**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

**Кафедра телекоммуникаций и информационных технологий**

РАДКЕВИЧ

Владислав Игоревич

**РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ КЛАССА Б2 НА ПРИМЕРЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ УЧЕБНОГО ЗАВЕДЕНИЯ**

Дипломная работа

Научный руководитель:  
кандидат технических наук,

доцент Г.К. Резников

Допущен к защите

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 г.

Зав. кафедрой телекоммуникаций и информационных технологий

кандидат физико-математических наук, доцент Ю.И. Воротницкий

Минск, 2017

**ОГЛАВЛЕНИЕ**

[ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ 3](#_Toc484776486)

[ВВЕДЕНИЕ 4](#_Toc484776487)

[ГЛАВА 1 6](#_Toc484776488)

[1.1 Введение в информационную безопасность и систему защиты информации. Терминология. 6](#_Toc484776489)

[1.2 Средства защиты информации 10](#_Toc484776490)

[1.3 Классификация объектов информатизации 14](#_Toc484776491)

[ГЛАВА 2 16](#_Toc484776492)

[ПРОЕКТИРОВАНИЕ СЗИ 16](#_Toc484776493)

[2.1 Анализ организационной структуры информационной системы 16](#_Toc484776494)

[2.2 Классификация информации, хранящийся и обрабатываемой в информационной системе 18](#_Toc484776495)

[2.3 Проведение оценки угроз и рисков для ИС 19](#_Toc484776496)

[2.4 Разработка технического задания 21](#_Toc484776497)

[2.5 Техническое задание на систему защиты информации 22](#_Toc484776498)

[ГЛАВА 3 32](#_Toc484776499)

[СОЗДАНИЕ СЗИ 32](#_Toc484776500)

[3.1 Разработка политики безопасности 32](#_Toc484776501)

[3.2 Политика безопасности 33](#_Toc484776502)

[ЗАКЛЮЧЕНИЕ 43](#_Toc484776503)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 44](#_Toc484776504)

# ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ИБ – информационная безопасность

ИБП – источник бесперебойного питания

ИС – информационная система

КЗ – контролируемая зона

КСБО – комплекс средств безопасности объекта

НСД – несанкционированный доступ

ОИ – объектов информатизации

СОВ – система обнаружения вторжений

ТС – технические средства

# ВВЕДЕНИЕ

В наше время организация эффективной системы защиты информационной системы становится очень важным стратегическим фактором, влияющим на развитие любой организации, потому что информация в наши дни является основой бизнеса. При этом значение понятия информация состоит не только из статических информационных ресурсов (базы данных, текущие настройки оборудования и другие), но и динамических информационных процессов обработки данных.

Ещё в 1815 году Натан Ротшильд сказал фразу, которая стала впоследствии крылатой «Кто владеет информацией, тот владеет миром». Поэтому я считаю, что как для учебного заведения, так и для любой другой структуры или организации задача защиты информации должна быть если не самой важной, то одной из важнейших.

Главной целью любой системы защиты является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов организации от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений.

Информационная среда организации, вне зависимости от своего состава, должна предусматривать систему защиты. Однако затраты на обеспечение высокого уровня безопасности могут быть неоправданны. Нахождение разумного компромисса и выбор приемлемого уровня защиты при допустимых затратах является важным условием постановки задачи обеспечения ИБ. Для решения этого вопроса необходимо проводить анализ рисков ИБ, позволяющий оценить существующий уровень защищенности ресурсов организации. Значение риска, являющееся произведением вероятности реализации угрозы по отношению к защищаемому ресурсу на ущерб от реализации данной угрозы, служит показателем полноты, комплексности и эффективности системы ИБ организации, а также позволяет выявить ее слабые места.

Цель курсовой работы – разработка системы защиты информации информационной системы класса Б2 на примере информационной системы учебного заведения. Для реализации этого проекта были поставлены следующие задачи:

* 1. Проанализировать набор стандартов СТБ 34.101, приказ №62 оперативно-аналитического центра при президенте РБ «О некоторых вопросах технической и криптографической защиты информации»
  2. Изучить этапы проектирования и создания системы защиты информации.
  3. Проанализировать объект защиты информации:
* классификация информации, хранящейся и обрабатываемой в информационной системе;
* анализ организационной структуры информационной системы и информационных потоков.
  1. Определение потенциальных угроз для объекта защиты и анализ возможных последствий их осуществления (потенциального ущерба).
  2. Определение требований к системе защиты информации в техническом задании на информационную систему.
  3. Разработка политики безопасности учебного заведения.

# ГЛАВА 1

## 1.1 Введение в информационную безопасность и систему защиты информации. Терминология.

Под информационной безопасностью обычно понимают состояние (свойство) защищенности ресурсов информационной системы в условиях наличия угроз в информационной сфере.

Защита информации - комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации [2].

Защищенность системы достигается обеспечением совокупности свойств ИБ ресурсов и инфраструктуры, основными из которых являются:

* конфиденциальность,
* целостность,
* доступность,
* подлинность,
* сохранность информации.

Конфиденциальность - требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь [2].

Целостность и подлинность - свойства, определяющее защищенность от несанкционированного изменения. Разделяют логическую и физическую целостность. Физическая целостность подразумевает неизменность физического состояния данных на машинном носителе. Логическая целостность отражает корректность выполнения процессов (транзакций), полноту и непротиворечивость информации, например, в СУБД, файловых системах, электронных архивах, хранилищах данных, системах управления документооборотом и т.д.

Доступность - свойство информации быть доступной за приемлемое время по запросу со стороны санкционированного субъекта [3]. С доступностью часто связывают такую характеристику системы как готовность - способность к выполнению заявленных функций в установленных технических условиях. Атаки, имеющие целью нарушить степень доступности, получили название атак на отказ в обслуживании (DOS-атаки).

Сохранность информации - свойство, предполагающее неизменность содержания информации и однозначность интерпретации в условиях случайных или преднамеренных воздействий в течение всего времени ее существования.

Определяющими факторами информационной безопасности являются угроза и риск [7].

Угрозой называют потенциальную причину (событие, нарушение, инцидент), снижающую уровень информационной безопасности системы, т.е. потенциально способную привести к негативным последствиям и ущербу системы или организации.

Риск представляет собой возможный ущерб, т.е. комбинацию (как правило, произведение) вероятности реализации угрозы и ущерба от нее. Отметим, что угроза и риск определяются не вообще, а относительно конкретного защищаемого ресурса.

В терминологии менеджмента бизнес-процессов вместо ресурса используется синонимическое понятие - актив, под определение которого подпадает все, что имеет ценность для организации. В информационной сфере примерами активов являются: информация, программное обеспечение, аппаратное обеспечение, информационная система (сложный актив, включающий предыдущие), человек, имидж организации. В итоге, активами представляются все те объекты, которые подлежат защите путем выстраивания процессов информационной безопасности.

