**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

**Кафедра телекоммуникаций и информационных технологий**

РАДКЕВИЧ

Владислав Игоревич

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

Дипломная работа

Научный руководитель:  
кандидат технических наук,

доцент Г.К. Резников

Допущена 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](#_Toc485208228)

[РЕФЕРАТ 4](#_Toc485208229)

[ВВЕДЕНИЕ 7](#_Toc485208230)

[ГЛАВА 1 СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ОБЩИЕ СВЕДЕНИЯ 9](#_Toc485208231)

[1.1 Введение в информационную безопасность и систему защиты информации. Терминология. 9](#_Toc485208232)

[1.2 Средства защиты информации 12](#_Toc485208233)

[1.3 Классификация объектов информатизации 15](#_Toc485208234)

[ГЛАВА 2 ПРОЕКТИРОВАНИЕ СЗИ 18](#_Toc485208235)

[2.1 Анализ организационной структуры информационной системы 18](#_Toc485208236)

[2.2 Классификация информации, хранящейся и обрабатываемой в информационной системе 20](#_Toc485208237)

[2.3 Проведение оценки угроз и рисков для ИС 21](#_Toc485208238)

[2.4 Разработка технического задания 24](#_Toc485208239)

[2.5 Техническое задание на систему защиты информации 24](#_Toc485208240)

[ГЛАВА 3 СОЗДАНИЕ СЗИ 35](#_Toc485208241)

[3.1 Разработка политики безопасности 35](#_Toc485208242)

[3.2 Политика безопасности 37](#_Toc485208243)

[ЗАКЛЮЧЕНИЕ 48](#_Toc485208244)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 49](#_Toc485208245)

# 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

# РЕФЕРАТ

Дипломная работа, 54 страницы, 5 рисунков (схемы, рисунки), 7 таблиц, 11 источников.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ СИСТЕМА, УЧЕБНОЕ ЗАВЕДЕНИЕ, ОБЪЕКТ ИНФОРМАТИЗАЦИИ, СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.

*Объект исследования* – информационная система учебного заведения.

*Цель работы* – проектирование системы защиты информации информационной системы класса Б2 на примере информационной системы учебного заведения.

В процессе работы над дипломной работой был изучен закон Республики Беларусь «Об информации, информатизации и защите информации», набор стандартов СТБ 34.101, которые являются основными руководящими и нормативно-техническими документам при разработке систем защиты информации, а также приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации». Всё это позволило узнать особенности проектирования и создания систем защиты информации.

С целью выполнения необходимых работ по проектированию системы защиты информации была произведена классификация информации, которая хранится и обрабатывается в информационной системе учебного заведения. Также был произведён анализ организационной структуры учебного заведения, разработано техническое задание на систему защиты информации и политика безопасности для учебного заведения.

**РЭФЕРАТ**

Дыпломная праца, 54 старонкi, 5 малюнкаў (схемы, малюнкі), 7 табліц, 11 крыніц.

СІСТЭМА АБАРОНЫ ІНФАРМАЦЫІ, ІНФАРМАЦЫЙНАЯ БЯСПЕКА, ІНФАРМАЦЫЙНАЯ СІСТЭМА, НАВУЧАЛЬНАЯ УСТАНОВА, АБ'ЕКТ ІНФАРМАТЫЗАЦЫІ, СРОДКІ АБАРОНЫ ІНФАРМАЦЫІ.

*Аб'ект даследавання* – інфармацыйная сістэма навучальнай установы.

*Мэта працы* – праектаванне сістэмы абароны інфармацыі інфармацыйнай сістэмы класа Б2 на прыкладзе інфармацыйнай сістэмы навучальнай установы.

У працэсе работы над дыпломнай працай быў вывучаны закон Рэспублікі Беларусь «Аб інфармацыі, інфарматызацыі і абароне інфармацыі», набор стандартаў СТБ 34.101, якія з'яўляюцца асноўнымі кіруючымі і нарматыўна-тэхнічнымі дакументам пры распрацоўцы сістэм абароны інфармацыі, а таксама загад Аператыўна-аналітычнага цэнтра пры Прэзідэнце Рэспублікі Беларусь ад 30 жніўня 2013 г. № 62 «Аб некаторых пытаннях тэхнічнай і крыптаграфічнай абароны інфармацыі». Усё гэта дазволіла даведацца пра асаблівасці праектавання і стварэння сістэм абароны інфармацыі.

З мэтай выканання неабходных работ па праектаванню сістэмы абароны інфармацыі была праведзена класіфікацыя інфармацыі, якая захоўвацца і апрацоўваецца ў інфармацыйнай сістэме навучальнай установы. Таксама быў праведзены аналіз арганізацыйнай структуры навучальнай установы, распрацавана тэхнічнае заданне на сістэму абароны інфармацыі і палітыка бяспекі для навучальнай установы.

**ABSTRACT**

The degree work, 54 pages, 5 drawings (diagrams, drawings), 7 tables, 11 sources.

INFORMATION PROTECTION SYSTEM, INFORMATION SECURITY, INFORMATION SYSTEM, EDUCATIONAL INSTITUTION, OBJECT OF INFORMATIZATION, INFORMATION PROTECTION MEANS.

*The object of the study* is the information system of an educational institution.

*The purpose* is to design an information security system of the information system of B2 class on the basis of an information system of an educational institution.

In the process of work on the degree work I studied the law of the Republic of Belarus "On Information, Informatization and Information Protection", a set of STB 34.101 standards which are the main guiding and normative technical documents in the process of development of information security systems, as well as the Order of the Operational analytical center under the President of the Republic of Belarus dd. August 30, 2013 No. 62 "On some issues of technical and cryptographic protection of information." All this allowed to learn the stages of designing and creating information security systems.

To perform the necessary set of works on designing of the information security system, the classification of information stored and processed in the information system of the educational institution was carried out. Also, I carried out an analysis of the organizational structure of the educational institution, developed Terms of Reference for the information security system and the security policy for the educational institution.

# ВВЕДЕНИЕ

В наше время организация эффективной системы защиты информационной системы становится очень важным стратегическим шагом, влияющим на развитие любой организации, так как информация в наши дни является основой бизнеса. При этом значение понятия информация состоит не только из статических информационных ресурсов, таких как базы данных, текущие настройки оборудования и др., 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 каждого учебного заведения, так и для любой другой структуры или организации, задача защиты информации должна быть если не самой важной, то одной из важнейших.

