УДК 004.056.

СОЗДАНИЕ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ФИЗИЧЕСКОМ И ДИСТАНЦИОННОМ ДОСТУПЕ

Губаев В.К., студент гр. 2ОИБ, 2 курс
Научный руководитель: Никифоров Д.К., к.ф.-м.н., доцент
ГАПОУ КО «Калужский технический колледж»
г. Калуга

Аннотация: *обобщены понятия применения современных дистанционных способов коммуникации, проанализированы их преимущества и недостатки. Рассмотрены способы и методы защиты информации. В программе BPwin разработаны диаграммы обеспечения защиты информации , подробно рассмотрен каждый этап схемы процессов всего комплекса. Описан неразрывный процесс взаимодействия программных средств для обеспечения надежности, безопасности и конфиденциальности информации.*

Ключевые слова: *защита информации, BPwin, информационные технологии, методы защиты информации.*

В современном мире многое напрямую связано с хранением и обменом информации, которая обычно нуждается в сохранении конфиденциальности и тщательной защите. Порой собственных ресурсов организации бывает недостаточно, для обеспечения надежной защиты и сохранности данных. Только благодаря профессиональной разработке и установки систем, которые контролируют и предотвращают утечку информации и ее использование, можно обеспечить стабильную работу и выполнение всех процессов организации.

Существет несколько способов и видов защиты информации, которые осуществляются по Федеральному закону "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [1]. Путём правового метода информация защищается благодаря разработке правовых норм и документов осуществляемых государством, а также четкий контроль над их исполнением. Эти меры остановят тех, кто не готов ради информации игнорировать правила, нарушать законы и нести последующее наказание [2].

Далее идет физический метод защиты информации. От создания антивирусов и шифрования не будет никакого толку, если злоумышленник может просто пробраться в серверную и похитить жесткие диски с информацией. Поэтому серверные и информационные системы нужно в первую очередь защищать снаружи, с помощью физических средств защиты, таких как: решетки, двери, сигнализации, камеры наблюдения и сложные замки. Также информацию из вне, можно защитить посредством подбора

надежных и ответственных сотрудников, подписание договора о неразглашении информации, и системой уровней доступа для сотрудников, которая позволит, чтобы определенная информация была доступна только определенному кругу лиц.

Криптографическая защита делится на две основные функции, во-первых шифрует данные. Даже если злоумышленник сможет получить доступ к данным, он увидит только зашифрованную информацию, для расшифровки которой требуется особый ключ. Во-вторых, она не только подтверждает подлинность информации, но и определяет личность отправителя, если файл попытаться изменить или подделать, это сразу будет видно.

Последний способ защиты информации - технический, путем использования программного обеспечения. Когда мы говорим о защите информации, то сразу вспоминаем антивирусы и пароли. Это как раз и является техническим методом защиты информации. К нему относятся: антивирусы, системы аккаунтов и паролей, программные межсетевые экраны (файерволы), инструменты виртуализации, DLP (предотвращают утечку информации) и SIEM (фиксируют подозрительную активность) системы [3].

В работе с помощью программы BPwin были разработаны и представленны схемы процессов защиты информации [4]. Благодаря такому наглядным примерам, легко понять как происходит процесс защиты информации, а также как правильно и надежно обеспечить эту защиту.

Еще ни одно программное решение не защищает информацию полностью, оно лишь блокирует одни возможности атаки, но оставляет пространство для других. Для построения надежной системы защиты информации нужно подобрать несколько программных средств и выстраить комплекс, где каждое средство взаимодействует с другими, именно поэтому на схеме каждый процесс неразрывно связан цепочкой с другим процессом и только при четком соблюдении всех процессов между собой можно достигнуть полного обеспечения защиты информации (ЗИ).

Для простоты понимания все этапы были разделены на процессы. Обеспечение защиты можно разделить на «Обеспечение защиты информации при управлении доступом» и «Обеспечение защиты вычислительных систем» (рис.1). К первой относится: защита физического доступа (путем организационных мер и создания припятствий от НСД), управление учетными записями (например, контроль учетных записей уволенных и не пользующихся сотрудников), идентификация, аутентификация и авторизация (однофакторная аутентификация пользователей, многофакторная аутентификация администраторов, пароли на BIOS, установка сложных паролей, а также разграничение доступа), идентификация, классификация, учет ресурсов и объектов доступа (контроль и учет состава ресурсов, операция по изменению, а также состав объектов доступа).