Угрозы классифицируют по ряду критериев [7]:

* по причине возникновения (природные или техногенные, в том числе преднамеренные или случайные);
* по расположению источника (внешние или внутренние);
* по компрометируемой подсистеме или сегменту (сетевые, криптографические и др.);
* по этапу формирования в жизненном цикле системы (реализационные и эксплуатационные);
* по результирующему действию (нарушают целостность, конфиденциальность, доступность).

Рис. 1.1. Примеры угроз информационной безопасности

Довольно подробные каталоги угроз подготовлены немецким федеральным агентством по информационной безопасности (BSI).

Одной из основных угроз ИБ компьютерных систем является возможность реализации уязвимости в ресурсах системы. Под уязвимостью понимают реализационный дефект («слабость»), снижающий уровень защищенности ресурсов от тех или иных угроз. Отметим, наличие уязвимости становится угрозой, если ее можно реализовать так, что это приведет к недопустимому ущербу организации. Например, наличие сетевых уязвимостей в программном обеспечении изолированного компьютера не является угрозой.

Умышленная реализация уязвимостей в компьютерных системах, приводящая к ущербу организации, называется атакой на ресурсы.

Повышение и обеспечение заданных уровней конфиденциальности, целостности и доступности ресурсов осуществляется путем применения мер (механизмов) безопасности, которые на профессиональном жаргоне часто называются контролями (от. англ. слова controls - инструменты/средства управления). Очень важно не путать этот жаргонизм с привычным словом «контроль», имеющим другое значение: наблюдение за поведением управляемой системы с целью обеспечения ее оптимального функционирования.

Контроли могут иметь технический, организационный и физический характер. Под понятие «технические контроли» подпадают программные и программно-аппаратные средства защиты, такие как антивирусы, межсетевые экраны, системы обнаружения вторжений, средства шифрования данных и т. п. В качестве организационных контролей выступают правила, обязательные для исполнения сотрудниками. Например, наличие согласования заявки на предоставление доступа к системе у ее владельца (как правило, руководителя бизнес-подразделения, отвечающего за процессы, которые поддерживаются данной системой). Хорошими примерами физических контролей являются двери, решетки, заборы, ограничивающие физический доступ к нашим активам.

Контроли могут придерживаться различных целей, например, быть превентивными, детективными, корректирующими, восстанавливающими и другими. Более подробно контроли мы рассмотрим в следующей публикации, касающейся вопросов обеспечения безопасного доступа.

Применение различных видов и типов контролей тесно связано с концепцией эшелонированной обороны (defense in depth, multilevel security), представляющей идеологию проектирования систем защиты с несколькими уровнями мер (механизмов) безопасности, позволяющими обеспечить эффективную защиту даже в случае «пробивания» обороны на одном уровне.

Система защиты информации — это комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

## 1.2 Средства защиты информации

При осуществлении технической защиты информации используются средства технической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь [1].

Средства защиты информации – технические, программные, программно-аппаратные средства, предназначенные для защиты информации, а также средства контроля эффективности ее защищенности [11]

Техническое средство защиты информации – техническое устройство, специально изготовленное и (или) используемое для устранения или ослабления характерных признаков или физического проявления объекта защиты, которые определяются при помощи средств технической разведки и используются для получения информации, содержащей сведения, подлежащие защите, а также для создания помех техническим средствам разведки или специальным техническим средствам [11].

К техническим средствам защиты информации относятся: помехоподавляющие электрические фильтры, генераторы шума, излучающие сигналы различной физической природы (например, электрические, виброакустические) [11].

Техническое средство контроля защищенности информации – техническое устройство, специально изготовленное и (или) используемое для измерения количественных параметров, позволяющих оценить степень защищенности информации от ее утечки по техническим каналам.

К техническим средствам контроля защищенности информации относятся анализаторы спектра, шумомеры и иная электронная измерительная аппаратура.

Программными называются средства защиты информации, функционирующие в составе программного обеспечения.

Программно-аппаратные средства защиты информации – вся система обработки информации или часть ее физических компонентов с размещенными программами и данными. Программы при этом размещаются таким образом, чтобы их несанкционированное изменение было невозможным в ходе исполнения. Программы и данные, размещенные на ПЗУ с электронным программированием, допускающим стирание, рассматриваются как программное обеспечение [11].

К программным и программно-аппаратным средствам защиты информации относятся:

* средства криптографической защиты информации;
* антивирусные программы;
* средства идентификации и аутентификации пользователей;
* средства управления доступом;
* средства протоколирования и аудита и т.д.

Средства криптографической защиты информации – программные, программно-аппаратные средства защиты информации, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации.

На выпускаемые в обращение на территории Республики Беларусь средства защиты информации независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, распространяется действие технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (далее – технический регламент ТР 2013/027/BY), утвержденного постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375.

Средства защиты информации выпускаются в обращение на рынке в установленном порядке при их соответствии техническому регламенту ТР 2013/027/BY, а также другим техническим регламентам, действие которых на них распространяется.

Средства защиты информации, соответствие которых требованиям технического регламента ТР 2013/027/BY не подтверждено, не должны быть маркированы знаком соответствия техническому регламенту согласно ТКП 5.1.08-2012 «Национальная система подтверждения соответствия Республики Беларусь. Знаки соответствия. Описание и порядок применения» и не допускаются к выпуску в обращение на рынке.

Существует следующая классификация средств защиты информации:

* 1. Средства защиты от несанкционированного доступа

Мандатное управление доступом – разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

Избирательное управление доступом – управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

Управление доступом на основе ролей – развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

Журналирование – процесс записи информации о происходящих с каким-то объектом (или в рамках какого-то процесса) событиях в журнал (например, в файл). Также часто называется аудит.

1. Системы мониторинга сетей

Система обнаружения вторжений (СОВ) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

Системы предотвращения утечек конфиденциальной информации – технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

1. Анализаторы протоколов

Анализатор трафика, или – сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

1. Антивирусные средства

Антивирусная программа – любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики - предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

1. Межсетевые экраны

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача - не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

1. Криптографические средства
2. Системы бесперебойного питания

Источник бесперебойного питания (ИБП) – источник вторичного электропитания, автоматическое устройство, назначение которого обеспечить подключенное к нему электрооборудование бесперебойным снабжением электрической энергией в пределах нормы.

1. Системы аутентификации

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Аутентификацию не следует путать с идентификацией и авторизацией.

Один из способов аутентификации в компьютерной системе состоит во вводе вашего пользовательского идентификатора, в просторечии называемого «логином». Получив введенный пользователем логин и пароль, компьютер сравнивает их со значением, которое хранится в специальной базе данных и, в случае совпадения, пропускает пользователя в систему.

1. Системы резервного копирования

Системы резервного копирования – системы для осуществления процесса создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

## 1.3 Классификация объектов информатизации

Согласно пункту 9.2 приказа оперативно-аналитического центра при президенте РБ «О некоторых вопросах технической и криптографической защиты информации», №62 от 30.08.2013, одним из этапов проектирования системы защиты информации, является «присвоение информационной системе класса типового объекта информатизации» [1].

