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

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 старонкі, 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.

4. Определение потенциальных угроз для объекта защиты и анализ возможных последствий их осуществления (потенциального ущерба).

5. Определение требований к системе защиты информации в техническом задании на информационную систему.

6. 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, определяющее защищенность от несанкционированного изменения. Выделяют логическую и физическую целостность. Физическая целостность представляет собой неизменность физического состояния данных на машинном носителе. Логическая целостность отображает корректность выполнения процессов (транзакций), полноту и непротиворечивость информации, например, в СУБД, файловых системах, электронных архивах, хранилищах данных, системах управления документооборотом и т.д.

Доступность – свойство информации быть доступной за приемлемое время по запросу со стороны санкционированного субъекта [2]. С доступностью часто связывают такую характеристику системы как готовность. Готовность – это способность к выполнению заявленных функций в установленных технических условиях. Атаки, имеющие целью нарушить степень доступности, называются атаками 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.

Угроза и риск являются определяющими факторами информационной безопасности [3].

Угроза – это потенциальная причина (событие, нарушение, инцидент), которая снижает уровень информационной безопасности системы, т.е. которая может привести к нежелательным последствиям, а также причинить вред системе (организации).

Риск представляет собой возможный ущерб, т.е. комбинацию (как правило, произведение) вероятности реализации угрозы и ущерба от нее. Можно отметить, 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 данного понятия подпадает все, что имеет значимость для организации. Можно привести примеры активов в информационной сфере: информация, программное обеспечение, аппаратное обеспечение, информационная система (сложный актив, включающий предыдущие), человек, имидж организации. В итоге, активами становятся все те объекты, которые должны быть защищены путем выстраивания процессов информационной безопасности.

Угрозы классифицируют по ряду критериев [3]:

- 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).

На рисунке 1.1 приведены примеры угроз информационной безопасности.

Направления обеспечения безопасности	Техногенные		Природные
	Преднамеренные	Случайные	
Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо
Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
Управление коммуникациями	Прослушивание сети	Флуктуации в сети	Магнитные бури
Защита информационных хранилищ	Взлом парольной системы	Сбой криптосредств	Грибки
Управление непрерывностью деятельности	Последствие DOS-атаки	Последствия тестов на проникновения	Карстовые процессы
Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

Рисунок 1.1 – Примеры угроз информационной безопасности

Достаточно 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. Уязвимость – это реализационный дефект («слабость»), который снижает уровень защищенности ресурсов от любых угроз. Необходимо отметить, что 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, которая причиняет вред организации, называется атакой на ресурсы.

Повышение и обеспечение заданных уровней защиты ресурсов осуществляется путем применения мер (механизмов) безопасности. На профессиональном жаргоне такие меры нередко 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. К техническим контролям относятся 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). Неплохими примерами физических контролей являются

решетки, двери, заборы – все что ограничивает физический доступ к нашим активам.

Контроли могут служить для разнообразных целей, например, быть превентивными, детективными, корректирующими, восстанавливающими и другими.

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

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

1.2 Средства защиты информации

При осуществлении технической защиты информации используются средства технической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь [4].

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.

Программные средства защиты информации – это средства, 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 [5].

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 – это 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 котором права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

Журналирование – процесс записи информации о происходящих с некоторым объектом (или в рамках некоторого процесса) событиях в журнал (например, в файл). Также часто это процесс называют аудит.

2. 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, которые пересекают периметр защищаемой информационной системы. Если в данном потоке обнаруживается конфиденциальная информация, то срабатывает активная компонента системы и происходит блокировка передачи (потока, сообщения, сессии).

3. 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.

4. 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.

5. 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, которые заданы в конфигурации.

6. Криптографические средства.

7. 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.

8. Системы аутентификации.

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

Аутентификацию часто путают с идентификацией и авторизацией, однако необходимо четко разделять данные понятия.

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.

9. Системы резервного копирования.

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

1.3 Классификация объектов информатизации

Согласно пункту 9.2 приказа оперативно-аналитического центра при президенте РБ «О некоторых вопросах технической и криптографической защиты информации», №62 от 30.08.2013, одним из этапов проектирования системы защиты информации, является «присвоение информационной системе класса типового объекта информатизации» [4].

