**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

**Кафедра телекоммуникаций и информационных технологий**

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

Курсовая работа

Радкевича Владислава Игоревича

студента 4 курса,

специальность

«Компьютерная безопасность»

Руководитель:  
к.т.н., доцент

Г.К. Резников

Минск, 2016

Оглавление

[ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ 3](#_Toc484523860)

[ВВЕДЕНИЕ 4](#_Toc484523861)

[Глава 1 6](#_Toc484523862)

[ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ И СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ. ТЕРМИНОЛОГИЯ. 6](#_Toc484523863)

[СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. 10](#_Toc484523864)

[КЛАССФИКАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ 14](#_Toc484523865)

[**Глава 2** 16](#_Toc484523866)

[ПЛАНИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ 16](#_Toc484523867)

[2.1 Определение объектов ИС подлежащих защите 16](#_Toc484523868)

[2.2 Выявление потенциальных угроз и каналов утечки информации 17](#_Toc484523869)

[2.3 Проведение оценки угроз и рисков для ИС 18](#_Toc484523870)

[**Глава 3** 22](#_Toc484523871)

[Проектирование СЗИ. 22](#_Toc484523872)

[3.1 Разработка технического задания 22](#_Toc484523873)

[3.2 Техническое задание на систему защиты информации 22](#_Toc484523874)

[Глава 4 32](#_Toc484523875)

[ЗАКЛЮЧЕНИЕ 33](#_Toc484523876)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 34](#_Toc484523877)

# ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

ИБ – информационная безопасность

ИС – информационная система

ОИ – объектов информатизации

ТС – технические средства

КЗ – контролируемая зона

КСБО – комплекс средств безопасности объекта

НСД – несанкционированный доступ

СОВ – система обнаружения вторжений

ИБП – источник бесперебойного питания

# 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 – проектирование 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.

# Глава 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.

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.

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 - характеристика, определяющая возможность за приемлемое время получить требуемую информационную услугу авторизованному пользователю. 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.

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:

* 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.

# 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.

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

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.

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

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.

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.

# КЛАССФИКАЦИЯ 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».

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:

* 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
* Классов В1 и В2 не должно существовать согласно действующего законодательства.
* 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**

# ПЛАНИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 2.1 Определение объектов ИС подлежащих защите

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

* 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.

Учебное заведение состоит из факультетов, факультеты из кафедр. В штат ВУЗов входят профессора, доценты, старшие преподаватели, преподаватели, ассистенты, учебно-вспомогательный персо­нал, научные сотрудники, аспиранты и докторанты, методисты и т.д.

## 2.2 Выявление потенциальных угроз и каналов утечки информации

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.

Организационная структура кафедры университета представлена на рисунке 2.1.

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

Рисунок 2.1 Организационная структура кафедры университета.

Кафедра

Заместитель зав. кафедры  
(2)

Преподавательский состав (3)

Лаборатория  
(4)

Лаборанты

Заведующий лабораторией

Зав. кафедры  
(1)

Методисты

(5)

## 2.3 Проведение оценки угроз и рисков для ИС

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

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:

* 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 |

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. |

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 |

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.

|  |  |
| --- | --- |
| 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 |

# **Глава 3**

# Проектирование СЗИ.

## 3.1 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

## 3.2 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 – «Системы защиты информации информационной системы класс Б2».

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

Заказчик: Белорусский государственный университет. Адрес: 220000, проспект Независимости 4, Минск.

Испольнитель: ООО «Рокет Эпс» Адрес: 220000, Бизнес-центр Альянс, 3-я улица Щорса 9, Минск

**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 34.101.9-2004 «Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы». |
|  | 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 ул. Курчатова 5, Минск.

**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 5 этаже учебного корпуса РФиКТ.

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

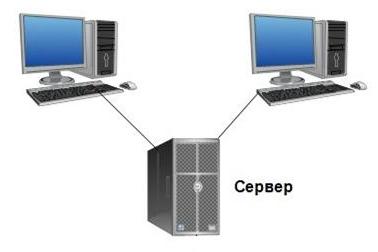


Рисунок 3.1. Схема информационного взаимодействия объектов.

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 | Закупка средств защиты информации, указанных в техническом проекте.  На этом этапе производится закупка средств защиты информации, предусмотренных техническим проектом; Средства защиты должны быть закуплены в полном объёме. | Доставка на объект заказчика закупленных средств защиты информации. |
| 7 | Установка и настройка параметров закупленных средств защиты информации.  Закупленные средства защиты должны быть установлены на объекте заказчика и соответствующим образом настроены для выполнения своих функций. Настройка должна производиться специалистами, имеющими соответствующую квалификацию. | Распаковка, монтаж, подключение и настройка параметров средств защиты на объекте заказчика. |
| 8 | Проведение испытаний созданной системы защиты информации | Акт ввода в опытную эксплуатацию. |
| 9 | Составление документации на автоматизированную систему защиты информации, необходимой нормативно-распорядительной документации на объекте информатизации | Технический паспорт на созданную систему защиты информации. Инструкция администратора систем, инструкция пользователя системы. |
| 10 | Аттестация СЗИ | Программа и методика аттестационных испытаний  Протокол аттестационных испытаний  Заключение по результатам аттестационных испытаний  Аттестат соответствия |
| 7 | 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 4

Разработка СЗИ

4.1 Разработка политики безопасности

4.2 Политика безопасности

# 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 произведено планирование 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.

После этапа планирования должен быть произведён этап реализации СЗИ, в ходе которого должна быть разработана политики безопасности.

# 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. ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"
6. Дорофеев Александр Владимирович, Марков Алексей Сергеевич Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. №1 (2) С.67-73.
7. Дорофеев Александр Владимирович Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. №2 (3) С.66-73.
8. Марков А.С., Цирлов В.Л. Управление рисками - нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. № 8. С. 63-67.
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. План обработки рисков | Александр Астахов “Искусство управления информационными рисками" [Электронный ресурс] – Режим доступа: http://анализ-риска.рф/content/plan-obrabotki-riskov ‑ Дата доступа: 25.05.2016
11. Курс [Электронный ресурс] – Режим доступа: http://edu.softline.by/courses/smib.html ‑ Дата доступа: 25.12.2016
12. Создание систем информационной безопасности [Электронный ресурс] – Режим доступа: https://www.ot.ru/services/creation-of-information-security/ ‑ Дата доступа: 25.12.2016
13. Создание систем защиты информации [Электронный ресурс] – Режим доступа: http://iba.by/services/isecurity/iss-creation/ ‑ Дата доступа: 25.12.2016