Класс типового объекта информатизации присваивается в соответствии с СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация»

Классификация объектов информатизации (ОИ) проводится применительно к типовым ОИ.

Типовой ОИ – объект, оснащенный типовым набором аппаратных, программных, аппаратно-программных средств, в том числе и средств защиты информации.

Классификация ОИ проводится по степени конфиденциальности [3]:

* Подкласс 1 – ОИ обрабатывающие и/или содержащие гос. секреты;
* Подкласс 2 – ОИ обрабатывающие и/или содержащие информацию, распространение и (или) предоставление которой ограничено, а также другую информацию охраняемую в соответствии с законодательством РБ;
* Подкласс 3 – ОИ, на которых обрабатывается открытая информация.

и по организации вычислительных процессов:

* Подкласс А – технические средства (ТС) ОИ размещены в пределах одной контролируемой зоны (КЗ), обработка информации осуществляется в пределах области действия комплекса средств безопасности объекта (КСБО);
* Подкласс Б – ТС ОИ размещены в нескольких КЗ, объединённых каналами передачи данных, обработка информации осуществляется в пределах КСБО;
* Подкласс В – ТС ОИ размещены в пределах одной КЗ, обработка информации осуществляется в пределах КСБО, но один или несколько объектов имеют каналы обмена информацией, выходящие за пределы КЗ.

В соответствии со стандартом могут быть следующие классы ОИ:

* Класс А1 — ТС ОИ размещены в пределах одной КЗ, в пределах области действия КСБО обрабатываются сведения, отнесенные к гос. секретам
* Класс А2 — ТС ОИ размещены в пределах одной КЗ, в пределах области действия КСБО обрабатывается служебная информация ограниченного распространения.
* Класс А3 — ТС ОИ размещены в пределах одной КЗ, в пределах области действия КСБО обрабатывается открытая информация.
* Класс Б1 — ТС ОИ размещены в нескольких КЗ, объединённых защищенными каналами передачи данных, в пределах области действия КСБО обрабатываются сведения, отнесенные к гос. секретам
* Класс Б2 — ТС ОИ размещены в нескольких КЗ, объединённых защищенными каналами передачи данных, в пределах области действия КСБО обрабатывается служебная информация ограниченного распространения
* Класс Б3 — ТС ОИ размещены в нескольких КЗ, объединённых каналами передачи данных, в пределах области действия КСБО обрабатывается открытая информация
* Класса В1 не должно существовать согласно действующего законодательства, так как объекты информатизации, обрабатывающие информацию, содержащую сведения, отнесенные в установленном порядке к государственным секретам, не должны иметь каналов обмена информацией за пределами контролируемой зоны.
* Класс В2 — для данного класса профиль защиты не разрабатывается, так как объекты информатизации, обрабатывающие служебную информацию ограниченного распространения, не должны иметь каналов обмена информацией за пределами контролируемой зоны;
* Класс В3 — ТС ОИ размещены в пределах одной КЗ, в пределах области действия КСБО обрабатывается открытая информация, один или несколько объектов имеют каналы обмена информацией, выходящие за пределы КЗ.

# ГЛАВА 2

# ПРОЕКТИРОВАНИЕ СЗИ

## 2.1 Анализ организационной структуры информационной системы

Понятие определение области применения системы защиты информации включает в себя следующие пункты [9]:

* описание вида деятельности и бизнес-целей организации;
* указание границ систем, охватываемых СЗИ;
* описание активов организации (виды информационных ресурсов, программно-технические средства, персонал и организационная структура);
* описание бизнес-процессов, использующих защищаемую информацию;

Как правило, на этом этапе составляется документ, в котором фиксируют границы информационной системы, перечисляют информационные ресурсы компании, подлежащие защите, приводят систему критериев и методики для оценки ценности информационных активов компании.

Учебное заведение – это учреждение, осуществляющее образовательный процесс, то есть реализующее одну или несколько образовательных программ и (или) обеспечивающее содержание и воспитание обучающихся, воспитанников.

Задачами учебного заведения являются:

1. развитие творческих, духовных и физических возможностей личности, формирование прочных основ нравственности и здорового образа жизни;
2. воспитание гражданственности и патриотизма, любви к Родине - Республике Беларусь, уважения к государственным символам, почитания народных традиций, нетерпимости к любым антиконституционным и антиобщественным проявлениям;
3. подготовка квалифицированных специалистов, конкурентоспособных на рынке труда, переподготовка и повышение их квалификации;
4. приобщение к достижениям мировой и отечественной культуры; изучение истории, обычаев и традиций белорусского и других народов республики;
5. овладение государственным, русским, иностранными языками;
6. внедрение новых технологий обучения, информатизация высшего профессионального образования, выход на международные глобальные коммуникационные сети.

Структура учебного заведения - возглавляет высшее учебное заведение ректор, его заместителями по различным направлениям работы являются проректоры, которые решают оперативные и тактические вопросы работы ВУЗа. Стратегические вопросы развития вуза обычно решает его Учёный совет.

Для упрощения понимая будем исходить из того что университет состоит из факультетов, а каждый отдельный факультет состоит из кафедр.

Рисунок 2.1 Организационная структура университета

Главным исполнительным органом кафедры является заведующий кафедрой, в его подчинении находятся заместитель кафедры, преподавательский состав, лаборатории вместе с сопутствующим персоналом и методисты.

Организационная структура кафедры университета представлена на рисунке 2.2.

Так же стоит отметить, что поскольку мы работаем с информационной системой класса Б2, то это система не имеет доступа в сети общего пользования.

Рисунок 2.2 Организационная структура кафедры университета.

## 2.2 Классификация информации, хранящийся и обрабатываемой в информационной системе

Из-за того, что учебное заведение — это достаточно большое предприятие оно имеет достаточно много информации, хранящейся и обрабатываемом в ИС, некоторые из них:

* персональные данные студентов;
* личные данные сотрудников;
* научно-исследовательские работы;
* сведения об успеваемости;
* экзаменационные билеты;
* нагрузка преподавателей.

Все эта информации является информацией ограниченного распространения и должна быть защищена.

Так же в ИС учебного заведения имеется общедоступная информация, так как:

* расписание занятий;
* учебные планы;
* общая информация о работниках;
* новости;
* методические рекомендации по написанию курсовых, дипломных работ.

## 2.3 Проведение оценки угроз и рисков для ИС

Риск информационной безопасности – это потенциальная возможность понести убытки из-за нарушения безопасности информационной системы [10].

Риск может быть охарактеризован следующим набором параметров:

* угроза, возможной реализацией которой вызван данный риск;
* ресурс, в отношении которого может быть реализована данная угроза;
* уязвимость, через которую может быть реализована данная угроза в отношении данного ресурса.

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Уязвимость – это так называемое "слабое место" в системе защиты информации, которое является основанием для возникновения угрозы со стороны злоумышленников.

Любая хорошо продуманная методология оценки рисков информационной безопасности предусматривает такие шаги, как [8]:

* выявление угроз, направленных на рассматриваемые активы;
* определение последствий от реализации угроз;
* выявление уязвимостей;
* выявление существующих контролей (контрмер);
* определение вероятности реализации угроз.