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 [2]:

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

и по организации вычислительных процессов:

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

В соответствии со стандартом могут быть следующие классы ОИ:

- Класс А1 — ТС ОИ размещены в пределах одной КЗ, в пределах области действия КСБО обрабатываются сведения, отнесенные к гос. секретам;
- Класс А2 — ТС ОИ размещены в пределах одной КЗ, в пределах области действия КСБО обрабатывается служебная информация ограниченного распространения;
- Класс А3 — ТС ОИ размещены в пределах одной КЗ, в пределах области действия КСБО обрабатывается открытая информация;
- Класс Б1 — ТС ОИ размещены в нескольких КЗ, объединённых защищенными каналами передачи данных, в пределах области действия КСБО обрабатываются сведения, отнесенные к гос. секретам;
- Класс Б2 — ТС ОИ размещены в нескольких КЗ, объединённых защищенными каналами передачи данных, в пределах области действия КСБО обрабатывается служебная информация ограниченного распространения;

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

ГЛАВА 2
ПРОЕКТИРОВАНИЕ СЗИ

2.1 Анализ организационной структуры информационной системы

Определение области применения системы защиты информации включает в себя следующие пункты [6]:

- 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.

Можно выделить главные задачи учебного заведения:

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.

Каждая организация имеет свою структуру. Во главе высшего учебного стоит ректор. Его заместителями по различным направлениям работы являются

проректоры, которые решают оперативные и тактические вопросы работы ВУЗа. Стратегические вопросы развития вуза обычно решает его Учёный совет.

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

Организационная структура учебного заведения представлена на рисунке 2.1.

Рисунок 2.1 – Организационная структура учебного заведения

Для более детального понимания рассмотрим организационную структуру кафедры. Главным исполнительным органом кафедры является заведующий кафедрой, в его подчинении находятся заместитель кафедры, преподавательский состав, лаборатории вместе с сопутствующим персоналом и методисты.

Организационная структура кафедры учебного заведения представлена на рисунке 2.2.

Рисунок 2.2 – Организационная структура кафедры учебного заведения

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

2.2 Классификация информации, хранящейся и обрабатываемой в информационной системе

Учебное заведение – это достаточно большое предприятие, поэтому оно имеет достаточно много информации, хранящейся и обрабатываемом в ИС. Ниже приведены некоторые виды информации:

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

Вся эта информация является информацией ограниченного распространения и должна быть защищена.

Также в ИС учебного заведения имеется общедоступная информация, так как:

- расписание занятий;

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

2.3 Проведение оценки угроз и рисков для ИС

Риск информационной безопасности – это потенциальная возможность понести убытки из-за нарушения безопасности информационной системы [7].

Ниже приведены параметры, характеризующие риск:

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

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

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

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

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

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

До применения каких-либо шагов по оценке рисков, необходимо 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. В таблице 2.1 приведена классификация последствий.

Таблица 2.1 – Классификация последствий

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

Для оценки вероятности реализации ограничимся следующими критериями: имеющаяся статистика по аналогичным инцидентам, требуемые затраты на реализацию угрозы и возможность обнаружения. Оценка вероятностей реализации угроз отражена в таблице 2.2.

Таблица 2.2 – Оценка вероятностей реализации угроз

Вероятность	Статистика инцидентов	Затраты на реализацию угрозы	Возможность обнаружения
Высокая (В)	Аналогичный инцидент происходит каждую неделю.	Интеллектуальные: невысокая квалификация злоумышленника. Инструменты для реализации угрозы общедоступны.	Угрозу и ее источник очень сложно обнаружить.
Средняя (С)	Аналогичный инцидент происходит 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 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 сопоставляется вероятность реализации угрозы с размерами последствий от её реализации и получить значения рисков. В таблице 2.3 отражены значения рисков.

Таблица 2.3 – Значение рисков

Последствия / Вероятность	Н	С	В
Н	Н	Н	С
С	Н	С	В
В	С	В	В

После определения критериев, которые будем использоваться 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 [9]. Угрозы для исследуемых видов информации приведены в таблице 2.4.

Таблица 2.4 – Угрозы для исследуемых видов информации

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

2.4 Разработка технического задания

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

Техническое задание на систему защиты информации строиться по следующему плану:

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

С перечнем требований, подлежащих включению в техническое задание на систему защиты информации можно ознакомиться в Приложении А.

2.5 Техническое задание на систему защиты информации

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

2.5.1.1 Полное наименование системы

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

2.5.1.2 Наименование реквизитов разработчика и заказчика СЗИ

Заказчик: *НАЗВАНИЕ УЧЕБНОГО ЗАВЕДЕНИЯ*.

