Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Отчет

К практической работе №3:

Основы защиты информации

«Разработка политики информационной безопасности университета»

Выполнил:

Студент 2 курса 2 группы ФИТ

Радивил Данила Юрьевич

**Минск, 2022**

**Практическое занятие №3**

**Тема «Разработка политики информационной безопасности университета»**

Цель: Разработать проект политики информационной безопасности школы.

# Введение

Жизнь современного общества немыслима без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами, космическими кораблями. Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Однако именно высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т.п.). Доступность и широкое распространение информационных технологий, ЭВМ делает их чрезвычайно уязвимыми по отношению к деструктивным воздействиям.

Информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Сущность информационно-технической безопасности можно определить, как достижение такого состояния развития общественных отношений, при котором обеспечена надежная и всесторонняя защита интересов субъектов этих отношений - человека, общ ества и государства - от угроз деструктивного информационного воздействия.

Информационно-психологическая безопасность состоит в том, что основным ее содержанием является защита интересов безопасности человека, безопасности общества и безопасности государства, как осознанная социальная потребность субъекта на безопасное удовлетворение своих потребностей.

# 3.1 Общие положения

***1. Цели и задачи***

Концептуальная схема информационной безопасности школы 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.

Направление информационной безопасности создано в отделе собственной безопасности со следующими задачами и функциями, определяемыми постановлением Правительства 915-12 "О лицензировании отдельных видов деятельности" и Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

- 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.

***2. Организационно-правовой статус сотрудников информационной безопасности***

- сотрудники имеют право беспрепятственного доступа во все помещения, где установлены технические средства с Информационными системами, право требовать от руководства подразделений и администраторов ИС прекращения автоматизированной обработки информации, персональных данных, при наличии непосредственной угрозы защищаемой информации;

- имеют право получать от пользователей и администраторов необходимую информацию по вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности;

- главный специалист по ИБ имеет право проводить аудит действующих и вновь внедряемых ИС, ПО, на предмет реализации требований защиты и обработки информации, соответствию требований законодательства, запрещать их эксплуатацию, если не отвечают требованиям или продолжение эксплуатации может привести к серьезным последствиям в случае реализации значимых угроз безопасности;

-сотрудники имеют право контролировать исполнение утвержденных нормативных и организационно-распорядительных документов, касающихся вопросов информационной безопасности.

# 3.2 Структура организации

Традиционно, во главе школы стоит **директор**. По каждому крупному направлению работы – будь то учебная или воспитательная работа, международные связи – у директора есть заместители –заучи, они курируют работу школы по своим направлениям.

Тематически образовательная часть делится по образовательным **программам**, **направлениям** подготовки. Выпускники получат аттестат **среднего образования** либо **аттестат о базовом образовании**. **Среднее образование** получают ученики, окончившие 11 классов, а **базовое образование** те ученики, которые окончили 9 классов.