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

Информационная среда предприятия, вне зависимости от своего состава, должна иметь систему защиты. Но иногда расходы на обеспечение высокого уровня безопасности могут быть неоправданны. Поиск разумного компромисса и выбор приемлемого уровня защиты относительно расходов на построение СЗИ является важным условием постановки задачи обеспечения ИБ. Чтобы решить этот вопрос необходимо проводить анализ рисков ИБ, который позволяет оценить текущий 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 дипломной работы – проектирование системы защиты информации информационной системы класса Б2 на примере информационной системы учебного заведения.

Для реализации данного 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 СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ОБЩИЕ СВЕДЕНИЯ

## 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 [1].

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 [1].

Целостность и подлинность – это свойства, защищенность от несанкционированного . Выделяют логическую и целостность. Физическая представляет неизменность физического данных на машинном . Логическая целостность корректность процессов (транзакций), и непротиворечивость информации, , в СУБД, файловых , электронных , хранилищах данных, управления и т.д.

Доступность – свойство быть за приемлемое время по со стороны санкционированного [2]. С доступностью часто такую системы как готовность. – это способность к выполнению функций в установленных условиях. , имеющие целью степень доступности, атаками на отказ в (DOS-атаки).

информации – свойство, неизменность содержания и однозначность интерпретации в случайных или воздействий в течение времени ее существования.

и риск являются о факторами безопасности [3].

Угроза – это ая причина (событие, , инцидент), которая уровень безопасности системы, т.е. может привести к последствиям, а также вред (организации).

Риск собой возможный , т.е. комбинацию (как , произведение) реализации угрозы и от нее. Можно отметить, что и риск определяются не , а относительно к защищаемого ресурса.

В менеджмента бизнес-процессов ресурса используется понятие – . Под определение данного подпадает все, что имеет для организации. Можно примеры в информационной сфере: , программное обеспечение, обеспечение, информационная (сложный , включающий предыдущие), , имидж организации. В , активами становятся все те , которые быть защищены выстраивания процессов безопасности.

Угрозы по ряду [3]:

* по причине возникновения ( или техногенные, в том числе или случайные);
* по расположению (внешние или );
* по компрометируемой подсистеме или (сетевые, криптографические и др.);
* по формирования в жизненном системы ( и эксплуатационные);
* по результирующему (нарушают целостность, , доступность).

На рисунке 1.1 примеры информационной безопасности.

** 1.1 – Примеры угроз безопасности**

Достаточно каталоги подготовлены немецким агентством по информационной (BSI).

Одной из угроз ИБ систем является реализации уязвимости в системы. Уязвимость *–* это дефект («»), который снижает защищенности ресурсов от угроз. Необходимо , что наличие становится угрозой, ее можно реализовать так, что это к недопустимому ущербу . Например, сетевых уязвимостей в обеспечении изолированного , не является угрозой.

реализация в компьютерных системах, к причиняет вред , называется атакой на .

Повышение и заданных уровней ресурсов осуществляется применения мер (механизмов) . На профессиональном такие меры называются контролями (от. . слова controls – управления). важно не путать жаргонизм с привычным «контроль», имеющим значение: за поведением управляемой с целью обеспечения ее функционирования.

Контроли иметь , организационный и физический . К техническим контролям программные и программно-аппаратные защиты, как антивирусы, межсетевые , системы обнаружения , средства шифрования и т. п. В качестве контролей выступают , обязательные для исполнения . Например, наличие заявки на доступа к системе у ее (как правило, бизнес-подразделения, отвечающего за , которые данной системой). примерами физических являются решетки, , заборы–все что ет физический доступ к активам.

Контроли служить для разнообразных , например, превентивными, детективными, , восстанавливающими и другими.

различных видов и контролей связано с концепцией обороны (defense in , multilevel security), идеологию систем защиты с уровнями мер (механизмов) , позволяющими обеспечить защиту в случае «пробивания» на одном уровне.

защиты информации – это правовых, и технических мер, направленных на конфиденциальности, целостности, , доступности и сохранности .

## 1.2 Средства информации

При осуществлении защиты информации средства технической информации, сертификат соответствия, в Национальной системе соответствия Республики , или положительное заключение по результатам экспертизы, проводимой центром при Президенте Беларусь [4].

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

Техническое средство информации – техническое , специально и (или) используемое для или ослабления характерных или физического проявления защиты, определяются при помощи технической разведки и для получения информации, сведения, защите, а также для помех техническим разведки или специальным средствам.

К средствам защиты относятся: помехоподавляющие фильтры, генераторы , излучающие различной физической (например, электрические, ).

Техническое средство защищенности – техническое устройство, изготовленное и (или) для измерения количественных , позволяющих степень защищенности от ее утечки по техническим .

К техническим средствам защищенности относятся анализаторы , шумомеры и иная измерительная аппаратура.

е средства информации – это средства, в составе программного .

Программно**-**аппаратные защиты – вся система обработки или часть ее физических с размещенными программами и . Программы при размещаются таким , чтобы их несанкционированное было невозможным в исполнения. и данные, размещенные на ПЗУ с программированием, допускающим , рассматриваются как программное [5].

К программным и **-**аппаратным средствам информации относятся:

* криптографической защиты ;
* антивирусные ;
* средства идентификации и пользователей;
* средства доступом;
* средства и аудита и т.д.

криптографической защиты – программные, программно**-** средства защиты , реализующие или несколько криптографических (шифрование, выработка и электронной цифровой , хэширование, ) и криптографические протоколы, а функции управления ключами, механизмы и аутентификации.

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

Средства защиты выпускаются в обращение на в установленном при их соответствии техническому ТР 2013/027/BY, а также техническим регламентам, которых на них .

Средства защиты , соответствие которых технического регламента ТР 2013/027/ не подтверждено, не быть маркированы соответствия техническому согласно ТКП 5.1.08**-** «Национальная подтверждения соответствия Беларусь. Знаки . Описание и порядок » и не допускаются к в обращение на рынке.

следующая классификация защиты информации:

* 1. защиты от доступа.

Мандатное доступом – это разграничение субъектов к объектам, на назначении конфиденциальности для информации, в объектах, и выдаче разрешений (допуска) на обращение к такого уровня .

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

вление доступом на ролей – политики избирательного доступом, при котором доступа субъектов на объекты с учетом специфики их , образуя роли.

– процесс записи о происходящих с объектом (или в некоторого процесса) в журнал (например, в ). Также это процесс называют .

1. Системы мониторинга .

Система обнаружения (СОВ) – или аппаратное средство, для выявления фактов доступа в компьютерную или сеть несанкционированного управления ими в через Интернет.

предотвращения утечек информации – предотвращения утечек информации из информационной вовне, а также устройства ( или программно-аппаратные) для такого утечек системы на анализе потоков , которые т периметр защищаемой системы. Если в потоке обнаруживается информация, то активная компонента и происходит блокировка (потока, сообщения, ).