Адрес: *АДРЕС УЧЕБНОГО ЗАВЕДЕНИЯ*.

Исполнитель: *НАЗВАНИЕ ФИРМЫ*

Адрес: *АДРЕС ФИРМЫ.*

2.5.1.3 Перечень документов, на основании которых создаётся СЗИ

Для формирования требований были использованы документы, разработанные на предыдущих этапах создания СЗИ, которые приведены в таблице 2.5.

Таблица 2.5 – 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 2.6.

Таблица 2.6 – Перечень основных руководящих и нормативно-технических документов

№ п/п	Наименование документа
1	СТБ 34.101.1–2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель».
2	СТБ 34.101.2–2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности».
3	СТБ 34.101.3–2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности».
4	СТБ 34.101.8–2006 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования».
5	СТБ 34.101.28–2011 «Информационные технологии. Средства защиты речевой информации от утечки по акустическому и виброакустическому каналам. Общие технические требования»
6	СТБ 34.101.29–2011 «Информационные технологии. Средства контроля защищенности речевой информации. Общие технические требования»
7	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.

2.5.2 Назначение и цели создания системы

2.5.2.1 Назначение системы защиты

СЗИ предназначена для работы сотрудников учебного заведения.

2.5.2.2 Цели создания системы защиты

Цель создания данной системы защиты – защита информации учебного заведения.

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

2.5.2.3 Краткая характеристика информационной системы, структура

Данная система представляет из себя информационную систему учебного заведения.

2.5.2.4 Размещение СЗИ

СЗИ будет расположена по адресу *АДРЕС*.

2.5.2.5 Охрана и пропускной режим

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

2.5.2.6 Контролируемая зона

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

2.5.2.7 Схема информационного взаимодействия объектов в ИС

Схема информационного взаимодействия объектов отображена на рисунке 2.3.

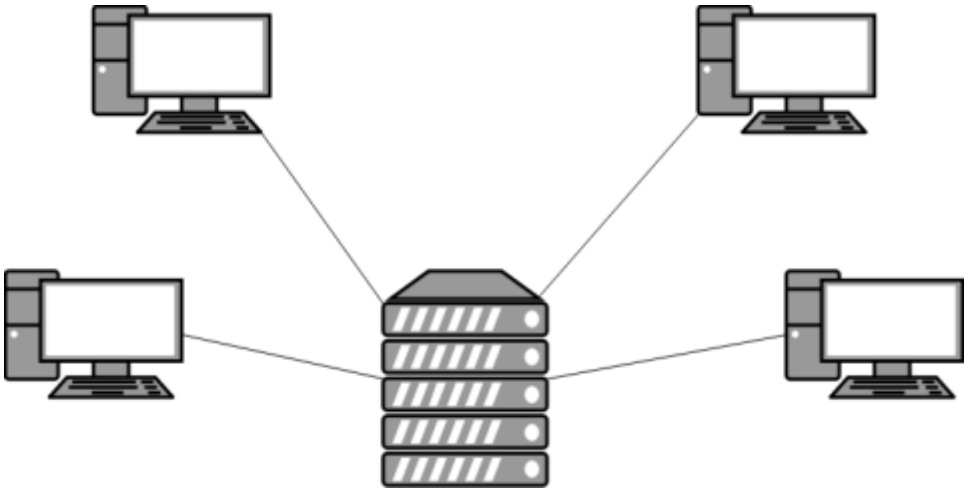

Рисунок 2.3 – Схема информационного взаимодействия объектов

Информационная система не имеет выхода в сети общего пользования.

2.5.2.8 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.

2.5.3 Требования к системе защиты информации ИС

2.5.3.1 Требования к функциям (задачам), выполняемым системой.

