МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УО “БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ”

**Кафедра информационных систем и технологий**

**“Защита информации и надёжность информационных систем”**

Отчёт по лабораторной работе №1

**Тема:** “Разработка политики информационной безопасности банка”

Выполнила

Студент 3 курса 1 группы

Пригодич Вера Валерьевна

Минск 2022

1. Обоснование актуальности, цели и задачи разработки ПИБ в организации (учреждении).

Актуальность: необходимость создания механизмов управления и планирования информационной безопасности в целях совершенствования следующих направлений деятельности компании:

* поддержка непрерывного бизнеса;
* повышение уровня доверия к компании;
* привлечение инвестиций;
* минимизация рисков безопасности с помощью защиты своих интересов в информационной сфере;
* снижение издержек;
* повышение качества деятельности по обеспечению ИБ.

Целью деятельности по обеспечению информационной безопасности банка является снижение уровня угроз информационной безопасности до приемлемого для банка значения.

Основные задачи деятельности по обеспечению информационной безопасности банка:

* выявление угроз и уязвимостей и их исключение;
* минимизация ущерба;
* повышение уровня информационной безопасности банка;
* разработка и поддержание в актуальном состоянии нормативных документов банка;
* внедрение, поддержка и при необходимости восстановление систем;
* участие и осуществление контроля выполнения требований информационной безопасности;
* контроль доступа к ресурсам банка.

2. Объекты защиты. Описание структуры организации (учреждения), периметра и внутренней структуры ИВС. Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности.

Основными объектами защиты системы информационной безопасности в банке являются информационные ресурсы, содержащие:

* коммерческую тайну;
* банковскую тайну;
* персональные данные физических лиц (сотрудников и клиентов);
* сведения ограниченного доступа.

Особые объекты защиты, имеющие высокую важность для банка:

* банковский платежный технологический процесс;
* банковский информационный технологический процесс;
* платежная информация;
* иная значимая для Банка информация, разглашение или модификация которой может привести к негативным последствиям для Банка;
* носители защищаемой информации, в т. ч. информационные ресурсы, речевая информация, документы на физических носителях информации, определенные как защищаемые нормативно-распорядительными документами Банка.

Описание структуры организации (учреждения), периметра и внутренней структуры ИВС:

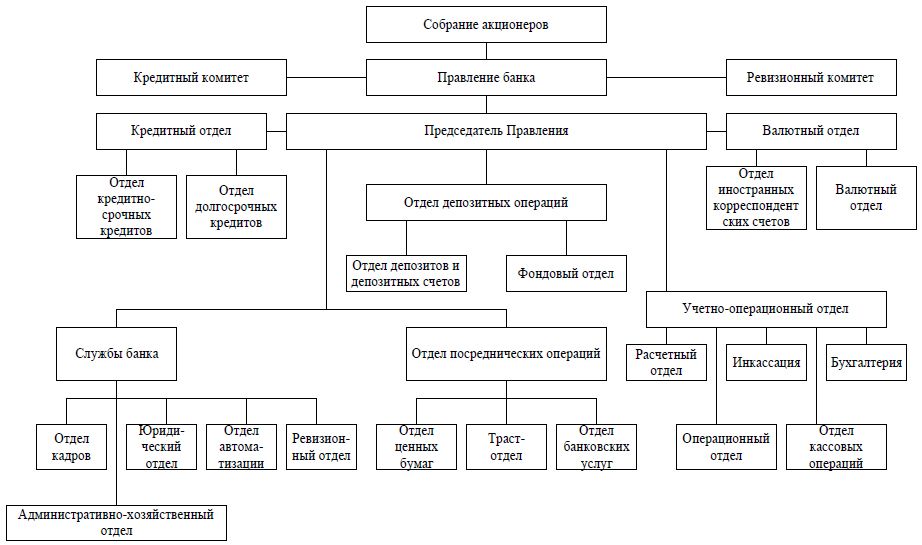


Рис. 1. Структура банка

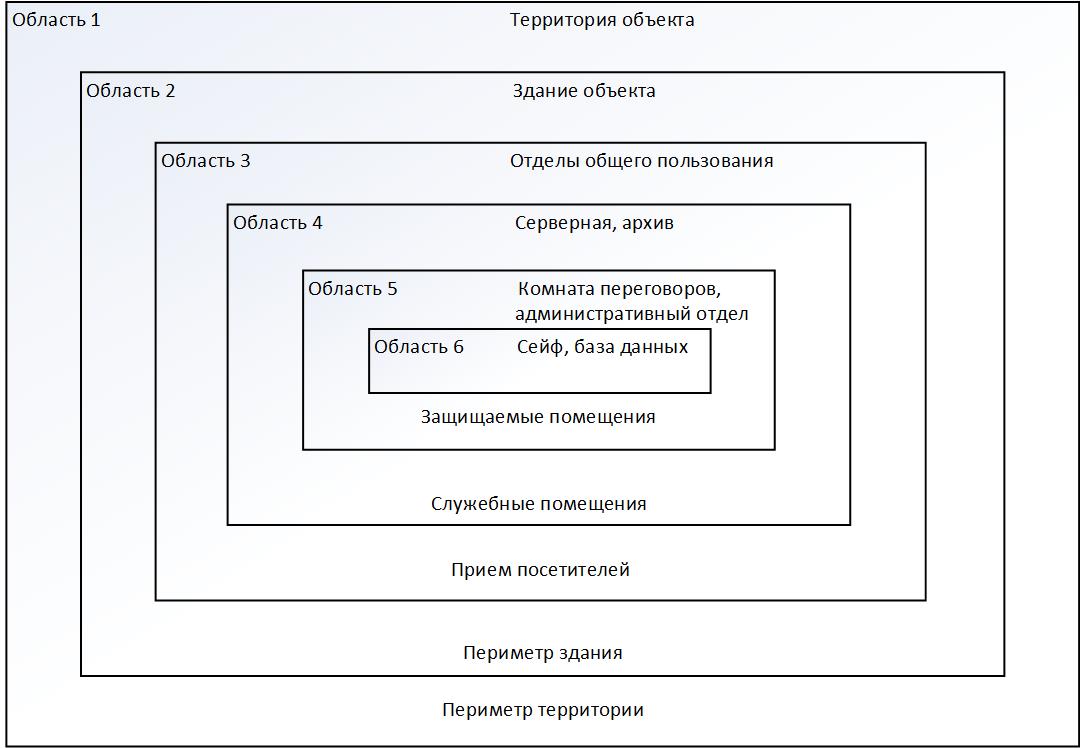


Рис. 2. Периметр помещения

1. Основные угрозы и их источники. Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.

Все многообразие дестабилизирующих факторов можно разделить на два класса: внутренние и внешние. Внутренние дестабилизирующие факторы влияют:

* на программные средства (ПС):

1. некорректный исходный алгоритм;
2. неправильно запрограммированный исходный алгоритм (первичные ошибки);

* на аппаратные средства (АС):

1. системные ошибки при постановке задачи проектирования;
2. отклонения от технологии изготовления комплектующих изделий и АС в целом;
3. нарушение режима эксплуатации, вызванное внутренним состоянием АС

Внешние дестабилизирующие факторы влияют:

* на программные средства:

1. неквалифицированные пользователи;
2. несанкционированный доступ к ПС с целью модификации кода;

* на аппаратные средства:

1. внешние климатические условия;
2. электромагнитные и ионизирующие помехи;
3. перебои в электроснабжении;
4. недостаточная квалификация обслуживающего персонала.

Все многообразие потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

Искусственные угрозы – это угрозы, вызванные деятельностью человека.

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними (о чем мы вспоминали выше). Основные источники угроз безопасности информации можно классифицировать следующим образом:

* непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей ИВС (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов ИВС;
* преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т. п.) действия легально допущенных к информационным ресурсам пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы:

1. деятельность преступных групп и формирований, политических и экономических структур, разведок иностранных государств, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности ИВС в целом и ее отдельных компонентов;
2. удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних информационно-телекоммуникационных сетей общего пользования (прежде всего сеть Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам;

* ошибки, допущенные при разработке компонентов информационной системы и системы ее защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты).

