МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ  
Учреждение образования  
«Белорусский государственный технологический университет»  
  
  
  
  
  
  
Отчёт по лабораторной работе №1

РАЗРАБОТКА И ВНЕДРЕНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ИЛИ УЧРЕЖДЕНИЯ

Выполнил: студент 3 курса специальности ИСиТ Калоша И.В.  
Проверила: Ржеутская Н. В.

Минск 2020

**Цели и задачи политики безопасности**

Политика информационной безопасности (далее – Политика ИБ) предназначена для специалистов по обеспечению безопасности информации, руководителей и организаторов работы по обработке подлежащей защите информации в Учреждении.

Защитные меры ИБ в Учреждении – это действия, процедуры и механизмы, способные обеспечить соответствующий уровень защиты от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление информации. Эффективная безопасность требует комбинации различных защитных мер для обеспечения заданных уровней безопасности при защите информации.

Для достижения основной цели защиты и обеспечения ИБ Учреждения должна обеспечивать эффективное решение следующих задач:

1. защиту от несанкционированного доступа в процессе функционирования Учреждения;
2. разграничение уровня доступа авторизованных пользователей к аппаратным, программным средствам Учреждения (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы для выполнения своих должностных обязанностей)
3. регистрацию действий авторизованных пользователей при использовании защищаемых ресурсов Учреждения в системных журналах и периодический анализ сведений, содержащихся в них, работниками специализированного подразделения по информационной безопасности;
4. контроль целостности среды исполнения программ и ее восстановление в случае нарушения;
5. защиту от несанкционированной модификации и контроль целостности используемых в информационной системе Участников программных средств, а также защиту информационной системы от внедрения несанкционированных и (или) вредоносных программ;
6. своевременное выявление источников угроз ИБ, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации;
7. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями злоумышленников, ослабление негативного влияния и ликвидация последствий нарушения ИБ.

**Объекты защиты**

Основными объектами защиты системы обеспечения ИБ являются:

* информация, содержащая коммерческую тайну, банковскую тайну, персональные данные физических лиц, другая информация ограниченного доступа;
* 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.

**Структура, состав и размещение основных элементов Учреждения, информационные связи с другими объектами**

ИС Учреждения является распределенной системой, объединяющей ИС Участников в единую вычислительную (информационно – телекоммуникационную) сеть.

Комплекс технических средств ИС Учреждения включает средства обработки данных (персональные ПК, сервера баз данных, файловые сервера и т.п.), средства обмена данными с возможностью выхода в глобальные информационные сети (кабельная система, мосты, шлюзы, модемы и т.д.), а также средства хранения (в т.ч. архивирования) данных. Указанные технические средства распределены по подсистемам различных Участников.

Взаимодействие с ведомствами (федеральными органами исполнительной власти, внебюджетными федеральными фондами) осуществляется посредством Системы межведомственного электронного взаимодействия (СМЭВ).

Взаимодействие между Участниками осуществляется по защищенным каналам связи.

Для защиты информации применяются программные и аппаратные средства криптографической защиты.

К основным особенностям функционирования Учреждения, относятся:

* объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации; широкий диапазон решаемых задач и типов обрабатываемых сведений (данных), сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов авторизованных пользователей;
* объединение в единых базах данных информации различного назначения, принадлежности и конфиденциальности;
* непосредственный доступ к ИС Учреждения большого числа различных категорий пользователей;
* наличие каналов взаимодействия с внешними источниками и потребителями информации;
* непрерывность функционирования Учреждения;
* высокая интенсивность информационных потоков в Учреждении;

Общая структурная и функциональная организация определяется Правилами Учреждения, а также задачами, решаемыми Участниками в зависимости от их роли в Учреждении с применением средств автоматизации.

Объекты информатизации Учреждения включают:

* технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);
* программные средства (операционные системы, системы управления базами данных,
* другое общесистемное и прикладное программное обеспечение;
* автоматизированные системы связи и передачи данных (средства телекоммуникации);
* каналы связи, по которым передается информация (в том числе информация ограниченного доступа);
* служебные помещения, в которых обрабатывается информация ограниченного доступа.

**Информация, подлежащая защите**

В ИС Учреждения обрабатывается общедоступная информация и информация ограниченного доступа.