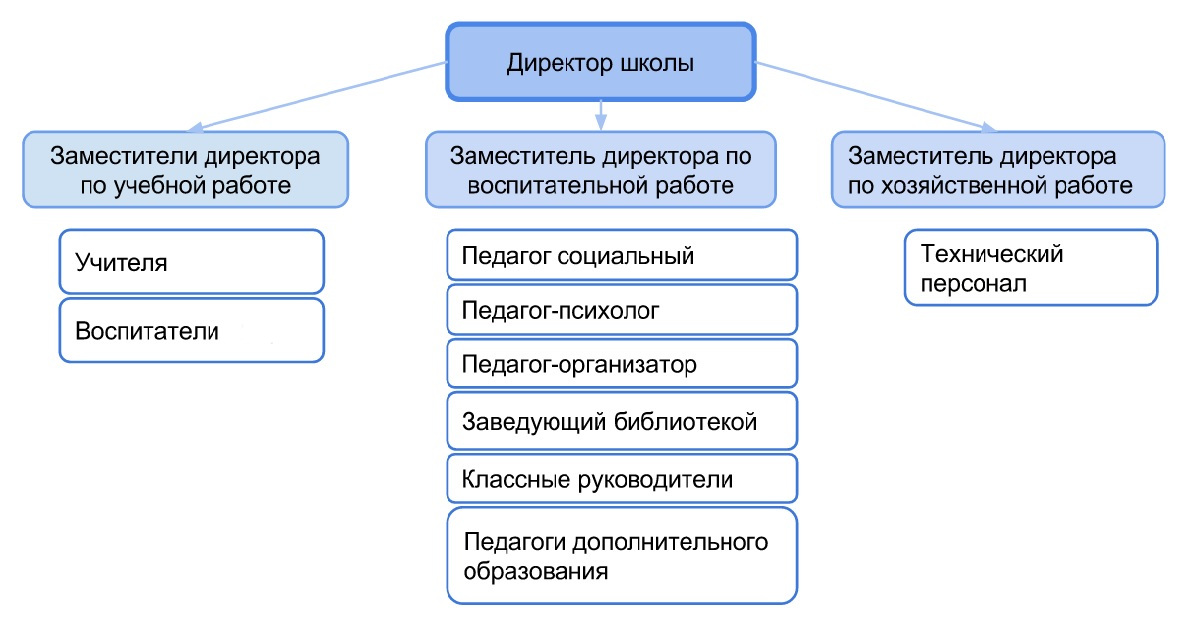
**Директор** **–** самый главный в школе. К нему вам нужно обращается в случае вопросов, которые другие работники школы не могут решить. Например, зачисление ребенка в школу, или перевод в 10-й класс для получения **среднего образования**.

Кроме **директора** в школе есть другие специалисты, например, **завуч по воспитательной работе, психолог.**

При поступлении в школу, вы будете зачислены в классы. Каждый класс имеет свое собственное название, состоящее из цифры и класса. Расписание у разных классов будет отличаться. Школьники из вашего класса называются одноклассники, а школьники из других классов такой же цифры - параллелью. На некоторых занятиях вы будете присутствовать вместе с только с определенными людьми, например, на уроках труда будут сформированы группы, из мальчиков и девочек.

Перечень должностей данного предприятия представлен на рисунке 1.1.

# 



ф

# 3.3 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 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.

Обеспечение ИБ 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.

### 3.4. Организация безопасной эксплуатации средств обработки, хранения и передачи информации

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных для этого работников. Изменения конфигурации средств обработки и хранения информации, а также изменения сетевой инфраструктуры, конфигурации сетевого оборудования выполняются администратором. Все изменения регистрируются в соответствующих журналах. Самостоятельное изменение конфигурации средств обработки, хранения и передачи информации пользователями АСУ ТП запрещено. Использование съемных носителей информации в автоматизированной системе управления технологическими процессами запрещено. При размещении средств разработки, тестирования и эксплуатации обеспечивается их физическое или логическое разделение в целях снижения риска несанкционированного доступа или внесения изменений в систему.

### 3.4.1 Защита от вредоносного программного обеспечения

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного ПО в АСУ ТП применяются средства защиты от вредоносного ПО. Средства защиты от вредоносного ПО устанавливаются на серверном оборудовании и АРМ операторов и специалистов автоматизированной системы управления технологическими процессами. 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.

Используемая антивирусная система защиты имеет:

– стойкую систему самозащиты, которая не по­зволит неизвестной вредоносной программе нарушить нормальную работу АСУ ТП и сделает возможным функционирование АСЗ до поступления обновления;

– систему обновлений, находящуюся под контролем системы самозащиты антивирусной системы и не использующую компоненты операционной системы, которые могут быть скомпрометированы;

– систе­му обновления, позволяющую мгновенно, по сигна­лу системы централизованного управления доставить на защищаемый антивирусом объект обновления для лечения активного заражения;

– дополнительные механизмами для обнаружения новых неизвестных вредоносных программ;

– проверяет все поступающие из локальной сети файлы до момента получения их используемыми приложениями, что исключает использование вредоносными приложениями неизвестных уязвимостей данных приложений;

– систему централизованного сбора информации с удаленных рабочих станций и серверов, позволяющую максимально быстро передавать в антиви­русную лабораторию всю необходимую для решения проблемы информацию.