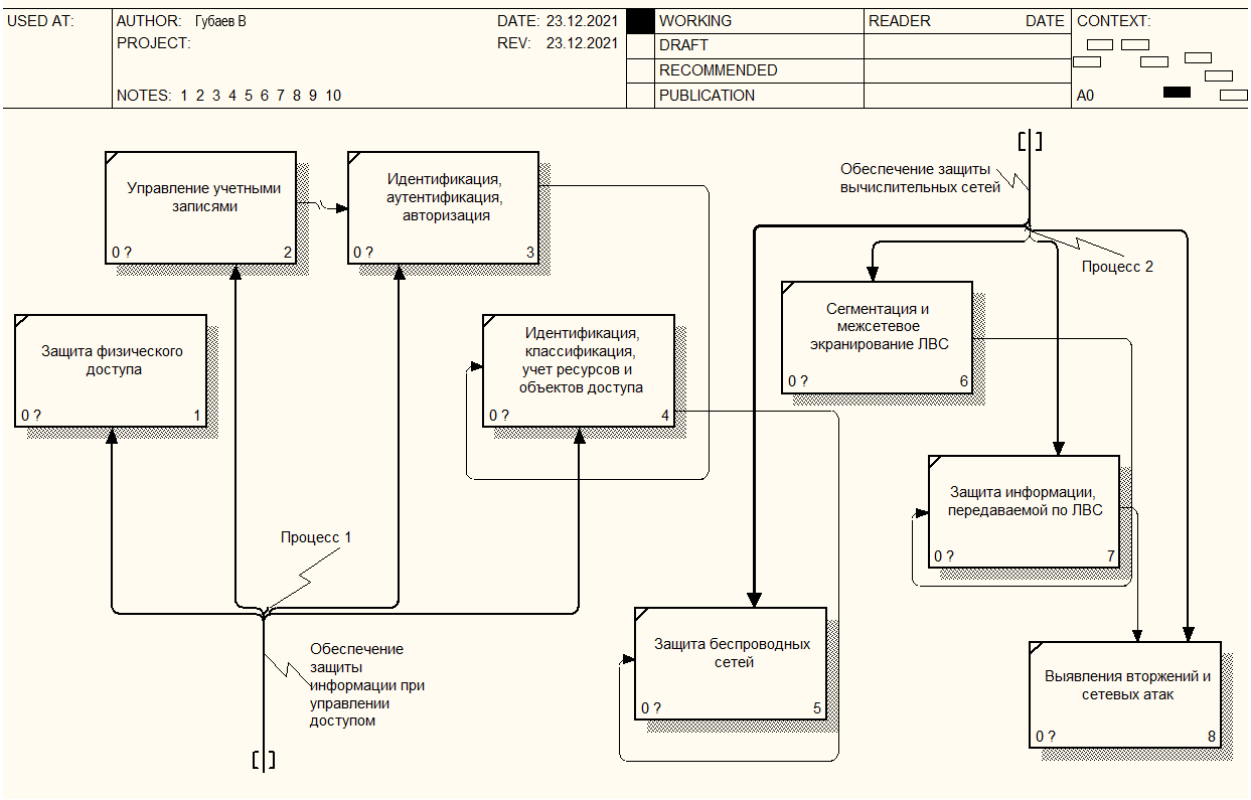

Рис. 1. Схема процессов обеспечения защиты информации при управлении доступом и обеспечения защиты вычислительных сетей

Во второй процесс входит: защита беспроводных сетей (описать в ОРД правила взаимодействия, использовать WIPS, сохранять в логах сетевого оборудования информацию об изменении конфигурации), сегментация и межсетевое экранирование ЛВС (описание контуров безопасности, установление правил фильтрации, использование внешнего и внутреннего почтовых серверов), защита информации, передоваемой по ЛВС (использование двухстороннего TLS и VPN между подразделениями), выявление вторжений и сетевых атак (использование средств обнаружения вторжений, средств защиты от DDoS-атак, антиспама)

Далее представлены одиночные процессы, в результате которых получено обеспечение защиты информации на этапах жизненного цикла АС и приложений (рис.2).

К контролю целостности и защищенности можно отнести: использование сканеров уязвимостей, тестирование на проникновение и устранение выявленных по результатам сканирования уязвимостей, хранение копий ОС, прикладного ПО, СЗИ, запрет установки или запуска неразрешенного ПО и т.д.

Защита от вредоностного кода включает в себя: различные антивирусы, тестирования на проникновение, решения по защите электронной почты с антивирусной проверкой почтовых сообщений, самостоятельный контроль.

Меры по предотвращению утечек информации: DLP-система с контентным анализом информации, контроль за внешними носителями,

принтеры с авторизацией печати по карточке или логину-паролю, различные запреты и ограничения.