И всего вышеперечисленного видно, что шаги методики определяются, исходя из определения понятия риска.

До применения каких-либо шагов по оценке рисков, мы должны определить критерии для их оценки. Один из подходов, позволяющих определить критерии для оценки последствий, заключается в том, чтобы оттолкнуться от целей, которые мы ставим перед информационной безопасностью. Защитой информации мы занимаемся для того, чтобы минимизировать финансовые потери, сохранить или даже улучшить положение кафедры на факультете.

|  |  |  |
| --- | --- | --- |
| Уровень последствия | Финансовые потери | Положение кафедры на факультете |
| Высокий (В) | Значительные | Заметно ухудшиться, вплоть до расформирования кафедры |
| Средний (С) | Средние | Ухудшиться, возможно, будут кадровые изменения |
| Низкий (Н) | Незначительные | Практически не ухудшиться, ответственные лица получат выговоры |

Таблица 2.1 Классификация последствий

Для оценки вероятности реализации ограничимся следующими критериями: имеющаяся статистика по аналогичным инцидентам, требуемые затраты на реализацию угрозы и возможность обнаружения.

|  |  |  |  |
| --- | --- | --- | --- |
| Вероятность | Статистика инцидентов | Затраты на реализацию угрозы | Возможность обнаружения |
| Высокая (В) | Аналогичный инцидент происходит в учебном заведении каждую неделю. | Интеллектуальные:  невысокая квалификация злоумышленника.  Инструменты для реализации угрозы общедоступны. | Угрозу и ее источник очень сложно обнаружить. |
| Средняя (С) | Аналогичный инцидент происходит в учебном заведении каждый месяц. | Интеллектуальные:  средняя квалификация злоумышленника.  Инструменты для реализации угрозы можно приобрести или создать за разумный срок. | Угрозу и ее источник можно вычислить, но для этого потребуются серьезные усилия. |
| Низкая (Н) | Аналогичный инцидент происходит в учебном заведении каждый год. | Интеллектуальные:  высокая квалификация злоумышленника.  Инструменты для реализации угрозы на данный момент не доступны. | Угроза и ее источник легко обнаруживается. |

Таблица 2.2 Оценка вероятностей реализации угроз

Исходя из таблицы вероятностей и таблицы последствий можно создать таблицу, в которой сопоставить вероятность реализации угрозы с размерами ее последствий и получить значения рисков.

|  |  |  |  |
| --- | --- | --- | --- |
| Последствия  Вероятность | Н | С | В |
| Н | Н | Н | С |
| С | Н | С | В |
| В | С | В | В |

Таблица 2.3 Значение рисков

После того, как критерии определены, которые будем использовать для оценки рисков, в соответствии с требованиями СТБ 34.101.2 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.», необходимо идентифицировать угрозы и, соответственно, риски [4].

|  |  |
| --- | --- |
| Виды информации | Угроза |
| персональные данные студентов | * хищение * уничтожение * модификация |
| личные данные сотрудников | * хищение * уничтожение * модификация |
| научно-исследовательские работы | * копирование |
| сведения об успеваемости | * модификация |
| экзаменационные билеты; | * разглашение * модификация |
| нагрузка преподавателей | * модификация |

Таблица 2.4 Угрозы для исследуемых видов информации

## 2.4 Разработка технического задания

Техническое задание устанавливает основное назначение разрабатываемого объекта, его технические и тактико-технические характеристики, показатели качества и технико-экономические требования, предписание по выполнению необходимых стадий создания документации (конструкторской, технологической, программной и т. д.) и её состав, а также специальные требования.

Техническое задание на систему защиты информации строиться по следующему плану:

1. Общие сведения
2. Назначения и цели создания системы
3. Требования к системе защиты информации
4. Требования к средствам зашиты
5. Порядок контроля и приёмки системы

## 2.5 Техническое задание на систему защиты информации

**1. Общие сведения**

Настоящее Техническое задание разработано в соответствии с приказом №62 «О некоторых вопросах технической и криптографической защиты информации» оперативно-аналитического центра при президенте Республики Беларусь и является основным документом, определяющим требования и порядок создания, развития, модернизации, сопровождения Системы защиты информации информационной системы класс Б2.

Результатом создания системы защиты информации информационной системы класс Б2 должна стать полностью работоспособная автоматизированная система защиты информации информационной системы класса Б2, соответствующая требованиям настоящего технического задания.

**1.1 Полное наименование системы**

Полное наименование системы – «Система защиты информации информационной системы класс Б2».

**1.2 Наименование реквизитов разработчика и заказчика СЗИ.**

Заказчик: *НАЗВАНИЕ УНИВЕРСИТЕТА*. Адрес: *АДРЕС УНИВЕРСИТЕТА*.

Исполнитель: *НАЗВАНИЕ ФИРМЫ* Адрес: *АДРЕС ФИРМЫ.*

**1.3 Перечень документов, на основании которых создаётся СЗИ.**

Для формирования требований были использованы документы, разработанные на предыдущих этапах создания СЗИ, которые приведены в таблице 1.

Таблица 1. Документы, разработанные на предыдущих этапах создания СЗИ

|  |  |
| --- | --- |
| № п/п | Наименование документа |
| 1 | Классификация информации, хранящейся и обрабатываемой в информационной системе, в соответствии с законодательством об информации, информатизации и защите информации, в том числе техническими нормативными правовыми актами; |
| 2 | Акт классификации системы защиты информации |

Основные руководящие и нормативно – технические документы приведены в таблице 2.

Таблица 2. Перечень основных руководящих и нормативно технических документов.

|  |  |
| --- | --- |
| № п/п | Наименование документа |
|  | СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель». |
|  | СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности». |
|  | СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности». |
|  | СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования». |
|  | СТБ 34.101.28-2011 «Информационные технологии. Средства защиты речевой информации от утечки по акустическому и виброакустическому каналам. Общие технические требования» |
|  | СТБ 34.101.29-2011 «Информационные технологии. Средства контроля защищенности речевой информации. Общие технические требования» |
|  | СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация». |

Плановые сроки начала и окончания работ по созданию системы защиты информации:

Начало работ – 01 декабря 2016 года. Окончание работ – 01 апреля 2017 года.

**2. Назначение и цели создания системы**

**2.1 Назначение системы защиты.**

СЗИпредназначена для сотрудников Белорусского государственного университета.

**2.1 Цели создания системы защиты**

Целями создания системы защиты является защита информации кафедры телекоммуникаций и информационных технологий факультета Радиофизики и компьютерных технологий БГУ.

Критерием оценки достижения целей создания системы является снижение величины наносимого ущерба вследствие реализации угроз безопасности, путём применения технических, организационных мер, надлежащее выполнение требований безопасности, предусмотренных нормативно-методическими документами.

**2.2 Краткая характеристика информационной системы, структура**.

Информационная система представляет из себя кафедру высшего учебного заведения.

**2.3 Размещение СЗИ*.***

СЗИ будет расположена по адресу *АДРЕС*.