### 3.4.2 Обеспечение безопасности сетевой инфраструктуры

В целях обеспечения непрерывного и устойчивого функционирования АСУ ТП осуществляется защита ее сетевой инфраструктуры. Защита сетевой инфраструктуры обеспечивается:

– физической защитой сетевого оборудования и средств защиты;

– контролем логического доступа к сетевому оборудованию;

– шифрованием каналов управления;

– контролем сетевых соединений;

– обнаружением и предотвращением вторжений;

– мониторингом подключаемых к ЛВС автоматизированной системы управления технологическими процессами сетевых устройств;

– использованием встроенных в сетевое оборудование средств защиты от подмены адреса (средств антиспуфинга);

– защитой информации ограниченного доступа при ее передаче вне контролируемых зон;

– применением средств мониторинга и регистрации событий.

Контроль сетевых соединений между ЛВС АСУ ТП и подключаемыми к ней беспроводными сетями также осуществляется средствами межсетевого экранирования. Защита информации ограниченного доступа при ее передаче вне контролируемых зон осуществляется применением сертифицированных средств криптографической защиты информации (построением защищенных виртуальных сетей). Защита от вторжений в ЛВС АСУ ТП осуществляется средствами обнаружения и предотвращения вторжений, размещаемыми на входе в ЛВС. Базы данных сигнатур средств обнаружения и предотвращения вторжений регулярно обновляются с сайта производителя применяемых средств. Категорически запрещается удаленное администрирование АСУ ТП.

В целях поддержания работоспособности ПО осуществляются меры по устранению уязвимостей ПО, а также другие меры защиты от:

– умышленного либо неумышленного раскрытия, модификации или уничтожения защищаемых данных. В частности, это подразумевает использования средств ограничения доступа к различным ресурсам офисного контроля;

– установки средств защиты кем-либо, кроме администратора, несанкционированного внесения изменений в порядок функционирования системы защиты, изменения ее возможностей. Данное требование приводит к необходимости разграничения прав доступа к настройкам системы, защите ее от несанкци­онированного воздействия. Это подразумевает использование в локальной сети только программных продуктов, поддерживающих ролевой принцип доступа, а также применение функций офисного контроля. Средства защиты должны устанавливаться как на рабочие станции, так и на сервер. В организации, соответствующей требованиям стандарта, должна использо­ваться только защищенная почта, что вместе с требованием о наличии защиты от вирусов и спама подразумевает установку средств антивирусной фильтрации почтовых сообщений. В свою очередь доступ в сеть Интернет должен использоваться только для обеспе­чения банковской деятельности. Устранение уязвимостей ПО достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками ПО. Обновление ОС, другого общесистемного и прикладного ПО осуществляется системными администраторами и администраторами прикладных систем. Обновления для ПО АСУ ТП получаются с серверов обновлений, размещенных в ИУС ПХД.

### 3.4.3 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.

# 3.5 Сетевая безопасность

***3.5.1 Доступ из Интернет в сеть школы:***

- доступ во внутреннюю сеть осуществляется только через настроенный межсетевой экран;

- доступ из вне периметра сети разрешен только по распоряжению директора ЦНИТ с согласованием у ответственного сотрудника ОСБ, по определенному порту и на определенное время;

- не допускается удаленный доступ в локальную сеть с использованием не персонифицированных, групповых и анонимных учетных записей;

- не допускается использование программ удаленного администрирования типа TeamViewer. Как исключение, по согласованию с сотрудником ИБ ОСБ возможно подключение для удаленной настройки ПО на ограниченное время. Настройка и конфигурация средств обнаружения вторжений, межсетевых экранов должны обеспечивать оперативное обнаружение несанкционированного доступа к ресурсам сети для принятия мер блокирования проникновения нейтрализации последствий.

При администрировании удаленного доступа к ресурсам корпоративной сети Университета предъявляются следующие требования:

- удаленный доступ пользователей к ресурсам и сервисам компьютерной сети университета обеспечивается на основе зарегистрированных персональных учетных записей, с использованием технологии VPN, других протоколов шифрования;

- доступ предоставляется сроком на 3 месяца, при необходимости продлевается с разрешения директора ЦНИТ;

- делается соответствующая запись в Журнале учета предоставления удаленного доступа; - список сотрудников, которым предоставлен удаленный доступ поддерживается в актуальном состоянии и передается в ОСБ по запросу.

