МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №1**

Выполнила студентка 3 курса 5 группы Максимчикова Ю. С.

Проверила: Блинова Е. А.

Минск 2020

**1 Обоснование актуальности, цели и задачи разработки ПИБ в Университете**

Актуальность разработки политики информационной безопасности для Университета объясняется необходимостью создания механизма управления и планирования информационной безопасности. Также ПИБ позволяет совершенствовать следующие направления деятельности Университета:

* упорядочивание бизнес-процессов;
* обеспечение соответствия с правовыми нормами;
* улучшение имиджа и деловой репутации.

Цель системы обеспечения информационной безопасности — создание и постоянное соблюдение в Университете условий, при которых риски, связанные с нарушением безопасности информационных ресурсов Университета, постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска.

Основными задачами деятельности по обеспечению информационной безопасности Университета являются:

* своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем университета;
* снижение рисков Университета, связанных с использованием информационных технологий;
* создание условий для максимальной автоматизации выполнения различных операций Университета и исключения ручных операций при условии минимизации рисков;
* своевременное выявление новых угроз;
* контроль состояния информационной безопасности на всех этапах жизненного цикла автоматизированных информационных систем;
* минимизация потерь Университета при реализации угроз информационной безопасности;
* обеспечение жизнедеятельности Университета и безопасности его информационных ресурсов в условиях форс-мажорных обстоятельств (экономические и политические кризисы, природные и техногенные катастрофы, террористические угрозы и пр.);
* оптимизация затрат на обеспечение информационной безопасности;
* защита от вмешательства в процесс функционирования систем университета посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
* разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам университета — обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей;
* обеспечение аутентификации пользователей, имеющих допуск в информационные сети и участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
* защита от несанкционированной модификации используемых в системах университета программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
* защита информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

**2 Объекты защиты**

Основными объектами защиты системы информационной безопасности в Университете являются:

* информационные ресурсы, содержащие служебную тайну и конфиденциальную информацию, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Университета, независимо от формы и вида ее представления;
* работники Университета и их представители, студенты и другие лица, являющиеся пользователями информационных систем Университета;
* информационная инфраструктура, включающая системы хранения, 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 Основные угрозы и их источники**

Любое лицо, имеющее логический или физический доступ к информационным ресурсам и компонентам соответствующих информационных технологий (программному обеспечению и данным, средствам вычислительной техники, коммуникационному оборудованию и каналам связи) может являться потенциальным злоумышленником. При этом предполагается возможность сговора сотрудника Университета с внешним злоумышленником, но не сговор двух и более сотрудников Университета.

Целью злоумышленника является получение контроля над информационным ресурсом, приводящего к нарушению его доступности, целостности или конфиденциальности.

Для достижения целей злоумышленник может использовать все экономически соизмеримые с потенциальным ущербом способы проведения атак на всех уровнях архитектуры информационных систем.

Источниками угроз информационным ресурсам Университета являются:

* внешние и внутренние злоумышленники;
* ошибочные действия персонала;
* вирусные атаки;
* отказы и сбои оборудования и программного обеспечения;
* техногенные и природные катастрофы;
* террористические угрозы.

**4 Оценка угроз, рисков и уязвимостей**

Цель оценивания рисков состоит в определении характеристик рисков для Университета и его ресурсов. На основе этих данных будут выбраны необходимые средства управления информационной безопасностью.

Для оценки рисков необходима шкала для численной оценки рисков от несанкционированного доступа (НСД) к информационным ресурсам Университета, которая представлена в таблице 4.1.

Таблица 4.1 – Условная численная шкала для оценки ущерба

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Последствий нет |
| 1 | Незначительные последствия |
| 2 | Минимальные последствия |
| 3 | Допустимые последствия |
| 4 | Значительные последствия |
| 5 | Высокая степень существенности последствия |

Также для оценки рисков необходимо учитывать вероятность возникновения атак. Для этого была разработана вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам, которая представлена в таблице 4.2.

Таблица 4.2 – 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 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Следующим этапом является непосредственная оценка рисков с использованием ранее созданных шкал для оценки ущерба и вероятностно-временной. Оценка рисков Университета представлена в таблице 4.3.