- Идентификация объектов ИС (далее – объекты) и закрепление за ними субъектов ИС (далее – субъекты);
- Идентификация и аутентификация субъектов;
- Управление идентификаторами (создание, присвоение, уничтожение);
- Управление средствами аутентификации (хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты/компрометации средств аутентификации);
- Исключение отображения аутентификационной информации;
- Изменение атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности;
- Полномочное управление (создание, активация, блокировка, уничтожение) учетными записями субъектов;

- Определение обязанностей и прав субъектов;
- Реализация правил разграничения доступа субъектов к объектам;
- Блокирование доступа к ИС по истечению установленного времени неактивности субъекта или по его запросу;
- Определение возможных действий субъектов, которые могут совершаться до их идентификации и аутентификации (при необходимости);
- 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 и регламентация порядка установки и использования разрешенного программного обеспечения;
- 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, которая хранится на учтенных машинных носителях информации;
- Уничтожение 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 событий безопасности уполномоченными субъектами
- Сбор, хранение, запись, мониторинг информации о сбоях в механизмах сбора информации и достижении предела объема памяти устройств хранения уполномоченными пользователями;
- Синхронизация временных меток в информационной системе;
- Синхронизация системного времени в информационной системе;
- Защита информации о событиях безопасности;

- Регламентация обновления базы данных признаков вредоносного программного обеспечения;
- Регламентация проведения проверок операционных систем на предмет обнаружения аномалий, которые вызваны присутствием вредоносного программного обеспечения в системе;
- Выявление уязвимостей информационной системы и их оперативное 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;
- 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 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 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.

2.5.3.2 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

2.5.3.3 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.

2.5.3.4 Требования по эксплуатации и техническому обслуживанию

Необходимо обеспечить бесперебойное питание ПЭВМ для нормальной эксплуатации разрабатываемой системы. 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 технических средств и оборудования 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.

2.5.3.5 Требования к патентной чистоте

По всем техническим и программным средствам, которые применяются 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.

2.5.3.6 Требования к эргономике и технической эстетике

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав системы должно осуществляться посредством визуального графического интерфейса (GUI). Главное требование к интерфейсу системы: он должен быть понятным и удобным, также он не должен быть перегружен графическими элементами и обеспечивать быстрое

отображение всех 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. В интерактивном режиме необходимо обеспечить выполнение ввода-вывода данных системы, прием управляющих команд и отображение результатов их исполнения. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям системы. Управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов, поэтому интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь» Клавиатурный режим ввода должен используется главным образом при заполнении (редактировании) полей ввода экранных форм. Все надписи экранных форм, а также сообщения, выдаваемые пользователю (не учитываются системные сообщения) должны быть на русском языке.

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

Этапы работы по созданию СЗИ отражены в таблице 2.7.

Таблица 2.7– Этапы работы по созданию СЗИ

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	

Продолжение таблицы 2.7

3	Присвоение информационной системе класса типового объекта информатизации в порядке, установленном СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация»	
4	Определение требований к системе защиты информации в техническом задании на информационную систему	Техническое задание
5	Согласование технического проекта. Разработанный технический проект отправляется на ознакомление и согласование заказчику. В ходе этого этапа могут быть внесены дополнения и изменения в проект, если это потребуется. Итогом согласования проекта является подписание его сторонами	
6	Разработка политики информационной безопасности	Политика безопасности
7	Внедрение планируемых к использованию средств защиты информации, проверка их работоспособности и совместимости	В ходе внедрения средств защиты информации осуществляется их монтаж и наладка в соответствии с эксплуатационной документацией.
8	Внедрение организационных мер защиты информации осуществляется в целях реализации требований, изложенных в локальных нормативных правовых актах организации, которые доводятся до сведения субъектов информационной системы под подпись	

Продолжение таблицы 2.7

9	Опытная эксплуатация системы защиты информации	Опытная эксплуатация системы защиты информации осуществляется для проверки ее работоспособности в различных режимах функционирования информационной системы, в том числе при необходимости в условиях чрезвычайной ситуации. В случае выявления в процессе опытной эксплуатации системы защиты информации недостатков осуществляется их устранение с последующей повторной опытной эксплуатацией
10	Приемочные испытания системы защиты информации	Приемочные испытания системы защиты информации проводятся в целях проверки выполнения требований к системе защиты информации, изложенных в задании по безопасности или в техническом задании
11	Аттестация СЗИ	Аттестат соответствия. Наличие аттестата соответствия является основанием для ввода информационной системы в эксплуатацию и использования ее в течение срока, установленного в аттестате соответствия
12	Ввод системы в эксплуатацию	Акт ввода системы в промышленную эксплуатацию

2.5.3.8 Требования к разработчику системы защиты

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

2.5.4 Порядок контроля и приёмки системы

2.5.4.1 Порядок проведения приёмки

Испытания СЗИ проводятся на объекте заказчика.