В целях обеспечения безопасности и нормального функционирования компьютерных сетей запрещается:

- самовольно подключать компьютерное оборудование (беспроводные точки доступа, маршрутизаторы, компьютеры и др.) к сети университета и присваивать ему сетевое имя и адрес без согласования с ЦНИТ;

- перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с ЦНИТ;

- использовать информационные ресурсы университета для сетевых игр, распространения коммерческой рекламы; организации СПАМа. - сканировать узлы сети неуполномоченными на то сотрудниками . 2.2. Средства защиты, маршрутизаторы и межсетевые экраны:

Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 определяет как необходимость организацию управления (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы. В Университете используется система межсетевого экранирования, которая реализует функции фиксации во внутренних журналах информации о проходящем IP-трафике, фильтрацию пакетов служебных протоколов, блокирования доступа не идентифицированного объекта.

Для анализа защищенности ИС сотрудниками ИБ ОСБ применяются специализированные программно-аппаратные средства – сканеры безопасности. Проводится выявление и анализ уязвимостей и несоответствия в настройках ОС, ПО, СУБД, сетевого оборудования.

Выявленные уязвимости протоколируются и передаются в ЦНИТ для устранения в установленные сроки. Запрещается использовать ПО снятое с поддержки, имеющее уязвимости, с просроченными сертификатами. Подсистема обнаружения вторжений, обеспечивает выявление сетевых атак на элементы ИС подключенные к сетям общего пользования и (или) международного обмена. Функционал подсистемы реализуется программными и программноаппаратными средствами, на межсетевых экранах.

Администратор сети ведет протоколирование и регулярный мониторинг доступа, контролирует содержание трафика с использованием специализированного ПО, проводит анализ логфайлов. На межсетевом экране заводится лог-файл, куда записываются все обращения к ресурсам (попытки создания соединений). Доступ к лог-файлам имеют администратор сети и сотрудник ОСБ. Анализ лог-файлов проводится с применением соответствующего ПО (анализатор логов) сотрудником ОСБ Сотрудник ИБ ОСБ должен иметь независимый доступ к элементам системы защиты для контроля настроек конфигураций, просмотра системных журналов . Доступ из одного сегмента сети в другой ограничивается и разделяется маршрутизаторами. Настройкой маршрутизаторов занимается отдел сетевого и системного администрирования. Приобретение и установка средств и систем защиты ИС осуществляются по согласованию с сотрудником ИБ ОСБ. Сеть ИСПДн выделена в отдельный сегмент и защищена межсетевым экраном.

# 3.6 Локальная безопасность

***3.6.1 Антивирусная защита***

Исходя из требований ФСТЭК от 30 июля 2012 г. № 240/24/3095 к средствам антивирусной защиты антивирусное ПО должно соответствовать 6 классу защиты и типу «А» для применения в информационных системах персональных данных 4 класса.

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

Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на АРМ, серверах, осуществляется специалистами структурных подразделений и ЦНИТ в соответствии с руководствами по применению конкретных антивирусных средств. Отключение или не обновление антивирусных средств не допускается.

Установка и обновление антивирусных средств в организации контролируется централизованно ответственным сотрудником ЦНИТ. Система обнаружения атак, встроенная в антивирусную программу, сохраняет информацию об атаках и подозрительной активности в лог-файлы, которые анализирует ответственный сотрудник ЦНИТ и высылает генерируемые системой отчеты о сетевых атаках и вирусной активности сотруднику ИБ ОСБ.

В случае массированной вирусной атаки сотрудники ЦНИТ определяют масштаб заражения, принимают меры к локализации, блокированию распространения, совместно с сотрудником ИБ ОСБ определяют источник заражения, характер действия и распространения вируса, нейтрализуют последствия атаки. При необходимости ставятся патчи и необходимые обновления ПО, закрывающие уязвимости, используемые вирусами. Пользователи руководствуются требованиями антивирусной защиты, изложенными в Правилах использования информационных систем и ИТсервисов ТГУ.