1. Анализаторы .

Анализатор трафика, или анализатор трафика – или программно-аппаратное устройство, для перехвата и анализа, либо анализа сетевого , предназначенного для других .

1. Антивирусные .

Антивирусная программа – программа для обнаружения вирусов, а также (считающихся ) программ вообще и зараженных (модифицированных) программами файлов, а для профилактики **-** заражения (модификации) или операционной системы кодом.

1. Межсетевые .

Основной сетевого экрана защита компьютерных или отдельных узлов от доступа. сетевые экраны называют фильтрами, так как их задача –не пропускать () пакеты, не под критерии, которые в конфигурации.

1. Криптографические .
2. Системы бесперебойного .

Источник питания (ИБП) – вторичного электропитания, устройство, назначение обеспечить к нему электрооборудование снабжением электрической в пределах нормы.

1. аутентификации.

– проверка принадлежности доступа предъявленного им ; подтверждение подлинности.

часто с идентификацией и авторизацией, необходимо четко данные понятия.

из способов в компьютерной системе во вводе вашего идентификатора, в просторечии «логином». введенный пользователем и пароль, компьютер их со значением, которое в специальной данных и, в случае , пропускает пользователя в .

1. Системы резервного .

Системы копирования – системы для процесса создания данных на носителе ( диске, и т. д.), предназначенном для восстановления в оригинальном месте их в случае их повреждения или .

## 1.3 Классификация информатизации

Согласно 9.2 приказа оперативно**-** центра при президенте РБ «О вопросах и криптографической информации», №62 от 30.08.2013, из этапов проектирования защиты , является «присвоение системе класса объекта информатизации» [4].

типового информатизации присваивается в с СТБ 34.101.30–2007 « технологии. Методы и безопасности. информатизации. Классификация»

объектов информатизации () проводится применительно к ОИ.

Типовой ОИ – , оснащенный типовым аппаратных, программных, **-**программных средств, в том числе и защиты .

Классификация ОИ проводится по конфиденциальности [2]:

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

и по вычислительных :

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

В соответствии со могут следующие классы ОИ:

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

# ГЛАВА 2 ПРОЕКТИРОВАНИЕ СЗИ

## 2.1 организационной структуры системы

Определение применения защиты информации в себя следующие [6]:

* описание вида и бизнес**-** организации;
* указание систем, охватываемых СЗИ;
* о активов организации ( информационных , программно**-**технические , персонал и организационная );
* описание бизнес**-**, использующих информацию.

Как правило, на этапе составляется , в котором фиксируют информационной , перечисляют информационные компании, подлежащие , приводят систему и методики для ценности информационных компании.

Учебное – это учреждение, осуществляющее процесс, то реализующее одну или образовательных программ и () обеспечивающее содержание и обучающихся, .

Можно выделить задачи учебного :

1. Развитие творческих, и физических личности, формирование основ нравстве и здорового образа .
2. Воспитание и патриотизма, любви к – Республике Беларусь, к государственным символам, народных , нетерпимости к любым и антиобщественным проявлениям.
3. П квалифицированных специалистов, на рынке , переподготовка и повышение их .
4. Приобщение к достижениям и отечественной культуры; истории, и традиций белорусского и народов республики.
5. О государственным, русским, языками.
6. В новых технологий , информатизация высшего образования, выход на глобальные сети.

Каждая имеет свою . Во главе высшего стоит . Его заместителями по различным работы являются , которые решают и тактические работы ВУЗа. вопросы развития обычно решает его совет.

Для понимая будем из того что учебное состоит из факультетов, а отдельный состоит из кафедр.

структура учебного представлена на рисунке 2.1.

**2.1 – Организационная учебного заведения**

Для детального понимания организационную структуру . Главным органом кафедры заведующий кафедрой, в его находятся заместитель , преподавательский , лаборатории вместе с персоналом и методисты.

структура кафедры заведения на рисунке 2.2.

**Рисунок 2.2 – структура кафедры заведения**

Также стоит , что, поскольку мы с информационной класса Б2, то эта система не доступа в сети пользования.

## 2.2 К информации, хранящейся и в информационной системе

заведение – это достаточно предприятие, оно имеет достаточно информации, хранящейся и в ИС. Ниже приведены виды :

* персональные данные ;
* личные данные ;
* научно**-**исследовательские ;
* сведения об ;
* экзаменационные билеты;
* преподавателей.

Вся эта информация информацией ограниченного и должна защищена.

Также в ИС учебного имеется общедоступная , так как:

* расписание занятий;
* планы;
* информация о работниках;
* ;
* методические рекомендации по курсовых, дипломных .

## 2.3 Проведение угроз и рисков для ИС

информационной безопасности – это возможность понести из**-**за нарушения информационной системы [7].

приведены параметры, риск:

* угроза, реализацией вызван данный ;
* ресурс, в отношении может быть данная ;
* уязвимость, через может быть данная угроза в данного .

Угроза информационной – это потенциальная возможность режима информационной . Преднамеренная угрозы называется на информационную систему. , преднамеренно реализующие , являются .

Уязвимость – это так называемое « место» в системе информации, которое основанием для угрозы со стороны .

Любая хорошо методология оценки информационной предусматривает такие , как [8]:

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

Из всего вышеперечисленного , что шаги методики исходя из определения риска.

До каких**-**либо по оценке рисков, определить критерии для их . Один из , позволяющих определить для оценки последствий, в том, чтобы оттолкнуться от , которые мы перед информационной . Защитой информации мы для того, чтобы финансовые , сохранить или даже положение кафедры на . В таблице 2.1 приведена последствий.

**2.1 – Классификация последствий**

|  |  |  |
| --- | --- | --- |
| **последствия** | **Финансовые** | **Положение кафедры на** |
| Высокий (В) |  | Заметно ухудшится, до расформирования кафедры |
| (С) | Средние | Ухудшится, , будут изменения |
| Низкий (Н) |  | Практически не ухудшится, лица получат |

Для оценки реализации ограничимся критериями: имеющаяся по аналогичным инцидентам, затраты на угрозы и возможность . Оценка вероятностей угроз отражена в 2.2.