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

На основании решения о приемке осуществляется подписание комиссией акта приемки.

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

ГЛАВА 3
СОЗДАНИЕ СЗИ

3.1 Разработка политики безопасности

В соответствии с Приказом Оперативно-аналитического центра при Президенте Республики Беларусь №62 «О некоторых вопросах технической и криптографической защиты информации» на этапе создания системы защиты информации осуществляются разработка политики информационной безопасности [4].

Политика безопасности – совокупность правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности [10].

Организация может иметь несколько политик, по одной для каждой сферы деятельности, важной для организации. Некоторые политики независимы между собой, в то время как другие политики находятся в иерархическом соотношении. В области безопасности политики, как правило, иерархически организованы. Обычно политика безопасности является политикой высшего уровня. В свою очередь, политика информационной безопасности может подкрепляться более детальными политиками по конкретным предметам, такими как: политика контроля доступа, политики «чистого стола» и «чистого экрана», политика использования сетевых служб и др. [11]. Иерархия политик отображена на рисунке 3.1.

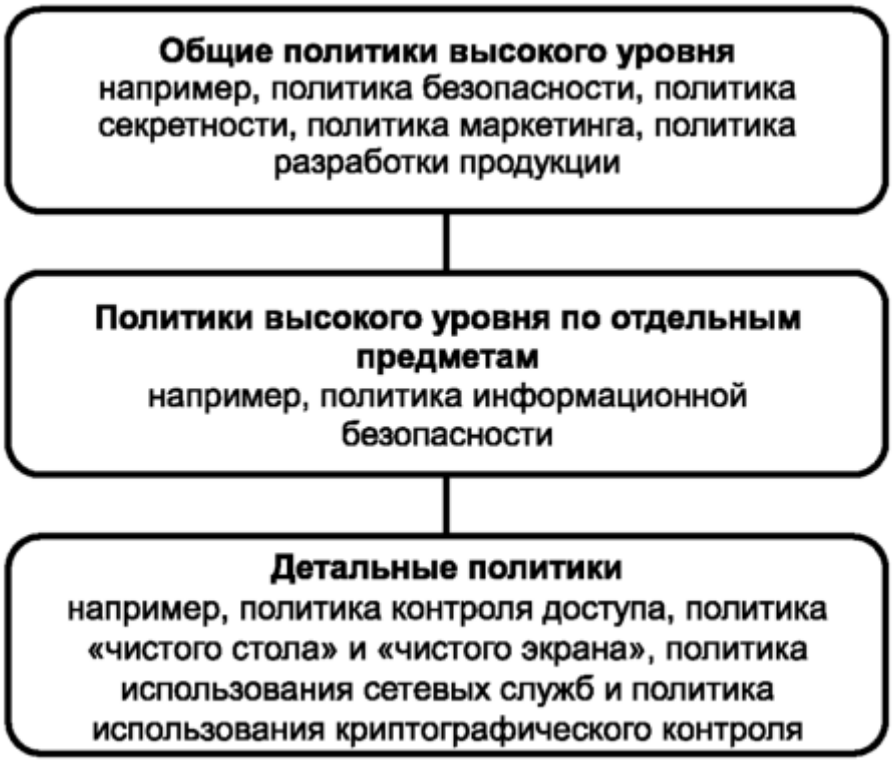

Рисунок 3.1 – Иерархия политик

Содержание политики основано на контексте, в котором работает организация. Однако Приказом Оперативно-аналитического центра при Президенте Республики Беларусь №62 «О некоторых вопросах технической и криптографической защиты информации» выделяется перечень пунктов, которые должна содержать политика [4]:

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

3.2 Политика безопасности

3.2.1. Краткое изложение политики

Независимо от формы представления, способа распространения, передачи и хранения, информация всегда должна быть защищена.

3.2.2. Введение

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

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

Настоящая Политика является документом, доступным любому сотруднику учебного заведения и пользователю его ресурсов, и представляет собой официально принятую руководством НАЗВАНИЕ УЧЕБНОГО ЗАВАДЕНИЯ (далее – Учебное заведение) систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Учебного заведения.