***3.6.2 Защита электронного документооборота.***

Передача информации конфиденциального характера за периметр сети осуществляется только по защищенным каналам. Защищенные каналы строятся с 10 использованием криптозащиты, на базе решений VipNet, VPN, Банк-клиент или других, сертифицированных ФСТЭК. Криптографическая защита предназначена для исключения НСД к защищаемой информации, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена. Криптографическая защита реализуется путем внедрения криптографических программно-аппаратных комплексов КриптоПро . Все экземпляры КриптоПро должны иметь лицензию и регистрируются в Журнале СКЗИ у сотрудника ИБ ОСБ. Электронные подписи выдаются удостоверяющим центром на определенное лицо, по его документам на основании заключенного договора. Инициатором заключения договора является структурное подразделение. После получения ключа ЭП, снимается копия сертификата и регистрируется в журнале учета СКЗИ у сотрудника ИБ ОСБ. Ключи электронных подписей должны храниться в сейфах ответственных лиц. Доступ неуполномоченных лиц к носителям ключей должен быть исключен.

Передача ключей запрещена. Запрещается оставлять носители с ЭП установленными в компьютер, при покидании рабочего места. Компьютеры, на которых установлены средства криптозащиты, должны соответствовать требованиям, изложенным в документации по КриптоПро. Соответствующий документации объем работы проводит сотрудник ЦНИТ по служебной записке сотрудника ИБ ОСБ. Внутренний документооборот является подсистемой ИСПДн, осуществляется в защищенном исполнении с использованием ПО, для которого актуальны угрозы 3-го типа, связанные с наличием НДВ в ПО.

Разграничение прав доступа к информационным системам и системам хранения данных, защита от НСД Для доступа к информационным системам университета сотрудник должен ввести логин и пароль. При предоставлении доступа к ОС, приложениям ИС, реализуется принцип минимума привилегий доступа. В целях защиты информации организационно и технически разделяются подразделения Университета, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности и смысловой направленности). Данная задача решается с использованием возможностей конкретных ИС, где в целях обеспечения защиты данных доступ и права пользователей ограничивается набором прав и ролей. В случае обработки информации конфиденциального характера права назначаются администратором ИС по ролевой матрице доступа, в соответствии с функциональными обязанностями, определяемыми должностью и по служебной записке руководителя подразделения согласованной с сотрудником ОСБ. 11 Администратором ИС проводится анализ журналов доступа к ресурсам ИС, фиксируются попытки НСД, о которых докладывается ответственному сотруднику ИБ ОСБ. Для защиты от НСД на компьютерах в сегментах сети, где обрабатывается информация конфиденциального характера используются продукты линейки Dallas Lock, Secret Net, c администрированием в Центре безопасности, развернутом в домене. Администратором Центра безопасности является администратор домена. Не допускается использование учетных записей уволенных сотрудников.

***3.6.3 Использование электронной почты, сети Интернет***

Не допускается распространять материалы, использование и распространение которых ограничено действующим законодательством РБ.

Пересылка информации конфиденциального характера осуществляется только с использованием корпоративной почты.

Электронная почта на рабочем месте сотрудника используется только для служебной, и иной, предусмотренной должностными обязанностями переписки.

Логин и пароль к корпоративной электронной почте для сотрудников выдает ответственный сотрудник ЦНИТ по служебной записке на имя директора ЦНИТ, для студентов – по студенческому билету.

Запрещается открывать письма с подозрительными вложениями, с незнакомого адреса и.т.п., о получении подобных писем сообщается сотруднику ИБ ОСБ. Запрещается публиковать информацию конфиденциального характера в социальных сетях, пересылать через системы мгновенного обмена сообщениями (ICQ, Jabber и. т. п.).

Запрещается использование облачных сервисов на рабочих местах сотрудников, обрабатывающих информацию конфиденциального характера.

Доступ через беспроводную сеть разрешается только к общедоступным ресурсам сети.

