Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники
Кафедра инженерной психологии и эргономики

На правах рукописи

УДК 004.056.5:656.2

Клименко
Иван Александрович

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Автореферат

1-59 81 01 – Управление безопасностью производственных процессов

Магистрант И.А. Клименко

Научный руководитель
А.М. Лазаренков, доктор
технических наук, профессор

Заведующий кафедрой ИПиЭ
К.Д. Яшин, кандидат технических
наук, доцент

Минск 2018

Важнейшей задачей транспортной безопасности является создание эффективной организационно-технической системы обеспечения требуемого уровня антитеррористической и антикриминальной безопасности железнодорожного транспорта.

Объектом данной работы являются информационные ресурсы железнодорожного транспорта. Предмет – безопасность информационных ресурсов.

Цель работы заключается в повышении безопасности информационных ресурсов.

Предстоит рассмотреть следующие задачи:

1. Проанализировать нормативные и методические документы и определить угрозы безопасности информационных ресурсов железнодорожного транспорта.

2. Оценить уязвимость объектов инфраструктуры и транспортных средств.

3. Построить модель нарушителя информационной безопасности.

4. Разработать рекомендации по улучшению обеспечения безопасности информационных ресурсов.

Состав требований к информационной безопасности системы железнодорожного транспорта описываются в нормативных документах (стандарты, руководящие материалы, методические рекомендации). Содержащиеся в этих документах указания могут носить характер справочный, обязательный или рекомендательный.

Под безопасностью информации понимается такое ее состояние, при котором исключается возможность просмотра, изменения или уничтожения информации лицами, не имеющими на это права, а также утечки информации за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники.

В современных условиях хозяйствования железнодорожный транспорт, являясь материальной основой процесса обращения, все в большей степени становится основным условием обеспечения экономической безопасности национальной экономики.

Особое внимание при обеспечении безопасности железнодорожного транспорта следует уделять угрозам, которые следует непосредственно устранять, либо же подавлять их проявление.

Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д.

Чаще всего строится неформальная модель нарушителя, отражающая причины и мотивы действий, его возможности, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей: способы реализации исходящих от него угроз, место и характер действия, возможная тактика и т. п. Для достижения поставленных целей нарушитель должен приложить определенные усилия и затратить некоторые ресурсы.

Определив основные причины нарушений, представляется возможным оказать на них влияние или необходимым образом скорректировать требования к системе защиты от данного типа угроз. При анализе нарушений защиты необходимо уделять внимание субъекту (личности) нарушителя. Устранение причин или мотивов, побудивших к нарушению, в дальнейшем может помочь избежать повторения подобного случая.

Модель может быть не одна, целесообразно построить несколько отличающихся моделей разных типов нарушителей информационной безопасности объекта защиты.

Для построения модели нарушителя используется информация, полученная от служб безопасности и аналитических групп, данные о существующих средствах доступа к информации и ее обработки, о возможных способах перехвата данных на стадиях их передачи, обработки и хранении, об обстановке в коллективе и на объекте защиты, сведения о конкурентах и ситуации на рынке, об имевших место свершившихся случаях нарушения информационной безопасности и т. п.

Кроме этого оцениваются реальные оперативные технические возможности злоумышленника для воздействия на систему защиты или на защищаемый объект. Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать нарушитель в процессе совершения действий, направленных против системы информационной защиты.

Таким образом, для должного обеспечения безопасности информационных ресурсов главным критерием является создание правильной, как можно развернутой модели нарушителя. Но в последнее время, как показывает практика, чаще всего предприятия сталкиваются с проблемой нарушения безопасности информации именно со стороны, которую не рассматривали как таковую и не строили в модели нарушителя, такую модель я назову «неформальная модель нарушителя».

При анализе достаточного количества литературы было выявлено, что существуют следующие типы нарушителей, такие как:

– неопытный пользователь (сотрудник, который может предпринимать попытки выполнения запрещенных операций, доступа к запрещенным ресурсам

организации с превышением своих полномочий, но все эти действия совершены по ошибке, некомпетентности, халатности, без злого умыла, при этом использует только доступные для него программные средства);

– любитель (сотрудник организации, пытающийся преодолеть систему защиты без корыстных целей, для самоутверждения или из «спортивного интереса»);

– внешний нарушитель (постороннее лицо или сотрудник организации, действующий целенаправленно из корыстных интересов, из мести или из любопытства);

– внутренний злоумышленник (сотрудник организации, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных целей, мести).