Руководство Учебного заведения осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования образовательной деятельности, а также развития реализуемых учебным заведением технологий и ожиданий сотрудников, студентов и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества Учебному заведению, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

Требования информационной безопасности, которые предъявляются Учебным заведением, соответствуют целям и интересам деятельности Учебного заведения и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Учебного заведения имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами,

внутрихозяйственной деятельности. Факторы рисков в информационной сфере Учебного заведения составляют значимую часть операционных рисков Учебного заведения, а также имеют отношение и к иным рискам основной и управленческой деятельности Учебного заведения.

Необходимые требования обеспечения информационной безопасности Учебного заведения должны обязательно соблюдаться персоналом Учебного заведения и другими сторонами как это определяется положениями внутренних нормативных документов Учебного заведения, а также требованиями договоров и соглашений, стороной которых является Учебное заведение.

Настоящая Политика распространяется на бизнес-процессы Учебного заведения и обязательна для применения всеми сотрудниками и руководством Учебного заведения, а также пользователями его информационных ресурсов.

Положения настоящей Политики должны быть учтены при разработке политик информационной безопасности в дочерних и аффилированных организациях.

Настоящая Политика является корпоративным документом по ИБ первого уровня.

Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Учебного заведения, являются частные политики по обеспечению ИБ (далее – Частные политики), которые являются документами по ИБ второго уровня, оформляются как отдельные внутренние нормативные документы Учебного заведения, разрабатываются и согласовываются в соответствии с установленным в Университете порядком, утверждаются Куратором.

3.2.3. Область действия

Основными объектами защиты системы информационной безопасности в Университете являются:

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

3.2.4. Цели информационной безопасности

Целью деятельности, обеспечивающей информационную безопасность Учебного заведения, является снижение угроз информационной безопасности до приемлемого для Учебного заведения уровня.

Основные задачи деятельности по обеспечению информационной безопасности Учебного заведения:

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

3.2.5. Принципы информационной безопасности

Потенциальные угрозы безопасности информации подразделяются на три класса в зависимости от природы их возникновения: антропогенные, техногенные и естественные.

Деятельность человека обуславливает возникновение антропогенных угроз. Среди данных угроз можно выделить те, которые возникают вследствие непреднамеренных действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и др., так и другую группу угроз, которые возникают в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Антропогенные угрозы – это угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Учебного заведения и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

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

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

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

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

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

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

Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Университетом рассматриваются:

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

Внешние нарушители.

В качестве потенциальных внешних нарушителей Университетом рассматриваются:

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

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

- нарушитель скрывает свои несанкционированные действия от других сотрудников Учебного заведения;
- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а

также недостатков принятой технологии обработки, хранения и передачи информации;

- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

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

Руководство Учебного заведения приветствует и поощряет в установленном порядке деятельность работников Учебного заведения и пользователей информационных систем по обеспечению информационной безопасности.

Неисполнение или некачественное исполнение сотрудниками Учебного заведения и пользователями информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение административных мер воздействия к виновным, степень которых определяется установленным в Университете порядком либо требованиями действующего законодательства.

Стратегия Учебного заведения в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Учебного заведения, до специализированных мер информационной безопасности по каждому выявленному в Университете риску, основанных на оценке рисков информационной безопасности.

При планировании мероприятий по обеспечению информационной безопасности в Университете осуществляются:

Определение и распределение ролей персонала Учебного заведения, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.

Менеджмент рисков информационной безопасности, включающий:

- анализ влияния на информационную безопасность Учебного заведения применяемых в деятельности Учебного заведения технологий, а также внешних по отношению к Университету событий;

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

В рамках реализации деятельности по обеспечению информационной безопасности в Университете осуществляются:

- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;

- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства Учебного заведения информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
- повышение уровня знаний персонала Учебного заведения в вопросах обеспечения информационной безопасности;
- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Учебного заведения и информации, обрабатываемой в них;
- применение средств криптографической защиты информации;
- обеспечение бесперебойной работы автоматизированных систем и сетей связи;
- обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем Учебного заведения, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);
- контроль доступа в здания и помещения Учебного заведения.
- применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме – пассивная защита;
- применение мер и технических средств, создающих помехи при несанкционированном получении информации – активная защита;
- применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации – поиск.

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

- контроль правильности реализации и эксплуатации защитных мер;

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

В целях совершенствования деятельности по обеспечению информационной безопасности в Университете производится периодическое, а при надобности оперативное, уточнение (пересмотр) целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Учебного заведения).