**Таблица 2.2 – вероятностей реализации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Вероятность** | **Статистика** | **Затраты на реализацию** | **Возможность** |
| Высокая (В) | Аналогичный происходит каждую . | Интеллектуальные: невысокая злоумышленника. для реализации угрозы . | Угрозу и ее источник сложно обнаружить. |
| (С) | Аналогичный происходит каждый . | Интеллектуальные: средняя злоумышленника.  Инструменты для угрозы приобрести или создать за срок. | Угрозу и ее можно вычислить, но для потребуются усилия. |
| Низкая (Н) | инцидент происходит год. | Интеллектуальные: высокая злоумышленника.  для реализации угрозы на момент не доступны. | и ее источник легко . |

Исходя из вероятностей и таблицы можно создать , в которой сопоставляется реализации с размерами последствий от её и получить значения . В таблице 2.3 отражены рисков.

**2.3 – Значение рисков**

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

После критериев, которые использоваться для рисков, в соответствии с СТБ 34.101.2 «Информационные и безопасность. Критерии безопасности технологий. Часть 2. требования безопасности», идентифицировать угрозы и, , риски [9]. для исследуемых видов приведены в таблице 2.4.

**2.4 – Угрозы для исследуемых информации**

|  |  |
| --- | --- |
| **информации** | **Угроза** |
| данные студентов и | * хищение * уничтожение |
| личные студентов и сотрудников | * х * уничтожение * модификация |
| **-**исследовательские работы | * уничтожение |
| сведения об успеваемости |  |
| экзаменационные билеты | * модификация * уничтожение |
| преподавателей |  |

## 2.4 Разработка технического

Техническое задание основное назначение объекта, его и тактико**-**технические , показатели качества и **-**экономические требования, по выполнению стадий создания (конструкторской, технологической, и т. д.) и её состав, а также требования.

задание на систему информации строиться по плану:

1. Общие ;
2. Назначения и создания системы;
3. к системе защиты ;
4. Требования к средствам ;
5. Порядок и приёмки системы.

С требований, подлежащих ию в техническое задание на защиты можно ознакомиться в А.

## 2.5 Техническое задание на защиты информации

**2.5.1 сведения**

Техническое задание в соответствии с приказом №62 «О вопросах технической и защиты » оперативно**-**аналитического при президенте Республики и является основным , определяющим и порядок создания, , модернизации, сопровождения защиты информации системы Б2.

Результатом создания защиты информации системы класса Б2 стать работоспособная автоматизированная защиты информации системы класса Б2, требованиям технического задания.

**2.5.1.1 наименование системы**

наименование системы:« защиты информационной системы Б2».

**2.5.1.2 Наименование реквизитов и заказчика СЗИ**

Заказчик:  *УЧЕБНОГО* .

Адрес: *АДРЕС ЗАВЕДЕНИЯ*.

Исполнитель:  *ФИРМЫ*

Адрес: *С ФИРМЫ.*

**2.5.1.3 документов, на основании создаётся СЗИ**

Для формирования были использованы , разработанные на этапах создания СЗИ, приведены в таблице 2.5.

**2.5 – Документы, разработанные на этапах СЗИ**

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

Осно руководящие и нормативно- документы приведены в 2.6.

**Таблица 2.6 – основных руководящих и но-технических документов**

|  |  |
| --- | --- |
| № п/п | документа |
| 1 | СТБ 34.101.1– «Информационные и безопасность. Критерии безопасности информационных . Ч. 1. Введение и общая ». |
| 2 | СТБ 34.101.2– «Информационные технологии и . Критерии оценки информационных технологий. Ч. 2. требования ». |
| 3 | СТБ 34.101.3–2014 « технологии и безопасность. оценки безопасности технологий. 3. Гарантийные требования ». |
| 4 | СТБ 34.101.8–2006 « технологии. Методы и безопасности. средства защиты от вредоносных программ и программные средства. требования». |
| 5 | СТБ –2011 «Информационные . Средства защиты информации от утечки по и виброакустическому . Общие технические » |
| 6 | СТБ 34.101.29–2011 « технологии. Средства защищенности информации. Общие требования» |
| 7 | СТБ 34.101.30– «Информационные технологии. и средства . Объекты информатизации. ». |

Плановые сроки и окончания работ по системы информации:

Начало : 01 декабря 2016 .

Окончание : 01 апреля года.

**2.5.2 Назначение и создания системы**

**2.5.2.1 системы защиты**

СЗИ для работы учебного заведения.

**2.5.2.2 создания системы**

Цель создания системы – защита информации заведения.

Снижение наносимого ущерба реализации безопасности, путём технических, организационных мер, выполнение требований , предусмотренных **-**методическими документами критерием оценки целей создаваемой .

**2.5.2.3 Краткая информационной системы,**

Данная система из себя информационную учебного .

**2.5.2.4 Размещение СЗИ**

СЗИ будет по адресу *АДРЕС*.

**2.5.2.5 и пропускной режим**

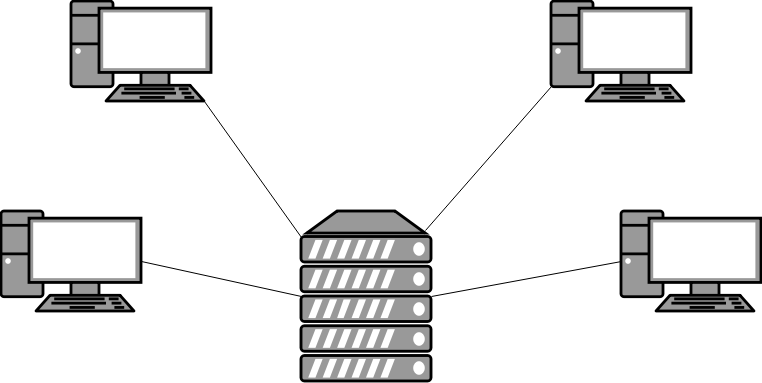
На , на котором внедрить систему информации, осуществляется к**-**пропускной режим. Также и выход с ограничен с 23:00 до 7:00.

**2.5.2.6 зона**

Контролируемая представлена в виде стен , располагающихся на первом учебного корпуса.

**2.5.2.7 информационного взаимодействия в ИС**

Схема взаимодействия объектов на рисунке 2.3.

**Рисунок 2.3 – информационного взаимодействия**

Информационная не имеет выхода в общего пользования.