Таблица 4.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб \* Вероятность) |
| Затопление | 5 | 0,1 | 0,5 |
| Пожар | 5 | 0,1 | 0,5 |
| Намеренное повреждение | 5 | 0,3 | 1,5 |
| Неисправности в системе электроснабжения | 5 | 0,1 | 0,5 |
| Неисправности в системе водоснабжения | 3 | 0,1 | 0,3 |
| Неисправности в системе кондиционирования воздуха | 1 | 0,2 | 0,2 |
| Ненадлежащее использование ресурсов | 2 | 0,1 | 0,2 |
| Аппаратные отказы | 5 | 0,4 | 2 |
| Колебания напряжения | 2 | 0,5 | 1 |
| Воздействие пыли | 1 | 0,5 | 0,5 |
| Кража | 5 | 0,4 | 2 |
| Несанкционированное использование носителей данных | 5 | 0,3 | 1,5 |
| Ошибка при обслуживании | 4 | 0,3 | 1,2 |
| Программные сбои | 3 | 0,4 | 1,2 |
| Использование программного обеспечения несанкционированными пользователями | 4 | 0,4 | 1,6 |
| Использование сетевых средств несанкционированным способом | 2 | 0,3 | 0,6 |
| Вредоносное программное обеспечение | 5 | 0,4 | 2 |
| Ошибка операторов | 3 | 0,1 | 0,3 |
| Нелегальное проникновение злоумышленников под видом санкционированных пользователей | 5 | 0,4 | 2 |
| Доступ несанкционированных пользователей к сети | 2 | 0,5 | 1 |
| Повреждение линий | 3 | 0,2 | 0,6 |
| Перехват информации | 5 | 0,5 | 2,5 |
| Несанкционированное проникновение к средствам связи | 3 | 0,5 | 1,5 |
| Технические неисправности сетевых компонентов | 1 | 0,2 | 0,2 |
| Несанкционированное проникновение к средствам связи | 5 | 0,4 | 2 |
| Ошибки пользователей | 1 | 0,5 | 0,5 |
| Ухудшение состояния носителей данных | 2 | 0,4 | 0,8 |
| Итого | 92 | 8,6 | 28,7 |

Таким образом, можно сделать выводы, что наиболее уязвимыми активами являются персональные данные и сведения, содержащие служебную тайну, а также аппаратное и программное обеспечение.

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

**5.1 Назначение и распределение ролей, и обеспечение доверия к персоналу**

«Ролевое» управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах.

Роли формируются с учетом принципа минимальности полномочий.

Ни одна роль не должна позволять пользователю проводить единолично критичные операции.

Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных системах без непосредственного доступа к данным.

В критичных системах по решению владельца информационного ресурса может вводиться роль администратора информационной безопасности автоматизированной системы, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.

Должностные обязанности сотрудников и трудовые договоры предусматривают обязанности персонала по выполнению требований по обеспечению информационной безопасности.

Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным нарушениям, доводятся до всех сотрудников Университета под роспись.

**5.2 Управление доступом к информационным ресурсам и регистрация**

Все информационные ресурсы Университета идентифицируются, категорируются и имеют своих владельцев.

Доступ к информационным ресурсам всем сотрудникам Университета предоставляется только на основании документально оформленных заявок, согласованных с их владельцами. По умолчанию определяется отсутствие доступа.

Доступ к информационным ресурсам не предоставляется (прекращается) в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения сотрудника.

Проводится периодический формальный контроль соответствия согласованных и реальных прав доступа к информационным ресурсам текущему статусу пользователя.

Прямой доступ пользователей к базам данных не предоставляется.

Доступ ко всем информационным ресурсам Университета осуществляется только после авторизации пользователя.

Журналы аудита действий пользователей и администраторов автоматизированных систем должны быть информативны‚ защищены от модификации и храниться в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов, связанных с нарушением информационной безопасности.

**5.3 Управление жизненным циклом автоматизированных систем**

Процедуры по обеспечению информационной безопасности предусматриваются на всех стадиях жизненного цикла автоматизированных систем: при разработке (приобретении), эксплуатации, модернизации, снятии с эксплуатации.

Разработка, тестирование автоматизированных систем отделяются от эксплуатации.

Разработчики программного обеспечения не допускаются к его промышленной эксплуатации.

Разработка и тестирование программного обеспечения проводятся на выделенных физически или логически средствах вычислительной техники (виртуальные серверы), не использующихся для промышленной эксплуатации автоматизированных систем.

В контрактах со сторонними разработчиками на поставку систем предусматривается их ответственность за наличие в системах скрытых недокументированных возможностей, ведущих к ущербу Университета, а также соблюдение условий конфиденциальности.

Все изменения, вносимые в автоматизированные системы, контролируются и документируются. Дистрибутивные комплекты и исходные тексты систем собственной разработки, а также дистрибутивные комплекты приобретаемых систем хранятся в ИТ-Управлении.

В состав документации на критичные автоматизированные системы в обязательном порядке входит документация по обеспечению ее информационной безопасности.

Ввод автоматизированных систем в эксплуатацию производится только после их аттестации на соответствие предъявленным требованиям по информационной безопасности. Не допускается эксплуатация автоматизированных систем, не прошедших аттестации или имеющих не устранённые критичные замечания.

При выводе автоматизированной системы из эксплуатации или замене входящего в ее состав оборудования осуществляется принудительное удаление информации с соответствующих машинных носителей и из памяти компьютеров за исключением ведущихся в установленном порядке контрольных архивов электронных документов.

**5.4 Антивирусная защита**

Каждый сотрудник Университета обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать СИБ при подозрениях на вирусное заражение.

Техническая возможность подключения пользователями к рабочим станциям ЛВС внешних накопителей информации, модемов, мобильных телефонов, беспроводных интерфейсов, использование СВ-ЛЭУВ- дисководов максимально ограничивается.

Антивирусная защита обеспечивается использованием в Университете специализированного программного обеспечения.