В заключение целесообразно отдельно отметить «человеческий фактор», классифицировав физических лиц, которые могут получить (а часто и реализуют) несанкционированный доступ к информации. К ним следует отнести:

* сотрудников организации (учреждения):

1. программисты, системные администраторы и даже администраторы информационной безопасности;
2. технический персонал;

* лиц, не являющихся сотрудниками:

1. посетители офиса;
2. ранее уволенные сотрудники (особенно «обиженные» увольнением);
3. хакеры.

4. Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты (воспользуйтесь приведенными в описании таблицами, заполните их).

С учетом изложенного, основные факторы (угрозы) ресурсам можно идентифицировать следующим образом:

1) действия внутреннего или внешнего злоумышленника (несанкционированный, в том числе удаленный доступ с целью нарушения работоспособности ИВС, кражи, удаления или модификации информации, несанкционированного распространения материальных носителей за пределами организации);

2) наблюдение за источниками информации;

3) подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов;

4) перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений;

5) разглашение информации компетентными людьми;

6) утеря носителей информации;

7) несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре;

8) воздействие стихийных сил (наводнения, пожары и т. п.);

9) сбои и отказы в аппаратуре сбора, обработки и передачи информации;

10) отказы системы электроснабжения;

11) воздействие мощных электромагнитных и электрических помех (промышленных и природных).

Условная численная шкала для оценки ущерба банку от несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб банку |
| 1 | Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение банка на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время банк терпит убытки, но его положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От банка уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, банк на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |
| 5 | Банк прекращает существование |

Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НДС) |
| 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 |

Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб \* Вероятность) |
| Взлом базы данных | 4 | 0,1 | 0,4 |
| DDoS-атака | 2 | 0,3 | 0,6 |
| Кража документов, содержащих конфиденциальную информацию о клиентах | 4 | 0,1 | 0,4 |
| Кража паролей от учётных записей офисных компьютеров | 3 | 0,1 | 0,3 |
| Ошибка программного обеспечения | 1 | 0,4 | 0,4 |
| Хищение данных банковских карт | 5 | 0,1 | 0,5 |
| Взлом банкоматов | 4 | 0,1 | 0,4 |
| Итого |  |  | 3 |

5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения). Выводы и предложения.

Выделяют следующие элементы системы защиты информации:

Нормативно-правовой элемент ЗИ:

Кроме законов и других государственных нормативных документов, включает такие документы организации, как:

* устав;
* коллективный трудовой договор;
* трудовые договоры с сотрудниками банка;
* правила внутреннего распорядка служащих банка;
* должностные обязанности руководителей, специалистов и служащих банка.
* инструкции пользователей информационно-вычислительных сетей и баз данных;
* инструкции администраторов ИВС и БД;
* положение о подразделении по защите информации;
* концепция системы защиты информации;
* инструкции сотрудников, допущенных к защищаемым
* сведениям;
* инструкции сотрудников, ответственных за защиту информации; памятка сотрудника о сохранении коммерческой или иной тайны;
* договорные обязательства.

Организационный элемент ЗИ:

Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы.

Программа работы с персоналом в банке сформулирована следующим образом:

* добывание в рамках действующего законодательства максимального объема сведений о кандидатах на работу, тщательная проверка представленных документов как через официальные, так и оперативные возможности, в том числе службы безопасности банка, системность в анализе информации, собранной на соответствующие кандидатуры;
* проведение комплекса проверочных мероприятий в отношении кандидатов на работу, их родственников, бывших сослуживцев, ближайшего окружения в тех случаях, когда рассматривается вопрос об их приеме на руководящие должности или допуске к информации, составляющей коммерческую тайну;
* использование современных методов, в частности собеседований и тестирований, для создания психологического портрета кандидатов на работу, который бы позволял уверенно судить об основных чертах характера и прогнозировать их вероятные действия в различных экстремальных ситуациях;
* оценка с использованием современных психологических методов разноплановых и разнопорядковых факторов, возможно препятствующих приему кандидатов на работу или их использованию на конкретных должностях;
* определение для кандидатов на работу в структурах банка некоторого испытательного срока с целью дальнейшей проверки и выявления деловых и личных качеств, иных факторов, которые бы могли препятствовать зачислению на должность;
* введение в практику регулярных и неожиданных комплексных проверок персонала, в том числе через возможности служб безопасности;
* обучение сотрудников кадровых подразделений и служб безопасности современным психологическим подходам к работе с персоналом, социальным, психоаналитическим, этикоморальным методам, навыкам использования современных технических средств для фиксирования результатов интервью и собеседований, приемам проведения целевых бесед «втемную» и процедурам информационно-аналитической работы с документами кандидатов;
* выделение из числа первых руководителей коммерческих структур куратора кадровой работы для осуществления контроля за деятельностью кадровых подразделений и служб безопасности при работе с персоналом.