В документообороте Учреждения присутствуют:

* ПДн граждан – работников и пациентов;
* платежные поручения и другие платежные и расчетные документы;
* отчеты (финансовые, аналитические и др.);
* обобщенная информация и другие документы, содержащие информацию ограниченного доступа.

Защите подлежит вся информация, обрабатываемая в Учреждении и содержащая:

* сведения, составляющие банковскую тайну, доступ к которым ограничен в соответствии с законом «О банках и банковской деятельности»;
* ПДн граждан, доступ к которым ограничен в соответствии с законом «О персональных данных»;
* технологическая информация, необходимая для поддержания безопасного функционирования Учреждения.

**Категории пользователей, режимы использования и уровни доступа к информации**

Авторизованные пользователи должны иметь различные уровни доступа к информационным, программным и другим ресурсам:

* пользователи баз данных;
* операторы баз данных;
* администраторы серверов;
* разработчики прикладного программного обеспечения;
* специалисты по обслуживанию технических средств вычислительной техники;
* работники специализированного подразделения по ИБ и др.

У каждого Участника должны быть установлены правила, определяющие разграничение уровня доступа авторизованных пользователей к ИС Учреждения.

**Общая модель угроз и нарушителя Учреждения**

На основании общей модели угроз и нарушителя Учреждения возможна разработка частных моделей угроз и моделей нарушителя для ИС подключенных к Учреждения.

**Угрозы безопасности информации и их источники**

В качестве основных типов угроз безопасности информации в ИС Учреждения рассматриваются нарушение:

* доступности информации подразумевает, что доступ к информации блокируется для авторизованных пользователей. Это может происходить по причине того, что программные или технические средства, при помощи которых осуществляется доступ к информации, потеряли свои потребительские качества и не могут в означенные сроки предоставить пользователю необходимую информацию;
* целостности информации подразумевает, что информация была несанкционированно искажена (разрушена), потеряла достоверность и отличается от информации, которая была сформирована первоначально как исходная информация;
* конфиденциальности информации подразумевает, что информация была перехвачена злоумышленником и защищаемые сведения стали доступны кругу лиц, не имеющих на это соответствующих прав.

Все угрозы безопасности информации в ИС Учреждения подразделяются на два класса:

* угрозы, не являющиеся атаками;
* атаки (потенциальные или проводимые).

К угрозам ИС Учреждения, не являющимся атаками, относятся:

* угрозы, не связанные с деятельностью человека;
* угрозы социально-политического и террористического характера;
* ошибочные действия и/или нарушения, связанные с недобросовестностью, халатностью, безответственностью, некомпетентностью и т.д.;
* угрозы техногенного характера.

К угрозам, не связанным с деятельностью человека, относятся стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.д.), которые могут, в частности, привести к пожарам в помещениях с оборудованием ИС Учреждения, затоплениям этих помещений, их разрушению, выходу из строя оборудования ИС Учреждения. Необходимо отметить, что ликвидация последствий этих угроз связана с возможным проникновением в помещения с оборудованием ИС Учреждения посторонних лиц (пожарные расчеты, спасатели и т.п.), среди которых могут находиться нарушители.

К угрозам социально-политического и террористического характера относятся забастовки, саботаж, локальные конфликты, террористические акты, сопровождаемые нападением на объекты ИС Учреждения, и т.д. Угрозы данного вида могут не только привести к временной неработоспособности ИС Учреждения, выходу из строя оборудования и/или потере, искажению и компрометации информации, но и создать условия, которые может использовать в своих целях нарушитель.

К ошибочным действиям и/или нарушениям, связанным с недобросовестностью, халатностью, безответственностью, некомпетентностью и т.д., в частности, относятся:

* непредумышленное искажение или удаление информации (электронных документов);
* нарушение правил хранения персональной ключевой, аутентифицирующей информации, а также любой другой информации ограниченного доступа;
* предоставление неавторизованным пользователям возможности обработки информации ограниченного доступа, доступа к средствам защиты информации, а так же к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований; внедрение и использование неучтенных программ;
* непредумышленное искажение или удаление программных компонентов автоматизированной системы защиты информации;

Основными угрозами техногенного характера являются:

* аварии (отключение электропитания, системы заземления, аварии системы водоснабжения и канализации, разрушение инженерных сооружений);
* неисправности, сбои, нестабильность параметров системы электропитания, заземления и т.д.;
* помехи и наводки, приводящие к сбоям в работе технических средств ИС Учреждения.