**2.4 Охрана и пропускной режим.**

На объекте, на котором планируется внедрить систему защиты информации осуществляется контрольно-пропускной режим. Так же вход и выход с объекта ограничен с 23:00 до 7:00.

**2.5 Контролируемая зона.**

Контролируемая зона представлена в виде периметра стен помещений, располагающихся на 1 этаже учебного корпуса.

**2.6 Схема информационного взаимодействия объектов в ИС.**

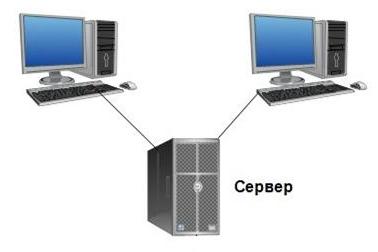


Рисунок 3.1. Схема информационного взаимодействия объектов.

Информационная система не имеет выхода в сети общего пользования.

**2.7. Частная модель угроз безопасности в ИС**

* разглашение экзаменационных билетов;
* изменение экзаменационных билетов;
* хищение персональных данных студентов;
* уничтожение персональных данных студентов;
* модификация персональных данных студентов;
* модификация сведений об успеваемости;
* хищение личных данных сотрудников;
* уничтожение личных данных сотрудников;
* модификация личных данных сотрудников;
* изменение нагрузки преподавателей;
* изменение часовой оплаты занятий;
* копирование научно-исследовательская работ.

**3 Требования к системе защиты информации ИС**

**3.1 Требования к функциям (задачам), выполняемым системой.**

* Идентификация объектов информационной системы (далее – объекты) и закрепление за ними субъектов информационной системы (далее – субъекты)
* Идентификация и аутентификация субъектов
* Управление идентификаторами, в том числе создание, присвоение, уничтожение
* Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
* Исключение отображения аутентификационной информации
* Изменение атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности
* Полномочное управление (создание, активация, блокировка и уничтожение) учетными записями субъектов
* Определение прав и обязанностей субъектов
* Реализация правил разграничения доступа субъектов к объектам
* Блокирование доступа к информационной системе после истечения установленного времени бездействия (неактивности) субъекта или по его запросу
* Определение при необходимости действий субъектов, которые могут совершаться такими субъектами до их идентификации и аутентификации
* Наличие актуальной схемы сети с указанием объектов, внешних подключений и информационных потоков
* Управление (фильтрация, маршрутизация, контроль соединений) информационными потоками между объектами, а также между информационными системами
* Ограничение входящего и исходящего трафика только необходимыми соединениями
* Запрет на использование в информационной системе технологий беспроводного доступа
* Регламентация порядка использования в информационной системе мобильных технических средств и контроля за таким использованием
* Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования
* Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования
* Регламентация доступа к учтенным машинным носителям информации
* Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на учтенных машинных носителях информации
* Уничтожение (удаление) данных с машинных носителей информации при их передаче лицам, не являющимся субъектами информационной системы, в том числе для ремонта, технического обслуживания
* Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
* Сбор, запись и хранение информации о событиях безопасности в течение установленного срока хранения
* Мониторинг (просмотр, анализ) событий безопасности уполномоченными субъектами
* Сбор, запись и хранение, а также мониторинг (просмотр, анализ) информации о сбоях в механизмах сбора информации и достижении предела объема (емкости) памяти устройств хранения уполномоченными пользователями
* Синхронизация временных меток и (или) системного времени в информационной системе
* Защита информации о событиях безопасности
* Защита информации о событиях безопасности
* Регламентация обновления базы данных признаков вредоносного программного обеспечения
* Регламентация проведения проверок операционных систем на предмет обнаружения аномалий, вызванных присутствием в системе вредоносного программного обеспечения
* Выявление уязвимостей информационной системы и оперативное их устранение
* Контроль за установкой обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
* Контроль за работоспособностью, параметрами настройки и правильностью функционирования программного обеспечения и средств защиты информации
* Контроль за работоспособностью, параметрами настройки и правильностью функционирования программного обеспечения и средств защиты информации
* Регламентирование порядка резервирования информации и программного обеспечения, включая программное обеспечение средств защиты информации
* Идентификация и аутентификация субъектов и объектов в виртуальной инфраструктуре, в том числе уполномоченных пользователей по управлению средствами виртуализации
* Управление доступом субъектов к объектам в виртуальной инфраструктуре, в том числе внутри виртуальных машин
* Установление контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации
* Контроль и управление физическим доступом внутри контролируемой зоны к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они размещены (установлены), исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, а также в помещения и сооружения, в которых они установлены.

**4. Требования к средствам защиты.**

При осуществлении технической защиты информации используются средства технической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь

**4.1 Требования по электрической и пожарной безопасности**

Технические средства, применяемые для реализации приведённых выше требований должны соответствовать нормам по электрической и пожарной безопасности, принятым на предприятии заказчика.

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование.

**4.2 Требования по эксплуатации и техническому обслуживанию**

Для нормальной эксплуатации разрабатываемой системы должно быть обеспечено бесперебойное питание ПЭВМ. При эксплуатации система должна быть обеспечена соответствующая стандартам хранения носителей и эксплуатации ПЭВМ температура и влажность воздуха. Размещение помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств. Размещение оборудования, технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности. Все пользователи системы должны соблюдать правила эксплуатации электронной вычислительной техники. Периодическое техническое обслуживание используемых технических средств должно проводиться в соответствии с требованиями технической документации изготовителей, но не реже одного раза в год.

Квалификация персонала и его подготовка должны соответствовать технической документации.

**4.3 Требования к патентной чистоте**

По всем техническим и программным средствам, применяемым в системе, должны соблюдаться условия лицензионных соглашений и обеспечиваться патентная чистота на территории Республики Беларусь.

Патентная чистота – это юридическое свойство объекта, заключающиеся в том, что он может быть свободно использован в Республике Беларусь без опасности нарушения действующих на ее территории патентов исключительного права, принадлежащего третьим лицам (права промышленной собственности).

**4.4 Требования к эргономике и технической эстетике**

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав системы должно осуществляться посредством визуального графического интерфейса (GUI). Интерфейс системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной системы. Ввод-вывод данных системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям системы. Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен используется главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм. Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке.

**4.5 Требования к составу и содержанию работ по созданию системы защиты информации персональных данных.**

Этапы работы по созданию СЗИ отражены в таблице 4.