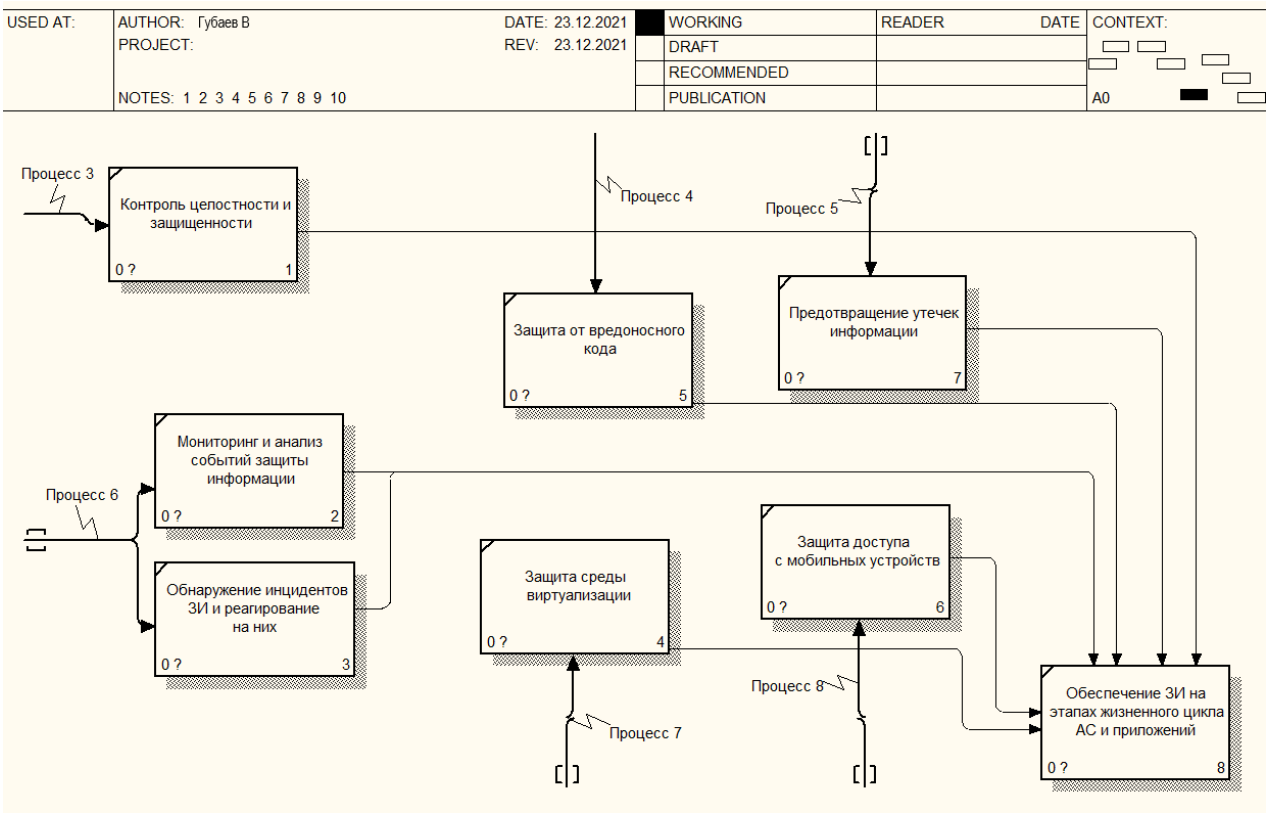

Рис. 2. Схема процессов обеспечения защиты информации на этапах жизненного цикла АС и приложений

В процесс 6 входит: централизованный сбор событий, использование службы синхронизации времени, передача данных по защищенному протоколам, выделение массива для хранения данных, автоматическое уведомление администраторов об исчерпании дискового пространства, защита доступа к хранилищу данных, обеспечение целостности данных средствами СУБД, резервирование базы данных, создание и хранение базы данных об инцидентах.

Такие решения как: запреты одновременного выполнения ролей и размещения серверных и пользовательских компонентов АС на одной ВМ, а также на параллельные сеансы RDP могут обеспечить защиту среды виртуализации.

Для осуществления защиты доступа с мобильных устройств следует использовать: Для аутентификации VPN или двухсторонней TLS, NAC, или клиент MDM.

На сегодня системы защиты информации имеют одну из самых важных ролей в деятельности любой организации. Грамотная и своевременная защита информации совместно с разработкой улучшенных систем безопасности предупредит любые потери, искажения и нарушения достоверности информации, а также сохранит ее полную конфиденциальность. Такой правильный и высо-

коквалифицированный подход обеспечит пользователям безопасность и уверенность при использовании своих личных данных.

Технологии с каждым днем развиваются все больше, и мы обретаем все более объемные и разносторонние знания о средствах защиты информации, которых тоже становится все больше. Появление новых вирусов и новых систем взлома заставляют непрерывно работать над повышением эффективности защиты, а также разработкой более совершенных программ шифрования и блокировки утечки.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
2. Официальный сайт Центр Защиты Информации [Электронный ресурс] - Режим доступа: https://baltzi.ru/
3. Официальный сайт ФСТЭК России [Электронный ресурс] - Режим доступа: https://fstec.ru/
4. Сайт BPWIN - ITteach [Электронный ресурс] - Режим доступа: https://itteach.ru/bpwin/