В целях выполнения задач по обеспечению информационной безопасности Учебного заведения, в соответствии с рекомендациями международных стандартов по безопасности в Университете должны быть определены следующие роли:

- Куратор;
- Ответственное подразделение;
- Сотрудник Учебного заведения.

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

Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Учебного заведения осуществляются и координируются Ответственным подразделением. Задачами Ответственного подразделения являются:

- установление потребностей Учебного заведения в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
- соблюдение действующего законодательства, нормативных актов органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, нормативных актов по обеспечению информационной безопасности;
- разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Учебного заведения, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;

- осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Учебного заведения;
- обучение, контроль и непосредственная работа с персоналом Учебного заведения в области обеспечения информационной безопасности;
- планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Университете;
- выявление и предотвращение реализации угроз информационной безопасности;
- выявление и реагирование на инциденты информационной безопасности;
- информирование в установленном порядке ответственных лиц об угрозах и рисковых событиях информационной безопасности;
- прогнозирование и предупреждение инцидентов информационной безопасности;
- пресечение несанкционированных действий нарушителей информационной безопасности;
- поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение персонала;
- типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на филиалы и представительства 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-З // 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.

ПРИЛОЖЕНИЕ А

Таблица А.1 – Перечень требований к системе защиты информации, подлежащих включению в задание по безопасности на информационную систему или в техническое задание на информационную систему

№ п/п	Требования к системе защиты информации, подлежащие включению в задание по безопасности на информационную систему или в техническое задание на информационную систему	Класс объекта информатизации		
		А2	Б2	В2
1	Идентификация объектов информационной системы (далее – объекты) и закрепление за ними субъектов информационной системы (далее – субъекты)	+	+	+
2	Идентификация и аутентификация субъектов	+	+	+
3	Управление идентификаторами, в том числе создание, присвоение, уничтожение	+	+	+
4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+
5	Исключение отображения аутентификационной информации (защита обратной связи при вводе аутентификационной информации)	+	+	+
6	Изменение атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности	+	+	+
7	Полномочное управление (создание, активация, блокировка и уничтожение) учетными записями субъектов	+	+	+
8	Определение прав и обязанностей субъектов	+	+	+
9	Реализация правил разграничения доступа субъектов к объектам	+	+	+
10	Контроль за соблюдением правил генерации и смены паролей субъектов	+	+	+
11	Ограничение неуспешных попыток аутентификации	+	+	+
12	Блокирование доступа к информационной системе после истечения установленного времени бездействия (неактивности) субъекта или по его запросу	+	+	+
13	Определение при необходимости действий субъектов, которые могут совершаться такими субъектами до их идентификации и аутентификации	+	+	+
14	Реализация защищенного удаленного доступа субъектов к объектам через внешние информационно-телекоммуникационные сети	–	–	+
15	Наличие актуальной схемы сети с указанием объектов, внешних подключений и информационных потоков	±	+	+
16	Управление (фильтрация, маршрутизация, контроль соединений) информационными потоками между объектами, а также между информационными системами	±	+	+
17	Ограничение входящего и исходящего трафика только необходимыми соединениями	–	+	+
18	Запрет на использование в информационной системе технологий беспроводного доступа	+	+	+
19	Регламентация порядка использования в информационной системе мобильных технических средств и контроля за таким использованием	+	+	+
20	Регламентация порядка взаимодействия с информационными системами третьих лиц (внешние информационные системы), контроля за таким взаимодействием и управления подключением	–	–	+
21	Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования	+	+	+
22	Учет машинных носителей информации, использующихся для обработки и хранения информации	+	+	+
23	Регламентация доступа к учтенным машинным носителям информации	+	+	+
24	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на учтенных машинных носителях информации	+	+	+
25	Исключение возможности использования учтенных машинных носителей информации в информационных системах третьих лиц	±[1]	±[1]	±[1]
26	Контроль за использованием интерфейсов ввода (вывода) информации на машинные носители информации	±[1]	±[1]	±[1]