**2.5.2.8 модель угроз в ИС**

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

**2.5.3 Требования к защиты информации ИС**

**2.5.3.1 к функциям (задачам), системой.**

* Идентификация ИС (далее – ) и закрепление за ними ИС (далее – субъекты);
* и аутентификация субъектов;
* идентификаторами( , присвоение, уничтожение);
* средствами аутентификации (, выдача, инициализация, средств и принятие мер в случае /компрометации средств );
* Исключение отображения информации;
* атрибутов безопасности, по умолчанию в соответствии с информационной безопасности;
* управление (, активация, блокировка, ) учетными записями ;
* Определение обязанностей и субъектов;
* правил разграничения субъектов к объектам;
* доступа к ИС по истечению времени субъекта или по его запросу;
* возможных действий , которые могут до их идентификации и (при необходимости);
* Наличие схемы сети с объектов, внешних и информационных ;
* Управление (фильтрация, , контроль соединений) потоками между , а также информационными системами;
* входящего и исходящего только необходимыми ;
* Запрет на в информационной системе беспроводного доступа;
* порядка использования в системе технических средств и за таким использованием;
* перечня и регламентация установки и разрешенного обеспечения;
* Определение разрешенного программного и регламентация его установки и использования;
* доступа к учтенным носителям информации;
* возможности ознакомления с содержанием , которая хранится на машинных носителях ;
* Уничтожение с машинных носителей при их передаче лицам, не субъектами информационной , в том числе для , технического обслуживания;
* состава и содержания о событиях безопасности, регистрации;
* , запись и хранение о событиях безопасности в установленного срока ;
* Мониторинг безопасности уполномоченными
* Сбор, хранение, , мониторинг информации о в механизмах информации и достижении объема памяти хранения уполномоченными ;
* Синхронизация меток в информационной ;
* Синхронизация системного в информационной системе;
* информации о безопасности;
* Регламентация базы данных вредоносного программного ;
* Регламентация проверок операционных на предмет обнаружения , которые вызваны вредоносного обеспечения в системе;
* уязвимостей информационной и их оперативное устранение;
* за установкой программного обеспечения, обновление программного средств защиты ;
* Контроль за , параметрами настройки и функционирования программного и средств защиты ;
* Регламентирование резервирования информации и обеспечения, включая обеспечение средств информации;
* и аутентификация субъектов и в виртуальной инфраструктуре, в том уполномоченных пользователей по средствами ;
* Управление доступом к объектам в виртуальной , в том числе внутри машин;
* контролируемой зоны, в которой постоянно стационарные технические и средства информации;
* Контроль и физическим доступом контролируемой зоны к средствам, защиты информации, обеспечения функционирования, а в помещения и сооружения, в они установлены, несанкционированный физический к средствам обработки , средствам защиты и средствам функционирования информационной , а также в помещения и , в которых они установлены.

**2.5.3.2 к средствам .**

При осуществлении технической информации используются технической защиты , имеющие соответствия, выданный в системе подтверждения Республики Беларусь, или экспертное по результатам государственной , проводимой Оперативно**-** центром при Президенте Беларусь

**2.5.3.3 по электрической и пожарной**

Технические средства, для реализации приведённых требований соответствовать нормам по и пожарной безопасности, на предприятии заказчика.

Все элементы средств системы, под напряжением, должны защиту от случайного , а сами средства иметь или защитное заземление.

требования пожарной должны нормам на бытовое .

**2.5.3.4 Требования по эксплуатации и обслуживанию**

Необходимо бесперебойное ПЭВМ для нормальной разрабатываемой системы. При система должна обеспечена стандартам хранения и эксплуатации ПЭВМ и влажность воздуха. помещений и их должны исключать бесконтрольного проникновения в них лиц и обеспечивать сохранность в этих конфиденциальных документов и средств. Размещение средств и оборудования соответствовать техники безопасности, нормам и требованиям безопасности. Все пользователи должны правила эксплуатации вычислительной техники. техническое обслуживание технических должно проводиться в с требованиями технической изготовителей, но не реже раза в год.

персонала и его подготовка соответствовать технической .

**2.5.3.5 Требования к патентной**

По всем и программным средствам, применяются в системе, соблюдаться условия соглашений и патентная чистота на Республики Беларусь.

чистота – это юридическое объекта, в том, что он может быть использован в Республике без опасности нарушения на ее территории исключительного права, третьим лицам.

**2.5.3.6 к эргономике и технической**

Взаимодействие с прикладным программным , входящим в состав должно осуществляться визуального интерфейса (GUI). требование к интерфейсу : он должен быть и удобным, он не должен быть графическими элементами и быстрое отображение экранных . Навигационные элементы быть выполнены в для пользователя форме. редактирования должны удовлетворять соглашениям в части функциональных клавиш, работы, , использования оконной . В интерактивном режиме обеспечить выполнение ввода-а данных , прием управляющих и отображение результатов их . Интерфейс должен современным требованиям и обеспечивать доступ к основным и операциям системы. У системой осуществляться с помощью экранных меню, , значков и т. п. элементов, интерфейс быть рассчитан на использование манипулятора «мышь» Клавиатурный ввода используется главным при заполнении (редактировании) ввода экранных . Все надписи форм, а также , выдаваемые пользователю (не системные сообщения) быть на языке.

**2.5.3.7 Требования к и содержанию работ по системы защиты персональных .**

Этапы работы по с СЗИ отражены в таблице 2.7.

**2.7– Этапы работы по СЗИ**

| **Этап** | **работ** | **Результаты** |
| --- | --- | --- |
| 1 | Классификация информации, и обрабатываемой в информационной , в соответствии с об информации, информатизации и информации, в том числе и нормативными правовыми |  |
| 2 | Анализ структуры информационной и информационных потоков в определения состава () и мест элементов системы ( и программных), ее физических и границ |  |

**Продолжение 2.7**

|  |  |  |
| --- | --- | --- |
| 3 | Присвоение системе класса объекта информатизации в , установленном СТБ 34.101.30-2007 « технологии. и средства безопасности. информатизации. Классификация» |  |
| 4 | требований к системе информации в задании на информационную | Техническое задание |
| 5 | технического проекта.  технический отправляется на ознакомление и заказчику. В ходе этапа могут внесены и изменения в проект, это потребуется. Итогом проекта является его сторонами |  |
| 6 | политики информационной | Политика безопасности |
| 7 | планируемых к использованию защиты , проверка их работоспособности и | В ходе внедрения защиты информации их монтаж и в соответствии с эксплуатационной . |
| 8 | Внедрение организационных мер информации осуществляется в реализации , изложенных в локальных правовых актах , которые доводятся до субъектов системы под подпись |  |

**таблицы 2.7**

|  |  |  |
| --- | --- | --- |
| 9 | Опытная системы защиты | Опытная системы защиты осуществляется для проверки ее в различных режимах информационной , в том числе при необходимости в чрезвычайной ситуации. В выявления в процессе эксплуатации защиты информации осуществляется их устранение с повторной опытной |
| 10 | Приемочные системы защиты | Приемочные испытания защиты информации в целях выполнения требований к защиты информации, в задании по безопасности или в задании |
| 11 | СЗИ | Аттестат соответствия. аттестата соответствия основанием для ввода системы в и использования ее в течение , установленного в аттестате |
| 12 | Ввод системы в | Акт ввода емы в промышленную эксплуатацию |

**Требования к разработчику защиты**

Привлекаемый на основе (юридическое лицо или предприниматель) должен лицензию на деятельность по и (или) защите информации оперативно-аналитическим центром при Республики Беларусь.