Угрозы ИБ могут быть направлены на следующие компоненты ИС Учреждения:

* серверы информационных систем;
* АРМ администраторов и операторов;
* программно-технические средства защиты;
* программное обеспечение функционально-технологических подсистем Участников;
* сетевую инфраструктуру: маршрутизаторы, коммутаторы и другое активное и пассивное оборудование;

**Описание нарушителей (субъектов атак)**

Возможности потенциальных нарушителей Учреждения существенно зависят от реализованной Политики ИБ и принятыми режимными, организационно-техническими и техническими мерами по обеспечению безопасности.

Все физические лица, имеющие доступ к техническим и программным средствам Учреждения, относятся к источникам угроз и могут рассматриваться как потенциальные нарушители. Согласно проведенному анализу, к потенциальным нарушителям Учреждения можно отнести следующих нарушителей:

* внешнего нарушителя;
* внутреннего нарушителя, имеющего санкционированный доступ к Учреждения, но не имеющего доступа к подлежащей защите информации;
* внутреннего нарушителя, имеющего санкционированный доступ к Учреждения и имеющего доступ к подлежащей защите информации.

С учетом специфики функционирования Учреждения и характера обрабатываемой в ней информации предполагается, что авторизованные пользователи Учреждения, которые имеют права администраторов на осуществление технического управления и обслуживания аппаратных и программных средств, в том числе и средств защиты, включая их настройку, конфигурирование и распределение ключевой и парольной документации относятся к особо доверенным лицам и исключаются из числа потенциальных нарушителей.

**Оценка угроз, рисков и уязвимостей**

**Предположения об имеющейся у нарушителя информации об объектах атак**

Предполагается, что потенциальные нарушители обладают информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой исключается системой обеспечения ИБ.

При определении ограничений на степень информированности потенциального нарушителя рассматривались:

* содержание технической документации на технические и программные компоненты среды функционирования криптосредств;
* долговременные ключи криптосредств;
* все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД по отношению к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.);
* сведения о линиях связи, по которым передается подлежащая защите информация;
* все сети связи, работающие на едином ключе;
* сведения, получаемые в результате анализа любых сигналов от технических средств криптосредств и среды их функционирования, которые может перехватить нарушитель;
* исходные тексты прикладного программного обеспечения ИС.

**Предположения об имеющихся у нарушителя средствах атак**

Предполагается, что потенциальный нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

При определении ограничений на имеющиеся у потенциального нарушителя средства атак рассмотрены:

* аппаратные компоненты криптосредств и среда их функционирования;
* доступные в свободной продаже технические средства и программное обеспечение;
* специально разработанные технические средства и программное обеспечение;
* штатные средства.

Таблица 1.2 — Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | 1 и более раз в год |
| 0,3 | 1 и более раз в месяц |
| 0,4 | 1 и более раз в неделю |
| 0,5 | Ежедневно или чаще |

Далее можно создать таблицу рисков (таблица 1.3). На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем (порогом), например, значением 0,5.

Далее проверяется каждая строка таблицы: превышен или не превышен порог для значения риска, связанного с анализируемой атакой? Если такое превышение имеет место, данная атака должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности (таблица 1.3).

Таблица 1.3 — Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| Нарушение доступности медицинской базы | 3 | 0,1 | 0,3 |
| Нарушение целостности медицинской базы | 2 | 0,2 | 0,4 |
| Нарушение конфиденциальности медицинской базы | 4 | 0,1 | 0,4 |
| Халатность персонала | 1 | 0,4 | 0,4 |
| Спам | 1 | 0,5 | 0,5 |
| Землетрясения, наводнения, ураганы | 5 | 0 | 0 |
| Забастовки, саботаж | 2 | 0,1 | 0,2 |
| Конфликт | 1 | 0,4 | 0,4 |
| Террористический акт | 4 | 0,1 | 0,4 |
| Отключения электричества | 2 | 0,2 | 0,4 |
| Хищение носителей информации и документальных отходов | 4 | 0,1 | 0,4 |
| Вирусы | 2 | 0,3 | 0,6 |
| DDoS атаки | 2 | 0,1 | 0,2 |
| Несанкционированный доступ к оборудованию и медикаментам | 3 | 0,1 | 0,3 |
| Несанкционированный доступ в здание | 1 | 0,4 | 0,4 |
| Итого |  |  | 5,3 |

**Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

Методы обеспечения ИБ разделяются на:

***административно-правовые;***

К административно-правовым методам обеспечения ИБ относится соблюдение требований: законодательства Республики Беларусь в области ИБ, Политик ИБ Оператора и Участников, регламентирующие правила обращения с информацией ограниченного доступа, закрепляющие права и обязанности Участников в процессе обработки и использования информации ограниченного доступа, а также устанавливающие ответственность за нарушения этих требований, препятствуя неправомерной обработке и являющиеся сдерживающим фактором для реализации угроз безопасности злоумышленникам.

***организационно-технические;***

Организационно-технические методы обеспечения ИБ основаны на использовании организационных мер, программных, аппаратных, программно-аппаратных средств, входящих в состав системы обеспечения ИБ и выполняющих функции защиты информации, и направленных на решение следующих задач:

* учет всех подлежащих защите ресурсов ИС (ПДн, других подлежащих защите данных, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
* предотвращение НСД к информации ограниченного доступа и(или) передачи ее лицам, не имеющим права на доступ к такой информации;
* своевременное обнаружение фактов НСД к информации ограниченного доступа;
* недопущение воздействия на технические средства автоматизированной обработки информации ограниченного доступа, в результате которого может быть нарушено их функционирование;
* возможность незамедлительного восстановления данных, модифицированных или уничтоженных вследствие НСД к ним;
* постоянный контроль за обеспечением уровня защищенности информации.
* подготовка персонала (проведение тренингов по ИБ, их правам и обязанностям и контроль знаний)

***экономические.***

Экономические методы обеспечения ИБ включают:

* разработку Оператором и Участниками программ обеспечения ИБ;
* разработка Участниками мер поощрения и наложения штрафных санкций за соблюдение или не соблюдение установленных правил и процедур обработки информации ограниченного доступа.

По времени применения методы обеспечения ИБ разделяются на: превентивные;

Превентивные методы обеспечения ИБ осуществляются на основе применения в процессе эксплуатации Учреждения комплекса организационных, технических и технологических мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИС Участников.

Организационные мероприятия по обеспечению ИБ направлены на организацию:

* деятельности работников, использующих ИС Участников;
* порядка применения информационных технологий в зданиях и сооружениях;
* систематического применения мер по поддержанию штатного функционирования Учреждения.

Технические мероприятия по обеспечению ИБ заключаются в обслуживании, поддержке и управлении составом технических средств Учреждения, обеспечивающих обработку информации ограниченного доступа в Учреждении в защищенном режиме.

Технологические мероприятия по обеспечению безопасности информации направлены на реализацию заданных функций и алгоритмов работы Учреждения, технологий обработки информации ограниченного доступа и защиту программ и данных от преднамеренных и непреднамеренных нарушений.

***восстановительные.***

Осуществление восстановительных методов обеспечения ИБ определяется Правилами Учреждения и внутренними документами Участников, устанавливающими требования к обязательным мероприятиям, проводимым как заблаговременно, так и после возникновения нарушений, угрожающих штатному функционированию Учреждения.

**Основные этапы работ по обеспечению ИБ**

Основные этапы работ по обеспечению ИБ информации ограниченного доступа включают:

* определение объектов защиты;
* установление целей защиты;
* определение угроз объектам защиты;
* установление требований к системе обеспечения ИБ информации;
* создание системы обеспечения ИБ;
* определение порядка контроля.

Определение угроз ИБ проводится путем формирования общей модели угроз и модели нарушителя Учреждения. При этом модель нарушителя формируется как составная часть модели угроз, определяющая возможные специфические угрозы.

Установление требований к системе обеспечения ИБ основано на формировании моделей угроз и нарушителя.