Таблица 4.

| Этап | Содержание работ\* | Результаты работ |
| --- | --- | --- |
| 1 | Классификация информации, хранящейся и обрабатываемой в информационной системе, в соответствии с законодательством об информации, информатизации и защите информации, в том числе техническими нормативными правовыми актами. |  |
| 2 | Анализ организационной структуры информационной системы и информационных потоков в целях определения состава (количества) и мест размещения элементов системы (аппаратных и программных), ее физических и логических границ. |  |
| 3 | Присвоение информационной системе класса типового объекта информатизации в порядке, установленном СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация». |  |
| 4 | Определение требований к системе защиты информации в техническом задании на информационную систему. | Техническое задание |
| 5 | Согласование технического проекта.  Разработанный технический проект отправляется на ознакомление и согласование заказчику. В ходе этого этапа могут быть внесены дополнения и изменения в проект, если это потребуется. Итогом согласования проекта является подписание его сторонами. |  |
| 6 | Разработка политики информационной безопасности. | Политика безопасности |
| 7 | Внедрение планируемых к использованию средств защиты информации, проверка их работоспособности и совместимости. | В ходе внедрения средств защиты информации осуществляется их монтаж и наладка в соответствии с эксплуатационной документацией. |
| 8 | Внедрение организационных мер защиты информации осуществляется в целях реализации требований, изложенных в локальных нормативных правовых актах организации, которые доводятся до сведения субъектов информационной системы под подпись. |  |
| 9 | Опытная эксплуатация системы защиты информации. | Опытная эксплуатация системы защиты информации осуществляется для проверки ее работоспособности в различных режимах функционирования информационной системы, в том числе при необходимости в условиях чрезвычайной ситуации. В случае выявления в процессе опытной эксплуатации системы защиты информации недостатков осуществляется их устранение с последующей повторной опытной эксплуатацией. |
| 10 | Приемочные испытания системы защиты информации. | Приемочные испытания системы защиты информации проводятся в целях проверки выполнения требований к системе защиты информации, изложенных в задании по безопасности или в техническом задании. |
| 11 | Аттестация СЗИ. | Аттестат соответствия. Наличие аттестата соответствия является основанием для ввода информационной системы в эксплуатацию и использования ее в течение срока, установленного в аттестате соответствия. |
| 12 | Ввод системы в эксплуатацию. | Акт ввода системы в промышленную эксплуатацию. |

**4.6 Требования к разработчику системы защиты**

Привлекаемый на договорной основе разработчик (юридическое лицо или индивидуальный предприниматель) должен иметь лицензию(ии) на деятельность по технической и (или) криптографической защите информации выдаваемую оперативно-аналитическим центром при Президенте Республики Беларусь.

**5. Порядок контроля и приёмки системы**

**5.1 Порядок проведения приёмки**

Испытания СЗИ проводятся на объекте заказчика;

Испытания могут проводиться с целью проверки как отдельной подсистемы или функционального модуля, так и на СЗИ в целом.

На основании решения о приемке осуществляется подписание комиссией акта приемки;

Опытная эксплуатация системы защиты выполняется на развернутом и настроенном рабочем месте, на котором потом будет осуществляться дальнейшая промышленная эксплуатация.

# ГЛАВА 3

# СОЗДАНИЕ СЗИ

## 3.1 Разработка политики безопасности

В соответствии с Приказом оперативно-аналитического центра при Президенте Республики Беларусь №62 «О некоторых вопросах технической и криптографической защиты информации» на этапе создания системы защиты информации осуществляются разработка политики информационной безопасности [1].

Политика безопасности – совокупность правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности [5].

Организация может иметь несколько политик, по одной для каждой сферы деятельности, важной для организации. Некоторые политики независимы между собой, в то время как другие политики находятся в иерархическом соотношении. В области безопасности политики, как правило, иерархически организованы. Обычно политика безопасности является политикой высшего уровня. В свою очередь, политика информационной безопасности может подкрепляться более детальными политиками по конкретным предметам, такими как: политика контроля доступа, политики «чистого стола» и «чистого экрана», политика использования сетевых служб и д. р [6].

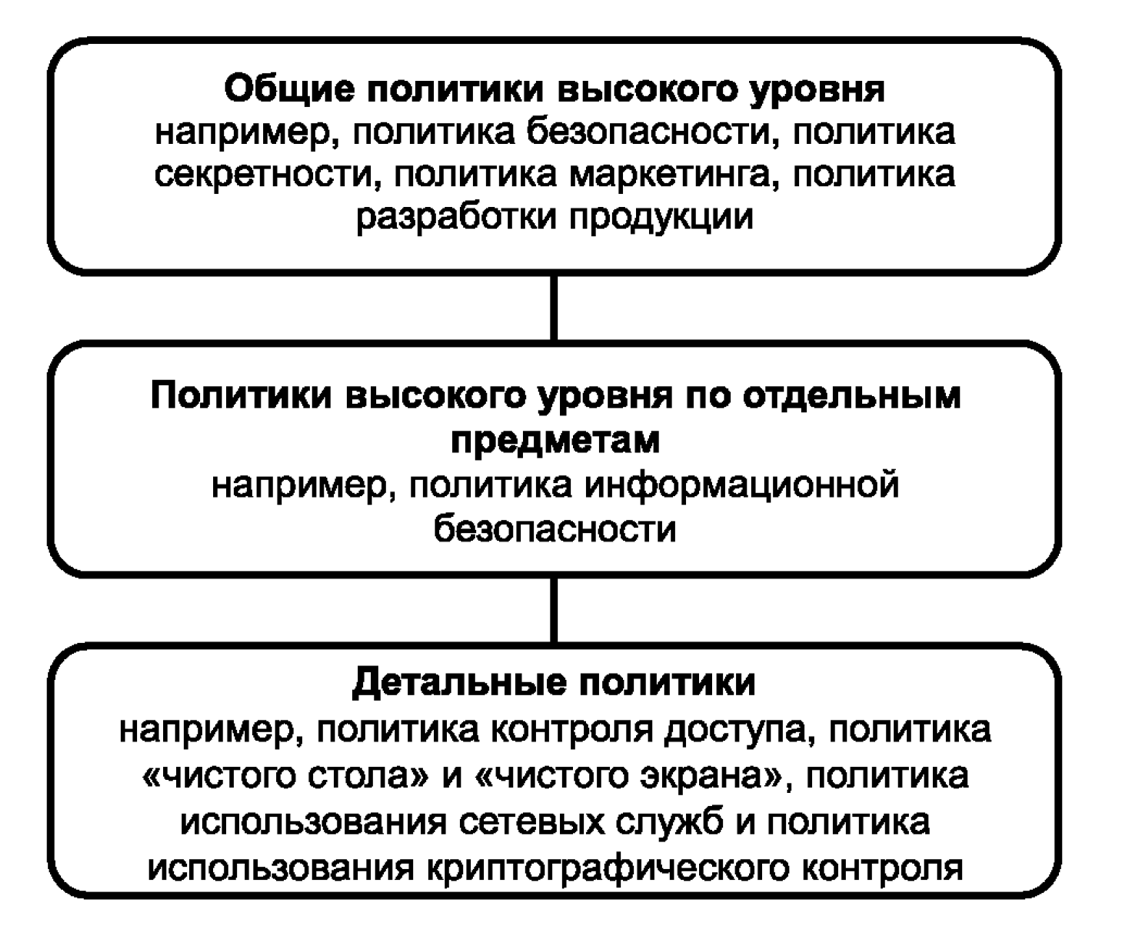


Рис 3.1 Иерархия политик

Содержание политики основано на контексте, в котором работает организация. Однако Приказом оперативно-аналитического центра при Президенте Республики Беларусь №62 «О некоторых вопросах технической и криптографической защиты информации» выделяется перечень пунктов, которые должна содержать политика [1]:

* цели создания системы защиты информации;
* перечень субъектов и объектов информационной системы, сведения о месте их размещения и порядке информационного взаимодействия субъектов с объектами этой системы и объектов между собой;
* способы разграничения доступа субъектов к объектам информационной системы;
* права и обязанности субъектов информационной системы;
* порядок взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия);
* перечень организационных мер, направленных на реализацию требований по созданию системы защиты информации;
* порядок действий при возникновении угроз обеспечения конфиденциальности, целостности, доступности, подлинности и сохранности информации, в том числе чрезвычайных и непредотвратимых обстоятельств (непреодолимой силы), и при ликвидации их последствий.