**2.5.4 контроля и системы**

**2.5.4.1 Порядок приёмки**

Испытания СЗИ на объекте заказчика.

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

На основании о приемке подписание комиссией приемки.

Опытная системы защиты на развернутом и рабочем месте, на потом будет дальнейшая промышленная .

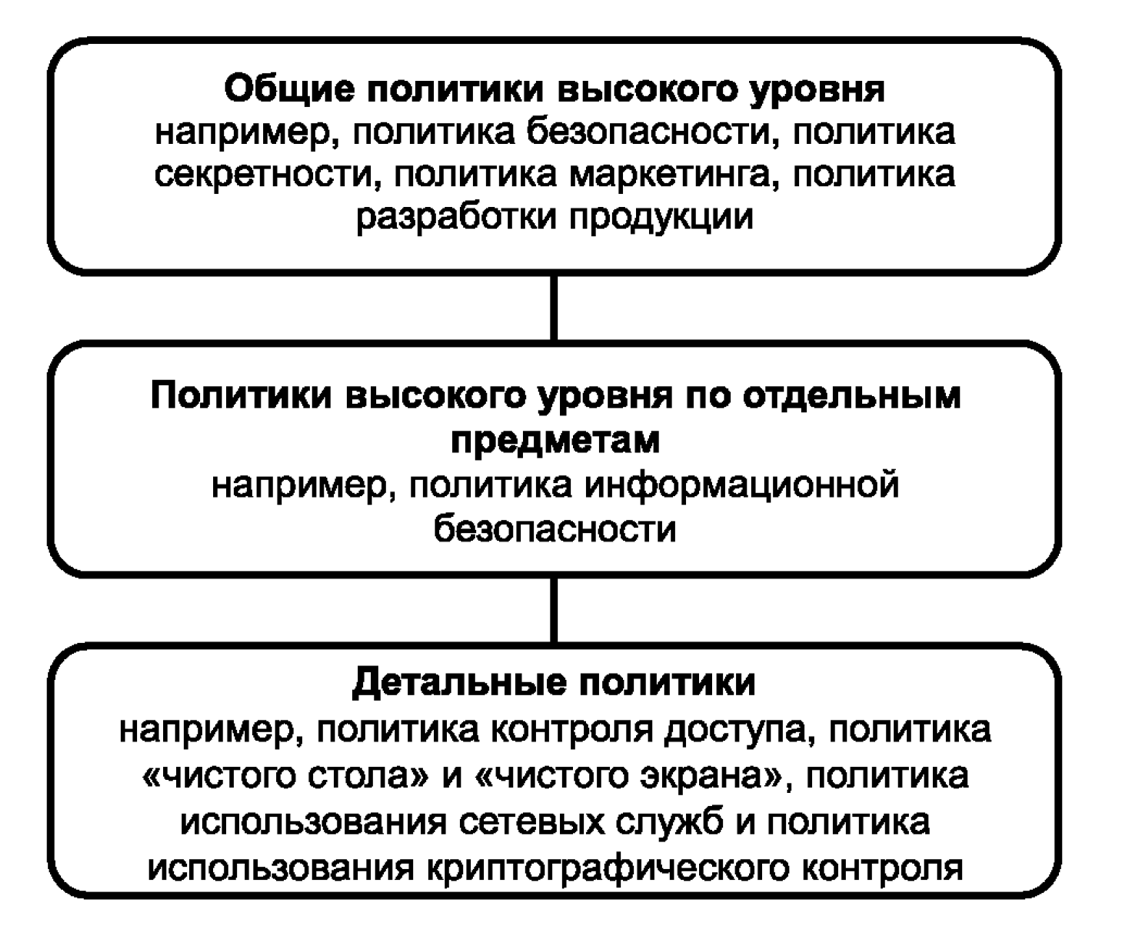
# ГЛАВА 3 СЗИ

## 3.1 Разработка политики

В соответствии с Приказом О**-**аналитического центра при Республики №62 «О некоторых вопросах и криптографической защиты » на этапе создания защиты осуществляются разработка информационной безопасности [4].

безопасности – совокупность , процедур, приемов или руково принципов в области , которыми руководствуется о в своей [10].

Организация может несколько политик, по для каждой сферы , важной для . Некоторые политики между собой, в то как другие политики в иерархическом . В области безопасности , как правило, иерархически . Обычно политика является высшего уровня. В очередь, политика безопасности может более политиками по конкретным , такими как: политика доступа, политики « стола» и « экрана», политика и сетевых служб и др. [11]. политик отображена на 3.1.

**Рисунок 3.1 – политик**

Содержание основано на контексте, в работает организация. Приказом О-аналитического центра при Республики Беларусь №62 «О вопросах технической и защиты » выделяется перечень , которые должна политика [4]:

* цели системы информации;
* перечень и объектов информационной , сведения о месте их и порядке взаимодействия субъектов с этой системы и между собой;
* разграничения субъектов к объектам системы;
* права и субъектов информационной ;
* порядок с иными информационными (в случае предполагаемого );
* перечень организационных мер, на реализацию по созданию системы информации;
* порядок при возникновении угроз конфиденциальности, , доступности, подлинности и информации, в том числе и непредотвратимых обстоятельств ( силы), и при их последствий.

## 3.2 Политика

**3.2.1. Краткое изложение**

Независимо от формы , способа , передачи и хранения, и всегда должна защищена.

**3.2.2. Введение**

Политика в соответствии с законодательством Беларусь и нормами в части обеспечения безопасности, и в том числе на:

* международном ISO/IEC 27002 « технологии – Методы – Свод правил для управления безопасностью»;
* приказе центра при Президенте Беларусь № 62 «О вопросах технической и защиты информации».

Политика является , доступным сотруднику учебного и пользователю его ресурсов, и собой официально руководством УЧЕБНОГО ЗАВАДЕНИЯ( – Учебное заведение) взглядов на проблему информационной , и устанавливает принципы системы управления безопасностью на основе изложения , процессов и процедур безопасности Учебного .

Руководство Учебного осознает и необходимость развития и мер и средств обеспечения безопасности в контексте законодательства и регулирования образовательной , а также развития учебным заведением и ожиданий , студентов и других сторон. Соблюдение информационной безопасности создать преимущества Учебному , обеспечить его финансовую , рентабельность, соответствие , регулятивным и требованиям и повышение .