Инженерно-технический элемент ЗИ:

Предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств. По функциональному назначению средства инженерно-технической защиты можно условно разделить:

* физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (доступу) злоумышленников на объекты защиты (территорию, в здание и помещения) и материальными носителями. Например, заборы, стальные двери, кодовые замки, сейфы и т. д.;
* средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и др. технических средств управления;
* средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализации, информирования и идентификации);
* средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т. п.);
* технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов, документов, дискет, книг и т. п.
* средства противопожарной охраны;
* средства защиты помещений от визуальных способов технической разведки.

Программно-аппаратный элемент ЗИ:

Предназначен для защиты конфиденциальной информации, обрабатываемой и хранящейся в компьютерах, серверах, рабочих станциях и т.д. Аппаратные средства защиты информации представлены техническими устройствами, предназначенными для защиты информации от разглашения, утечки или несанкционированного доступа. Аппаратные средства могут быть:

* средствами выявления;
* средствами защиты от несанкционированного доступа.

программные средства защиты имеют следующие разновидности специальных программ:

* идентификации технических средств, файлов и аутентификации пользователей;
* регистрации и контроля работы технических средств и пользователей;
* обслуживания режимов обработки информации ограниченного пользования;
* защиты операционных средств ЭВМ и программ пользователей;
* уничтожения информации в защитные устройства после использования;
* сигнализирующих нарушения использования ресурсов;
* вспомогательных программ защиты различного назначения.

Программная реализация защиты информации:

* Использование аппаратных решений для авторизации пользователей при входе в систему и при доступе к критичным файловым объектам (смарт-карта, Aladdin eToken, ruToken, iButton);
* Разграничения и аудит работы пользователей с локальными и сетевыми ресурсами (файловые ресурсы – FAT/NTFS/DFS/любые монтируемые ФС), ресурсы реестра ОС, сменные носители, принтеры, сервисы олицетворения, буфер обмена и т. д.);
* Разграничения и аудит работы программ (приложений) с локальными и сетевыми ресурсами;
* Разграничения и аудит работы пользователей с устройствами с использованием их серийных номеров (Flash-диски, CD/DVD, USB, WiFi, Bluetooth, IrDA, IEEE1394/ FireWire, PCMCIA, COM/LPT и т. д.);
* Разграничения и аудит работы пользователей и приложений с локальными и глобальными сетями (ЛВС, Internet/Intranet) – персональный Firewall;
* Шифрование данных «на лету» (3DES, AES, DES), включая сетевые ресурсы, скрытие, разграничение доступа, а также гарантированное удаление остаточной информации, реализации коллективного доступа к зашифрованным данным;
* Контроль рабочего времени пользователя, в том числе, средствами компьютерного видео наблюдения.

Основной вывод, который можно сделать из анализа развития банковской отрасли, заключается в том, что автоматизация и компьютеризация банковской деятельности (и денежного обращения в целом) продолжает возрастать. Основные изменения в банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий. Можно прогнозировать дальнейшее снижение оборота наличных денег и постепенный переход на безналичные расчеты с использованием пластиковых карт, сети Интернет и удаленных терминалов управления счетом юридических лиц.

В связи с этим следует ожидать дальнейшее динамичное развитие средств информационной безопасности банков, поскольку их значение постоянно возрастает.