Сложнее всего предотвратить нарушения внутреннего злоумышленника, который представляет собой зарегистрированного пользователя ИСПДн, осуществляющий ограниченный доступ к ресурсам с рабочего места. До сих пор не было построено как можно развернутой модели такого нарушителя, поэтому большинство организаций становится их жертвой. Неформальная модель внутреннего нарушителя содержит в себе содержательную модель (описывает характер действий злоумышленника) и математическую модель (описывает сценарий в виде логической последовательности), которая представлена в таблице 1:

Таблица 1 — Неформальная модель нарушителя информационной безопасности

Характеристика	Внутренний злоумышленник
Мотивы действий	игровые действия в сети
	реакция на выговор, неуплату за работу, злой умысел
	продажа информации
Возможности	может иметь физический доступ к линиям связи, системам электропитания и заземления
	возможности зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов
	имеет доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн
	располагает фрагментами информации о топологии ИСПДн и об используемых коммуникационных протоколах и их сервисах
Априорные знания	знает, по меньшей мере, одно легальное имя доступа
	располагает конфиденциальными данными, к которым имеет доступ

Окончание таблицы 1

	хорошо знаком со структурой, основными функциями и принципами работы программно-аппаратных средств
Преследуемые цели	внедрение вредоносного или разрушающего программного обеспечения
	манипулирование информацией
	проникновение в корпоративную сеть
	перехват информации
Способы реализации исходящих из него угроз	может использовать только штатные средства ИСПДн
	утрата
Набор способов и средств	агентурный метод получения реквизитов доступа
	подключение к каналам передачи данных
	внедрение программных закладок
Возможная тактика	осуще6ствляет попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности
	может изменять конфигурацию технических средств ИСПДн, вносить в нее аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн
Возможные каналы атак	электронные носители информации
	кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами
	штатные программно-аппаратные средства ИСПДн

Одним из главных приоритетов работы любой информационной системы является обеспечение информационной безопасности для обрабатываемых данных.

В рамках данной работы были рассмотрены и решены следующие задачи:

1. Проанализировав нормативные и методические документы, были определены угрозы безопасности информационных ресурсов железнодорожного транспорта.

2. Произведена оценка уязвимостей объектов инфраструктуры и транспортных средств.

3. Построена модель нарушителя информационной безопасности.

Проблема персональных данных, которую породило бурное развитие информационных технологий, заключается в несанкционированном

использовании персональных данных граждан в различных целях, начиная от рассылки спама и телефонного маркетинга, заканчивая несанкционированным дебетованием средств с пластиковых карточек и различных форм мошенничества.

Основные рекомендации для должного обеспечения безопасности информационных ресурсов можно сформулировать так:

1. Система и программные средства должны иметь фрагментарную архитектуру построения, при которой учетные данные, библиографическая информация и персональные данные хранятся в различных местах. Доступ к системе должен осуществляться кластерным способом – через единую точку входа в рамках корпоративной сети. В целях минимизации угроз безопасности обработки данных в системе должна существовать возможность выбора одной из схем развертывания, отличающихся по месту расположения демографического сервера и иной информации, а так же каналов подключения.

2. Для использования программного обеспечения необходимо, чтобы требовался ввод имени пользователя и пароля. При регистрации пользователя в системе указывать его роли. В соответствии с ролью пользователя определять объем прав по работе в программе, в том числе и объем предоставляемых сведений.

3. Вести учет количества пользователей, допущенных к работе с персональными данными. Возможен мониторинг действий с персональными данными и просмотр результатов действий в журнале событий.

Программа должна представлять собой единую платформу для работы нескольких операторов, однако сведения, занесенные одним из них, могут быть переданы другому только при наличии согласия на то основного оператора. В зависимости от решаемой задачи и роли пользователя, сведения предоставлять либо в неизменном, либо в обезличенном виде.

4. В программе должны отсутствовать средства разработки и отладки, что гарантирует отсутствие возможности третьих лиц повлиять на среду обработки персональных данных.

5. Система должна быть настроена так, что у лиц, работающих в программе, будет отсутствовать возможность пользования программой с автоматизированного рабочего места, находящегося вне контролируемой зоны. Такими гибкими настройками возможно разрешение только такого входящего и исходящего трафика, который является необходимым. Разграничение доступа на уровне межсетевого взаимодействия должно выполняться с помощью настроек одного каскада демографических серверов.

6. Основная точка входа в программу должна использовать защищенные протоколы HTTPS и SSL для предотвращения доступа третьих лиц к передаваемой по каналам информации. SSL является стандартом обеспечения

безопасности предаваемых данных между компьютером пользователя и просматриваемым веб-сайтом. Сайты, использующие SSL, должны предоставлять браузерам сертификаты безопасности для подтверждения их идентификационных данных.

7. Сохранность информации обеспечивается хранением ее на серверах платформы Amazon EC2, обеспечивающих доступность и бесперебойность на 99,95% и хранящей до 100 резервных копий обрабатываемой информации. В используемых ресурсах реализуются современные способы обеспечения безопасности.

Внедрение данных мероприятий позволит повысить безопасность информационных ресурсов железнодорожного транспорта.