Требования информационной , которые предъявляются заведением, целям и интересам Учебного заведения и для снижения рисков, с информационной , до приемлемого уровня. рисков в информационной Учебного заведения отношение к его управлению (менеджменту), и реализации бизнес-процессов, с контрагентами и клиентами, деятельности. рисков в информационной Учебного заведения значимую часть рисков заведения, а также отношение и к иным основной и управленческой Учебного .

Необходимые требования информационной безопасности заведения должны соблюдаться Учебного заведения и сторонами как это определяется внутренних нормативных Учебного , а также требованиями и соглашений, стороной является Учебное .

Настоящая тика распространяется на -процессы Учебного и обязательна для применения сотрудниками и Учебного заведения, а пользователями его информационных .

Положения настоящей должны учтены при разработке информационной безопасности в и аффилированных организациях.

Политика корпоративным документом по ИБ уровня.

Документами, положения корпоративной применительно к или нескольким областям ИБ, и технологиям деятельности заведения, являются политики по ИБ (далее – Частные ), которые являются по ИБ второго уровня, как отдельные нормативные документы заведения, разрабатываются и в соответствии с установленным в порядком, Куратором.

**3.2.3. Область**

Основными объектами системы информационной в Университете :

* + информационные ресурсы, коммерческую тайну, данные физических лиц, ограниченного , а также открыто информация, необходимая для Учебного заведения, от формы и ее представления;
  + сотрудники заведения, являющиеся и пользователями информационных Учебного ;
  + информационная инфраструктура, системы обработки и информации, технические и средства ее , передачи и отображения, в том каналы информационного и телекоммуникации, системы и защиты , объекты и помещения, в размещены такие .

**3.2.4. Цели информационной**

Целью , обеспечивающей информационную ь Учебного заведения, снижение угроз безопасности до для Учебного заведения .

Основные задачи по обеспечению информационной Учебного :

* выявление потенциальных информационной безопасности и объектов защиты;
* инцидентов безопасности;
* исключение минимизация выявленных .

**3.2.5. Принципы информационной**

Потенциальные ы безопасности информации на три класса в зависимости от их возникновения: антропогенные, и естественные.

человека обуславливает в антропогенных угроз. данных угроз выделить те, возникают вследствие действий: угрозы, ошибками в проектировании системы и ее , ошибками в действиях и др., так и другую группу , которые возникают в умышленных , связанные с корыстными, или иными устремлениями .

Антропогенные угрозы – это , связанные с и противоречивостью требований деятельности Учебного и контрольных органов, с в руководстве и (менеджменте), неадекватными и сложившимся условиям, с услугами, с человеческим .

Возникновение угроз обусловлено на объект угрозы физических процессов характера, состояния окружения угрозы или его самого, не напрямую деятельностью .

К техногенным могут быть сбои, в том числе в , или разрушение систем, человеком.

естественных угроз воздействиями на объект объективных физических природного , стихийных природных , состояний физической , которые не обусловлены деятельностью .

К естественным (природным) относятся угрозы , атмосферные, геофизические, и др., включая климатические условия, явления и стихийные .

По отношению к инфраструктуре заведения, угроз могут как внешними, так и внутренними.

По к Университету нарушители быть на две группы. К первой относятся внешние , а ко второй внутренние.

нарушители.

В потенциальных внутренних Университетом рассматриваются:

* пользователи информационных Учебного ;
* сотрудники Учебного , не являющиеся зарегистрированными и не допущенные к ресурсам систем заведения, но имеющие в здания и помещения;
* , обслуживающий технические корпоративной системы Учебного ;
* сотрудники самостоятельных подразделений Учебного , задействованные в и сопровождении программного ;
* сотрудники самостоятельных подразделений, обеспечивающие Учебного ;
* руководители различных .

Внешние нарушители.

В потенциальных внешних Университетом :

* бывшие сотрудники заведения;
* представители , взаимодействующих по вопросам обеспечения заведения;
* клиенты заведения;
* посетители и помещений Учебного ;
* конкурирующие с заведения образовательные ;
* члены преступных , сотрудники спецслужб или , действующие по их .

В отношении внутренних и нарушителей принимаются ограничения и предположения о их возможных :

* нарушитель скрывает несанкционированные действия от сотрудников Учебного ;
* несанкционированные нарушителя могут следствием ошибок , эксплуатирующего и обслуживающего , а также принятой технологии , хранения и передачи ;
* в своей деятельности нарушитель использовать любое средство перехвата , воздействия на информацию и системы, финансовые средства для персонала, шантаж, социальной инженерии и средства и для достижения стоящих ним целей;
* внешний может действовать в с внутренним .

Требования по обеспечению безопасности Учебного обязательны к соблюдению работниками заведения и пользователями систем.

Руководство заведения приветствует и в установленном деятельность работников заведения и пользователей систем по обеспечению безопасности.

или некачественное исполнение Учебного заведения и информационных систем по обеспечению безопасности может лишение доступа к системам, а также административных мер к виновным, степень определяется установленным в порядком либо действующего .

Стратегия Учебного в части противодействия информационной безопасности в сбалансированной взаимодополняющих мер по обеспечению : от организационных мер на уровне Учебного заведения, до мер информационной по каждому выявленному в риску, основанных на рисков информационной .

При планировании по обеспечению информационной в Университете осуществляются:

и распределение ролей Учебного , связанного с обеспечением безопасности (ролей безопасности).

Оценка информационных с учетом потребности в их свойств с точки информационной безопасности.

рисков безопасности, включающий:

* влияния на информационную Учебного заведения в деятельности заведения технологий, а внешних по отношению к событий;
* выявление обеспечения безопасности, анализ их возникновения и прогнозирование их ;
* определение моделей информационной ;
* выявление, анализ и значимых для Учебного угроз информационной ;
* выявление негативных последствий для заведения, которые т в результате проявления риска безопасности, в том числе с нарушением свойств информационных активов заведения;
* и анализ рисковых информационной безопасности;
* величины рисков безопасности и среди них рисков, для Учебного заведения;
* результатов оценки информационной , базирующейся на методах операционными рисками, в Университете;
* оптимизацию информационной за счет выбора и защитных мер, препятствующих факторов риска и к минимуму негативные последствия для заведения в случае рисковых событий;
* влияния мер на цели основной Учебного заведения;
* затрат на реализацию мер;
* рассмотрение и различных вариантов задач по обеспечению безопасности;
* разработку управления , предусматривающих различные меры и варианты их , и выбор из них оптимального, которого положительно отразится на основной деятельности заведения и будет с точки произведенных затрат и эффекта;
* документальное целей и задач информационной Учебного заведения, в актуальном состоянии -методического обеспечения в сфере безопасности.

