрацию и учет событий ИБ;

– организацию безопасного использования, преобразования, хранения и передачи информации;

– криптографическую защиту.

Контроль доступа, в том числе:

– управление доступом пользователей;

– определение ответственности пользователей;

– контроль доступа к прикладным системам;

– контроль доступа к ОС;

– контроль сетевого доступа;

– обеспечение безопасности при использовании мобильных устройств;

– обеспечение безопасности в беспроводных сетях;

– контроль доступа к сетевому оборудованию.

**Реализация организационно-технических мер обеспечения ИБ АСУ ТП достигается в первую очередь путем:**

– наделения пользователей автоматизированной системы управления технологическими процессами правами доступа и привилегиями по работе в АСУ ТП;

– корректного использования и администрирования встроенных механизмов безопасности технических средств обработки, хранения и передачи информации и средств защиты, входящих в состав АСУ ТП;

– контроля функционирования и настроек механизмов безопасности, а также соблюдения требований по ИБ;

– физической защиты технических средств обработки, хранения и передачи информации от неправомерного доступа к ним.

Обязанности пользователей АСУ ТП по обеспечению ИБ зависят от занимаемой должности и определены в их должностных инструкциях.

**Защита технических средств обработки, хранения и передачи информации**

В целях предотвращения несанкционированного доступа к информации и ее утечки, хищения технических средств обработки и хранения информации и несанкционированного управления ими, а также простоев в функционировании АСУ ТП обеспечивается физическая защита входящих в нее технических средств. *Серверное оборудование и критичное сетевое* *оборудование размещаются в запираемых шкафах с сигнализацией, располагаемых в серверных, ограничивающих доступ к ним посторонних лиц*. *Перед утилизацией или передачей в ремонт технических средств выполняется гарантированное удаление информации с них. Кабельные сети прокладываются так, чтобы максимально ограничить несанкционированный доступ к ним.* Для защиты от перебоев электричества *в эксплуатацию вводятся централизованные системы бесперебойного питания*. Система ИБ включает в себя максимальное количество элементов, обеспечивающих эффективную защиту системы при критической нагрузке.

**Защита от вредоносного ПО**

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного ПО в АСУ ТП применяются *средства защиты* от вредоносного ПО, они *устанавливаются на серверном оборудовании и автоматизированные рабочие места операторов и специалистов автоматизированной системы управления технологическими процессам*и. Управление и обновление средств защиты от вредоносного ПО осуществляются централизованно. Разрешается использование только сертифицированных на соответствие требованиям безопасности информации средств защиты от вредоносного ПО. Администрирование средств защиты от вредоносного ПО осуществляется системным администратором. Настройки системы защиты от вредоносного ПО согласовываются и контролируются администратором ИБ.

**Криптографическая защита**

В целях обеспечения конфиденциальности информации при ее передаче вне контролируемых зон применяются сертифицированные установленным порядком средства криптографической защиты информации. Это *специальные методы шифрования, кодирования* в результате которых содержание передаваемых файлов становится недоступным, без предъявления ключа криптограммы и обратного преобразования. *Криптографическая защита информации на предприятии реализована с помощью метода криптосистемы с открытым ключом*. В системе с открытым ключом используются два ключа — *открытый и закрытый*, которые математически связаны друг с другом. *Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.*

**Локальная безопасность**

**Локальная политика безопасности**, то есть точное описание настроек для корректной реализации правил аутентификации пользователей, управления доступом, защиты трафика и др., необходима любому средству защиты, реализующему какой-либо сервис информационной безопасности. При традиционном подходе администратору приходится отдельно настраивать каждое средство защиты или реплицировать какие-то простейшие настройки на большое число узлов с последующей их корректировкой. Очевидно, что это неизбежно приводит к большому числу ошибок администрирования и, как следствие, к существенному снижению уровня защищенности корпоративной сети.

***Антивирусная защита***

Антивирусная защита предназначена для обеспечения антивирусной защиты серверов и автоматизированных рабочих мест пользователей предприятий. *На каждом работающем компьютере, или сервере при вводе в эксплуатацию или после переустановки ОС* сотрудниками ЦНИТ *в обязательном порядке устанавливается и активируется антивирусная программа.*

**Заключение**

Политика безопасности — совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На политике безопасности нельзя экономить, так как данные, которые могут быть подвержены хищению, копированию или изменению, могут стоить дороже, чем ресурсы, потраченные на её разработку и осуществление.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность, общие меры предосторожностей, так же такие пункты как люди, и процессы, и избыточность, и непрерывность работы.

Политика безопасности должна быть разработана так, чтобы её взлом стоил дороже, чем сама информация.