## 3.2 Политика безопасности

**1. Краткое изложение политики**

Информация всегда должна быть защищена не зависимо от её формы и её способа распространения, передачи и хранения.

**2. Введение**

1. Настоящая Политика разработана в соответствии с законодательством Республики Беларусь и нормами права в части обеспечения информационной безопасности, и основывается в том числе на:

* международном стандарте ISO/IEC 27002 «Информационные технологии - Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью»;
* приказе оперативно-аналитического центра при Президенте Республики Беларусь № 62 «О некоторых вопросах технической и криптографической защиты информации».

1. Настоящая Политика является документом, доступным любому сотруднику университета и пользователю его ресурсов, и представляет собой официально принятую руководством НАЗВАНИЕ УНИВЕРСИТЕТА (далее – Университет) систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Университета.
2. Руководство Университета осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования образовательной деятельности, а также развития реализуемых университетом технологий и ожиданий сотрудников, студентов и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества Университету, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.
3. Требования информационной безопасности, которые предъявляются Университетом, соответствуют интересам (целям) деятельности Университета и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Университета имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности. Факторы рисков в информационной сфере Университета составляют значимую часть операционных рисков Университета, а также имеют отношение и к иным рискам основной и управленческой деятельности Университета.
4. Необходимые требования обеспечения информационной безопасности Университета должны неукоснительно соблюдаться персоналом Университета и другими сторонами как это определяется положениями внутренних нормативных документов Университета, а также требованиями договоров и соглашений, стороной которых является Университет.
5. Настоящая Политика распространяется на бизнес - процессы Университета и обязательна для применения всеми сотрудниками и руководством Университета, а также пользователями его информационных ресурсов.
6. Положения настоящей Политики должны быть учтены при разработке политик информационной безопасности в дочерних и аффилированных организациях.
7. Настоящая Политика является корпоративным документом по ИБ первого уровня.
8. Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Университета, являются частные политики по обеспечению ИБ (далее – Частные политики), которые являются документами по ИБ второго уровня, оформляются как отдельные внутренние нормативные документы Университета, разрабатываются и согласовываются в соответствии с установленным в Университете порядком, утверждаются Куратором.

**3. Область действия**

Основными объектами защиты системы информационной безопасности в Университете являются:

* + информационные ресурсы, содержащие коммерческую тайну, персональные данные физических лиц, информация ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Университета, независимо от формы и вида ее представления;
  + сотрудники Университета, являющиеся разработчиками и пользователями информационных систем Университета;
  + информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

**4. Цели информационной безопасности**

Целью деятельности по обеспечению информационной безопасности Университета является снижение угроз информационной безопасности до приемлемого для Университета уровня.

Основные задачи деятельности по обеспечению информационной безопасности Университета:

* выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
* предотвращение инцидентов информационной безопасности;
* исключение либо минимизация выявленных угроз.

**5. Принципы информационной безопасности**

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

1. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Университета и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

1. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

1. Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

1. Источники угроз по отношению к инфраструктуре Университета могут быть как внешними, так и внутренними.
2. По отношению к Университету нарушители могут быть разделены на внешних и внутренних нарушителей.

Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Университетом рассматриваются:

* зарегистрированные пользователи информационных систем Университета;
* сотрудники Университета, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Университета, но имеющие доступ в здания и помещения;
* персонал, обслуживающий технические средства корпоративной информационной системы Университета;
* сотрудники самостоятельных структурных подразделений Университета, задействованные в разработке и сопровождении программного обеспечения;
* сотрудники самостоятельных структурных подразделений, обеспечивающие безопасность Университета;
* руководители различных уровней.

1. Внешние нарушители.

В качестве потенциальных внешних нарушителей Университетом рассматриваются:

* бывшие сотрудники Университета;
* представители организаций, взаимодействующих по вопросам технического обеспечения Университета;
* клиенты Университета;
* посетители зданий и помещений Университета;
* конкурирующие с Университета образовательные организации;
* члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию.

1. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

* нарушитель скрывает свои несанкционированные действия от других сотрудников Университета;
* несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
* в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
  + внешний нарушитель может действовать в сговоре с внутренним нарушителем.

1. Требования об обеспечении информационной безопасности Университета обязательны к соблюдению всеми работниками Университета и пользователями информационных систем.
2. Руководство Университета приветствует и поощряет в установленном порядке деятельность работников Университета и пользователей информационных систем по обеспечению информационной безопасности.
3. Неисполнение или некачественное исполнение сотрудниками Университета и пользователями информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Университете порядком либо требованиями действующего законодательства.
4. Стратегия Университета в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Университета, до специализированных мер информационной безопасности по каждому выявленному в Университете риску, основанных на оценке рисков информационной безопасности.
5. При планировании мероприятий по обеспечению информационной безопасности в Университете осуществляются:
6. Определение и распределение ролей персонала Университета, связанного с обеспечением информационной безопасности (ролей информационной безопасности).
7. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.
8. Менеджмент рисков информационной безопасности, включающий:

* анализ влияния на информационную безопасность Университета применяемых в деятельности Университета технологий, а также внешних по отношению к Университету событий;
* выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
* определение моделей угроз информационной безопасности;
* выявление, анализ и оценка значимых для Университета угроз информационной безопасности;
* выявление возможных негативных последствий для Университета, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Университета;
* идентификацию и анализ рисковых событий информационной безопасности;
* оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для Университета;
* обработку результатов оценки рисков информационной безопасности, базирующейся на методах управления операционными рисками, определенных в Университете;
* оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Университета в случае наступления рисковых событий;
* оценку влияния защитных мер на цели основной деятельности Университета;
* оценку затрат на реализацию защитных мер;
* рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;
* разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Университета и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;
* документальное оформление целей и задач обеспечения информационной безопасности Университета, поддержка в актуальном состоянии нормативно – методического обеспечения деятельности в сфере информационной безопасности.