В рамках деятельности по обеспечению безопасности в Университете :

* сбор о событиях информационной ;
* выявление и анализ информационной безопасности;
* инцидентов безопасности;
* оперативное на инцидент информационной ;
* минимизация негативных инцидентов безопасности;
* оперативное до руководства Учебного информации по наиболее инцидентам безопасности и оперативное решений по ним, включая порядка реагирования на информационной ;
* выполнение принятых по всем инцидентам безопасности в установленные ;
* пересмотр требований, мер и механизмов по информационной безопасности по рассмотрения инцидентов безопасности;
* уровня знаний Учебного заведения в обеспечения информационной ;
* обеспечение и управления доступом к и программно-техническим средствам и автоматизированных систем заведения и , обрабатываемой в них;
* применение криптографической защиты ;
* обеспечение бесперебойной автоматизированных и сетей связи;
* возобновления работы систем и сетей после и нештатных ситуаций;
* средств защиты от программ;
* обеспечение безопасности на жизненного цикла систем Учебного , связанных с проектированием, , приобретением, , вводом в действие, (сервисным обслуживанием);
* доступа в здания и Учебного .
* применение мер и технических , снижающих вероятность получения информации в форме – защита;
* применение мер и средств, создающих при несанкционированном получении – активная ;
* применение мер и технических , позволяющих выявлять несанкционированного получения – поиск.

В проверки деятельности по информационной безопасности в осуществляются:

* контроль реализации и защитных мер;
* контроль конфигурации систем и Учебного заведения;
* факторов и соответствующий их пересмотр;
* реализации и исполнения сотрудниками Учебного действующих нормативных документов по информационной безопасности заведения;
* контроль сотрудников и пользователей информационных Учебного заведения, на выявление и предотвращение интересов.

В совершенствования деятельности по информационной безопасности в производится периодическое, а при оперативное, (пересмотр) целей и обеспечения информационной (при изменениях и задач деятельности Учебного ).

В целях выполнения по обеспечению информационной Учебного , в соответствии с рекомендациями стандартов по безопасности в должны быть следующие :

* Куратор;
* Ответственное ;
* Сотрудник Учебного .

При необходимости могут определены и роли по информационной .

Оперативная деятельность и деятельности по обеспечению безопасности заведения осуществляются и Ответственным подразделением. Ответственного подразделения :

* установление Учебного заведения в мер обеспечения информационной , определяемых как внутренними требованиями, так и нормативных актов;
* действующего законодательства, актов органов власти, в области обеспечения и противодействия техническим и технической защиты , нормативных по обеспечению информационной ;
* разработка и пересмотр нормативных документов по информационной Учебного заведения, планы, политики, , регламенты, инструкции, , перечни и иные виды нормативных документов;
* контроля актуальности и внутренних документов (политик, , методик и т.д.), затрагивающих информационной безопасности заведения;
* , контроль и непосредственная с персоналом Учебного в области обеспечения 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 Учебного заведения;
* 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 Учебного заведения;
* контроль обеспечения информационной безопасности Учебного заведения, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;
* информирование руководства Учебного заведения и руководителей его самостоятельных структурных подразделений Учебного заведения об угрозах информационной безопасности, влияющих на деятельность Учебного заведения.

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 Учебного заведения на основе совмещения работы в группе со своими основными должностными обязанностями.

Финансирование работ по реализации положений настоящей Политики осуществляется как в рамках целевого бюджета Ответственного подразделения Учебного заведения, так и в рамках бюджетов бизнес-подразделений и подразделений ИТ-блока.

Основными функциями Куратора в вопросах информационной безопасности являются:

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

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

* соблюдение требований информационной безопасности, устанавливаемых нормативными документами Учебного заведения;
* 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 Учебного заведения.

**3.2.6. Сферы ответственности**

Общее руководство обеспечением информационной безопасности Учебного заведения осуществляет Куратор.

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

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

**3.2.7. Ключевые результаты**

Инциденты информационной безопасности не должны приводить серьёзным непредвиденным затратам или серьёзным срывам работы служб и деятельности Учебного заведения.

Потери из-за мошенничества должны быть известны и находится в рамках приемлемых ограничений.

Вопросы информационной безопасности не должны оказывать неблагоприятного влияния на учебный процесс или деятельность Учебного заведения.

# 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 проектирование и частично создание 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 учебного заведения.

Стоит отметить, что этап создания 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. Об информации, информатизации и защите информации: Закон Респ. Беларусь, 10 ноября 2008 г., № 455-3 // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2012.
2. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация: СТБ 34.101.30–2007. – Введ. 01.04.2008. – Минск: Белорус. гос. ин–т стандартизации и сертификации, 2007. – 8 с.
3. Менеджмент информационной безопасности: основные концепции / А.В. Дорофеев [и др.] // Вопросы кибербезопасности. – 2014. – №1 (2). – С.67–73.
4. О некоторых вопросах технической и криптографической защиты информации: Приказ Оперативно–аналитического центра при Президенте Республики Беларусь, 30 августа 2013 г., № 62 // Эталон–Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2012.
5. Общие сведения [Электронный ресурс] / Оперативно-аналитический центр при Президенте Республики Беларусь. – Минск, 2016. – Режим доступа: http://oac.gov.by/tzi/protection/comments.html – Дата доступа: 25.12.2016
6. Создание СМИБ | Информационная безопасность [Электронный ресурс] / Softline. – Минск, 2016 – Режим доступа: http://itsec.by/sozdanie-sistemy-menedzhmenta-informacionnoj-bezopasnosti-smib/ – Дата доступа: 25.12.2016
7. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь: СТБ ISO/IEC 27000-2012. – Введ. 01.01.2013. – Минск: Белорус. гос. ин-т стандартизации и сертификации, 2012. – 24 с.
8. Дорофеев, А.В. Менеджмент информационной безопасности: управление рисками / А.В. Дорофеев // Вопросы кибербезопасности. – 2014. – №2 (3). – С.66–73.
9. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности: СТБ 34.101.2–2014. – Введ. 01.09.2014. – Минск: Белорус. гос. ин–т стандартизации и сертификации, 2014. – 186 с.
10. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учеб. пособие / Ю.А. Родичев – Ростов н/Д: «Издательский дом «Питер»», 2016. – 256 с.
11. Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности: СТБ ISO/IEC 27003-2014. – Введ. 01.02.2015. – Минск: Белорус. гос. ин–т стандартизации и сертификации, 2014. – 68 с.