Для снижения влияния человеческого фактора, исключения возможности отключения или отсутствия обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится централизованно автоматизированном режиме. При этом обеспечивается минимально возможный период обновления.

При невозможности централизованного обновления антивирусного и системного ПО периодичность, сроки и порядок проведения соответствующих мероприятий определяются оценкой имеющихся рисков вирусного заражения критичных информационных ресурсов и техническими возможностями такого обновления.

**5.5 Безопасное использование ресурсов Интернет**

Использование ресурсов Интернет в подразделениях Университета разрешается исключительно в производственных целях.

Взаимодействие с контрагентами по сети Интернет осуществляется с использованием специализированных систем и средств защиты, аттестованных на соответствие требованиям информационной безопасности.

Использование рабочих станций с доступом к ресурсам Интернет для обработки критичной информации запрещается.

Порядок публикации информации в сети Интернет определяется отдельными регламентами. Обсуждение сотрудниками Университета на форумах и в конференциях сети Интернет вопросов, касающихся их служебной деятельности, допускается только при наличии соответствующих указаний руководства.

Доступ сотрудников к ресурсам сети Интернет санкционируется руководством и согласовывается службой информационной безопасности, которая осуществляет контроль за соблюдением сотрудниками требований информационной безопасности, включая контентный анализ сообщений.

На узлах доступа в сеть Интернет принимаются необходимые меры для противодействия хакерским атакам и распространению спама.

**5.6 Использование средств криптографической защиты информации**

Применение средств криптографической защиты информации для обеспечения безопасности информационных ресурсов Университета и взаимодействия со сторонними организациями производится в соответствии с порядком, установленным государственными уполномоченными органами.

Использование средств ЭП обеспечивает целостность электронного документа и подтверждение авторства подписавшей его стороны и является лучшей практикой организации электронного документооборота при взаимодействии с контрагентами.

Во внутренних системах Университета механизмы криптографического контроля целостности используются в зависимости от результатов оценки рисков информационной безопасности.

Конфиденциальность информации при передаче по публичным сетям и внешним каналам связи обеспечивается обязательным применением шифрования.

Риски, связанные с возможной компрометацией криптографических ключей или доступом к защищаемой информации в обход средств криптографической защиты, должны минимизироваться специальными техническими и организационными мерами.

Криптографические ключи, предназначенные для защиты электронного документооборота Университета со сторонними организациями, изготавливаются сторонами самостоятельно.

**5.7 Обеспечение непрерывности бизнеса и восстановления после сбоев**

Непрерывность критичных процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности. Процедуры восстановления после сбоев документируются в соответствующих регламентах и планах.

**5.8 Обеспечение физической безопасности**

Помещения Университета категорируются в зависимости от критичности размещаемых в них хранилищ информационных ресурсов. В соответствии с категорией обеспечивается техническая укрепленность помещений, оснащение средствами видеоконтроля, контроля доступа, пожаротушения и сигнализации.

**Выводы и предложения**

Таким образом, можно сделать выводы, что наиболее уязвимыми активами являются персональные данные и сведения, содержащие служебную тайну, а также аппаратное и программное обеспечение.

В результате проведенного анализа системы информационной безопасности были выявлены основные угрозы информационной безопасности, произведена оценка риска рисков и выработаны основные меры по защите информации. Кроме того, следует соблюдать ряд общих требований:

* Доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.
* Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.
* Сотрудники должны проходить регулярное обучение в области информационной безопасности.
* Отдел автоматизации отвечает за определение детальных требований информационной безопасности и контролирует их исполнение в образовательных учреждениях.

Чтобы ограничить доступ к информации, содержащей персональные данные и служебную информацию, необходимо принять следующие меры:

* Специалист автоматизации обеспечивает защиту отдельных файлов и программ от чтения, удаления, копирования лицами, не допущенными к этому.
* Доступ к компьютерной сети образовательного учреждения осуществляется только с персональным паролем. Пользователь должен держать в тайне свой пароль. Сообщать свой пароль другим лицам, а также пользоваться чужими паролями запрещается.
* Категорически запрещается снимать несанкционированные копии с носителей информации, знакомить с содержанием электронной информации лиц, не допущенных к этому.
* Доступ к персональным данным должен быть описан в «Положения о защите персональных данных»

Для обеспечения физической защиты информации:

* Все объекты критичные с точки зрения информационной безопасности находятся в отдельном помещении, доступ в которое разрешен только сотрудникам, имеющими соответствующее разрешение от руководства образовательного учреждения.
* Вход в помещение осуществляется через дверь, оснащенную замком. Копии ключей находятся на вахте и у обслуживающего персонала.
* Помещение оборудовано вентиляцией и пожарной сигнализацией.
* Ключевые носители, программное обеспечение, документы и прочая конфиденциальная информация хранится в сейфах.
* Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право, находится в помещении в связи с выполнением своих должностных обязанностей.

Для обеспечения безопасности при работе с Интернет:

* Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.
* Запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности.
* Сотрудники образовательного учреждения не должны использовать сеть Интернет для хранения корпоративных данных.
* Специалист автоматизации имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.