1. В рамках реализации деятельности по обеспечению информационной безопасности в Университете осуществляются:
2. Менеджмент инцидентов информационной безопасности, включающий:

* сбор информации о событиях информационной безопасности;
* выявление и анализ инцидентов информационной безопасности;
* расследование инцидентов информационной безопасности;
* оперативное реагирование на инцидент информационной безопасности;
* минимизация негативных последствий инцидентов информационной безопасности;
* оперативное доведение до руководства Университета информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
* выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
* пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
* повышение уровня знаний персонала Университета в вопросах обеспечения информационной безопасности;
* обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Университета и информации, обрабатываемой в них;
* применение средств криптографической защиты информации;
* обеспечение бесперебойной работы автоматизированных систем и сетей связи;
* обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
* применение средств защиты от вредоносных программ;
* обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем Университета, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);
* контроль доступа в здания и помещения Университета.

1. Обеспечение защиты информации от утечки по техническим каналам, включающее:

* применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;
* применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита;
* применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

1. В целях проверки деятельности по обеспечению информационной безопасности в Университете осуществляются:

* контроль правильности реализации и эксплуатации защитных мер;
* контроль изменений конфигурации систем и подсистем Университета;
* мониторинг факторов рисков и соответствующий их пересмотр;
* контроль реализации и исполнения требований сотрудниками Университета действующих внутренних нормативных документов по обеспечению информационной безопасности Университета;
* контроль деятельности сотрудников и других пользователей информационных систем Университета, направленный на выявление и предотвращение конфликтов интересов.

1. В целях совершенствования деятельности по обеспечению информационной безопасности в Университете осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Университета).
2. В целях выполнения задач по обеспечению информационной безопасности Университета, в соответствии с рекомендациями международных стандартов по безопасности в Университете должны быть определены следующие роли:

* Куратор;
* Ответственное подразделение;
* Сотрудник Университета.

При необходимости могут быть определены и другие роли по информационной безопасности.

1. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Университета осуществляются и координируются Ответственным подразделением. Задачами Ответственного подразделения являются:
   * установление потребностей Университета в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
   * соблюдение действующего законодательства, нормативных актов органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, нормативных актов по обеспечению информационной безопасности;
   * разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Университета, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;
   * осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Университета;
   * обучение, контроль и непосредственная работа с персоналом Университета в области обеспечения информационной безопасности;
   * планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Университете;
   * выявление и предотвращение реализации угроз информационной безопасности;
   * выявление и реагирование на инциденты информационной безопасности;
   * информирование в установленном порядке ответственных лиц об угрозах и рисковых событиях информационной безопасности;
   * прогнозирование и предупреждение инцидентов информационной безопасности;
   * пресечение несанкционированных действий нарушителей информационной безопасности;
   * поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение персонала;
   * типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на филиалы и представительства Университета;
   * обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;
   * мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности Университета;

* контроль обеспечения информационной безопасности Университета, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;
* информирование руководства Университета и руководителей его самостоятельных структурных подразделений Университета об угрозах информационной безопасности, влияющих на деятельность Университета.

1. Ответственное подразделение может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые сотрудником Ответственного подразделения, и может, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, привлекать для работы в них сотрудников других самостоятельных структурных подразделений Университета на основе совмещения работы в группе со своими основными должностными обязанностями.
2. Финансирование работ по реализации положений настоящей Политики осуществляется как в рамках целевого бюджета Ответственного подразделения Университета, так и в рамках бюджетов бизнес - подразделений и подразделений ИТ-блока.
3. Основными функциями Куратора в вопросах информационной безопасности являются:

* назначение ответственных лиц в области ИБ,
* координация и внедрение информационной безопасности в Университете.

1. Основными задачами работников Университета при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности Университета являются:

* соблюдение требований информационной безопасности, устанавливаемых нормативными документами Университета;
* выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;
* выявление и реагирование на инциденты информационной безопасности;
* информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковых событиях информационной безопасности;
* прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;
* мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;
* информирование своего руководства и Ответственного подразделения о выявленной угрозе в информационной среде Университета.

**6. Сферы ответственности**

Общее руководство обеспечением информационной безопасности Университета осуществляет Куратор.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы обеспечения информационной безопасности Университета лежит на руководстве Ответственного подразделения.

Ответственность работников Университета за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками Университета, а также положениями внутренних нормативных документов Университета.

**7. Ключевые результаты**

1. Инциденты информационной безопасности не должны приводить серьёзным непредвиденным затратам или серьёзным срывам работы служб и деятельности Университета.
2. Потери из-за мошенничества должны быть известны и находится в рамках приемлемых ограничений.
3. Вопросы информационной безопасности не должны оказывать неблагоприятного влияния на учебный процесс или деятельность Университета.

# ЗАКЛЮЧЕНИЕ

В ходе работы над проектом были изучены базовые положения о информационной безопасности и системам защиты информации. Также были проанализирован набор стандартов СТБ 34.101 и приказ №62 оперативно-аналитического центра при президенте РБ «О некоторых вопросах технической и криптографической защиты информации».

На основании полученных знаний, было произведена разработка СЗИ:

* произведена классификация информации, хранящейся и обрабатываемой в информационной системе, в соответствии с законодательством об информации, информатизации и защите информации, в том числе техническими нормативными правовыми актами;
* определен подход к оценке рисков для учебного заведения;
* выявлены риски;
* проанализирована организационная структура информационной системы;
* разработано техническое задание на систему защиты информации;
* разработана политика безопасности для Университета.

Стоит отметить, что этап разработки СЗИ ещё не был завершён, поскольку он, кроме разработки политики безопасности, предполагает:

* внедрение планируемых к использованию средств защиты информации, проверка их работоспособности и совместимости;
* внедрение организационных мер по защите информации;
* опытная эксплуатация системы защиты информации;
* приемочные испытания системы защиты информации.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. О некоторых вопросах технической и криптографической защиты информации : Приказ оперативно-аналитического центра при президенте Республики Беларусь от 30 августа 2013 г. № 62
2. Об информации, информатизации и защите информации : Закон Республики Беларусь от 10 ноября 2008 г. № 455-З.
3. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация : СТБ 34.101.30-2007. – Минск : Белорус. гос. ин-т стандартизации и сертификации, 2007.
4. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. : СТБ 34.101.2-2014. – Минск : Белорус. гос. ин-т стандартизации и сертификации, 2014.
5. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности: учеб. пособие / Родичев Ю. А. – Ростов н/Д: «Издательский дом «Питер»», 2016 – 256 с.
6. ГОСТ Р ИСО/МЭК 27003-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности»
7. Дорофеев Александр Владимирович, Марков Алексей Сергеевич Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. №1 (2) С.67-73.
8. Дорофеев Александр Владимирович Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. №2 (3) С.66-73.
9. Создание системы менеджмента информационной безопасности (СМИБ) - Информационная безопасность [Электронный ресурс] – Режим доступа: http://itsec.by/sozdanie-sistemy-menedzhmenta-informacionnoj-bezopasnosti-smib/ ‑ Дата доступа: 25.12.2016
10. ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
11. Общие сведения [Электронный ресурс] – Режим доступа: http://oac.gov.by/tzi/protection/comments.html ‑ Дата доступа: 25.12.2016