Продолжение таблицы А.1

27	Контроль за вводом (выводом) информации на машинные носители информации	±[1]	±[1]	±[1]
28	Уничтожение (удаление) данных с машинных носителей информации при их передаче лицам, не являющимся субъектами информационной системы, в том числе для ремонта, технического обслуживания	+	+	+
29	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+
30	Сбор, запись и хранение информации о событиях безопасности в течение установленного срока хранения	+	+	+
31	Мониторинг (просмотр, анализ) событий безопасности уполномоченными субъектами	+	+	+
32	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	+	+	+
33	Синхронизация временных меток и (или) системного времени в информационной системе	±	+	+
34	Защита информации о событиях безопасности	+	+	+
35	Сбор, запись и хранение информации о действиях отдельных субъектов в течение установленного времени хранения, а также регламентирование прав и обязанностей уполномоченных пользователей, осуществляющих просмотр и анализ такой информации	±[1]	±[1]	±[1]
36	Реализация антивирусной защиты	+	+	+
37	Регламентация обновления базы данных признаков вредоносного программного обеспечения	+	+	+
38	Регламентация проведения проверок операционных систем на предмет обнаружения аномалий, вызванных присутствием в системе вредоносного программного обеспечения	+	+	+
39	Реализация подсистемы обнаружения вторжений	–	±[1]	+
40	Обновление базы сигнатур подсистемы обнаружения вторжений	–	±[1]	+
41	Выявление уязвимостей информационной системы и оперативное их устранение	+	+	+
42	Контроль за установкой обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+
43	Контроль за работоспособностью, параметрами настройки и правильностью функционирования программного обеспечения и средств защиты информации	+	+	+
44	Контроль за неизменностью состава технических средств, программного обеспечения и средств защиты информации	+	+	+
45	Регламентирование порядка резервирования информации и программного обеспечения, включая программное обеспечение средств защиты информации	+	+	+
46	Контроль за содержанием информации, передаваемой из информационной системы (основанный на свойствах объекта доступа и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, шаблонов и иных методов)	–	±[1]	+
47	Идентификация и аутентификация субъектов и объектов в виртуальной инфраструктуре, в том числе уполномоченных пользователей по управлению средствами виртуализации	+	+	+
48	Управление доступом субъектов к объектам в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+
49	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+
50	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+	+	+
51	Контроль за обеспечением целостности виртуальной инфраструктуры и ее конфигураций	+	+	+
52	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	+	+	+

Продолжение таблицы А.1

53	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+	+
54	Деление виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки в них информации отдельным пользователем и (или) группой пользователей	+	+	+
55	Установление контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации	+	+	+
56	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	+	+	+
57	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации	+	+	+
58	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе по беспроводным каналам связи	–	+	+
59	Обеспечение доверенного канала между рабочими местами уполномоченных пользователей и объектами, на которых данные уполномоченные пользователи осуществляют администрирование, мониторинг, а также иные определенные (в соответствии с правами и обязанностями) функции	+	+	+
60	Контроль за обеспечением санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи	±	+	+
61	Контроль за обеспечением санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	±	+	+
62	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	±[1]	±[1]	±[1]
63	Исключение возможности отрицания пользователем факта отправки информации другому пользователю, а также получения информации от другого пользователя	±[1]	±[1]	±[1]
64	Защита архивных файлов, параметров настройки средств защиты информации, программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	+	+	+
65	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов	+	+	+
66	Деление информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	±[1]	+	+
67	Запрет на использование незащищенного подключения к другим информационным системам	±	+	+
68	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	±[1]	±[1]	±[1]
69	Защита периметра информационной системы при ее взаимодействии с иными информационными системами и при использовании сетей электросвязи общего пользования, в том числе глобальной компьютерной сети Интернет	–	+	+
70	Прекращение сетевых соединений по их завершении или по истечении заданного временного интервала неактивности сетевого соединения	±	+	+

Продолжение таблицы А.1

71	Использование в информационной системе или в ее сегментах различных типов общесистемного программного обеспечения	±[1]	±[1]	+
72	Воспроизведение ложных и (или) сокрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы	–	±[1]	±[1]
73	Регламентирование порядка доступа к настройкам средств защиты и контроль за таким доступом	+	+	+
74	Реализация комплекса мер по криптографической защите информации, обрабатываемой в информационной системе и (или) передаваемой за пределы такой системы в соответствии с требованиями, изложенными в Положении о порядке криптографической защиты информации в государственных информационных системах, информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации	+	+	+

Примечание. Обозначения, используемые в настоящем приложении, означают:

«+» – обязательные требования;

«–» – необязательные требования;

«±» – обязательные требования к системе защиты информации информационной системы, организованной посредством локально-вычислительной сети;

«±[1]» – требования, обязательность использования которых определяется руководителем собственника (владельца) информационной системы.