Беспроводные точки устанавливают и администрируют сотрудники ЦНИТ. Самостоятельно скачивать и устанавливать программное обеспечение разрешается только уполномоченным на то сотрудникам ЦНИТ. Запрещается несогласованная с ЦНИТ установка роутеров WiFi.

## 3.7 Физическая защита

Все объекты критичные с точки зрения информационной безопасности (сервера баз данных, маршрутизаторы ) находятся в контролируемых зонах. Сотрудники ЦНИТ обязаны вскрывать и сдавать под охрану помещение серверной в соответствии с Инструкцией по вскрытию и сдаче под охрану помещения серверной. 12 Порядок доступа сотрудников ЦНИТ определяется Порядком доступа в серверные помещения. При неавтоматизированной обработке информации конфиденциального характера документы (личные дела сотрудников, студентов, абитуриентов, карточки лицевых счетов, картотека и.т.д.) должны храниться в шкафах, исключаемых несанкционированный доступ к ним. Требования к обеспечению безопасности определены в документе Порядок доступа в помещения, в которых обрабатывается информация конфиденциального характера. В контролируемых зонах университета ведется видеонаблюдение. На территории университета действует пропускной режим, порядок которого определяется локальным нормативным актом.

**3.8** **Обработка персональных данных**

Необходимая нормативная и организационно-регламентирующая документация размещена на сайте Отдела собственной безопасности. Все сотрудники школы, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные внутренними нормативными документами правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности обработки ПДн. Компетентность пользователей в области обеспечения ИБ достигается обучением правилам безопасной (с точки зрения ИБ) работы, осведомленности об источниках потенциальных угроз и периодическими проверками их знаний и навыков.

Занятия с пользователями проводятся сотрудником ИБ ОСБ на регулярной основе не реже двух раз в год. Все действия пользователей компьютеров и обязанности по соблюдению требований ИБ определяются Порядком действий пользователя информационной системы по обеспечению информационной безопасности в Тольяттинском государственном университете, который они изучают, имеют распечатанный экземпляр с подписью сотрудника об ознакомлении.

При допуске сотрудника к выполнению обязанностей связанных с обработкой персональных данных непосредственный начальник подразделения, в которое он поступает, организует ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, подает служебную записку директору ЦНИТ о предоставлении доступа к ИСПДн с указанием предполагаемой роли сотрудника. Далее сотрудник проходит инструктаж у администратора безопасности ИСПДн, и расписывается об ознакомлении с Положением о защите персональных данных и Порядком обеспечения конфиденциальности при обработке персональных данных, получает у администратора ИСПДн логин и пароль к учетной записи с правами, согласно ролевой матрицы доступа. Порядок работы с запросами на предоставление сведений по персональным данным определяется утвержденными локальными нормативными документами. 13

Общедоступными персональными данными сотрудников являются фамилия, имя, отчество, занимаемая должность, подразделение, а студентов, аспирантов, слушателей - фамилия, имя, отчество, группа, специальность. Сотрудники Университета должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Сотрудникам, обрабатывающим ПДн, запрещается устанавливать любое программное обеспечение, подключать личные мобильные устройства и отчуждаемые незарегистрированные в ОСБ носители информации, а так же записывать на них защищаемую информацию, за исключением случаев, предусмотренных функциональными обязанностями.

Сотрудникам запрещается разглашать содержание защищаемой информации, которая стала им известна при работе с информационными системами Университета, третьим лицам, согласно Положения о защите персональных данных. Запрещается хранение информации конфиденциального характера локально на компьютере, не оснащенном программными средствами предотвращения несанкционированного доступа (SecretNet, DallasLock и др.) Допуск к ИСПДн третьих лиц для осуществления ими договорных обязательств осуществляется при выполнении требований, предъявляемых к защите информации и соблюдения конфиденциальности, отражаемых в договоре, согласованном с ОСБ на этапе заключения. СКЗИ при обработке персональных данных в университете не используются. Текст Политики в отношении обработки персональных данных размещается на сайте ОСБ в свободном доступе.

# 

# 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.

**Вывод:** в ходе лабораторной работы я разработал проект политики информационной безопасности школы.