18+

В ЗОНЕ ДОСТУПА

УПРАВЛЕНИЕ ДОСТУПОМ НА ПРЕДПРИЯТИИ

Категория: Информационная безопасность, Управление доступом, Наука

Автор: Александр Захаров
Редактор: Вероника Кузьмина, Елена Захарова

Александр Захаров

В зоне доступа. Управление доступом на предприятии

https://litres.ru/74160983
ISBN 9785007043861

Аннотация

Тот, кто владеет информацией — владеет миром. Но мало ею только владеть, ее надо использовать по назначению, а для этого предоставлять к ней доступ. Одной из самых больших проблем в информационной безопасности является безопасное управление доступом к информации. В настоящей книге описана разработанная и испытанная автором модель управления доступом, базирующаяся на методиках DAC, MAC, RBAC и ABAC. Совмещение подходов позволяет гибко и безопасно решать задачу по управлению доступами.

Содержание

В зоне доступа
Управление доступом на предприятии

Александр Захаров

Редактор Елена Захарова
Редактор Вероника Кузьмина
Корректор Венера Ахунова
Художник Алексей Мецлер

ISBN 978-5-0070-4386-1
Создано в интеллектуальной издательской системе Ridero

Введение

Тот, кто владеет информацией — владеет миром. Но мало ею только владеть, ее надо использовать по назначению, а для этого предоставлять к ней доступ лицам, которым это положено для трудовых обязанностей.

Внимание к информационной безопасности и защите информации компании любого размера в современном мире является гарантией существования компании в целом, а отсутствие контроля порождает несанкционированный доступ, злоупотребление полномочиями и как результат — утечки информации или ее искажение/уничтожение.

Одной из самых больших проблем в информационной безопасности является, как ни странно, безопасное управление доступом к информации, к местам ее хранения и обработки. В крупных компаниях, где систем и ресурсов очень много, как и видов информации, это и вовсе превращается в невыполнимую задачу.

Кому можно получать доступ, а кому нельзя? Порой на этот простой вопрос не могут ответить даже авторы самой информации и владельцы процессов, в которых она обрабатывается. Вопросы о механизмах такого доступа и способах управления и вовсе ставят людей в тупик.

В настоящей книге описана разработанная и неоднократно испытанная автором модель управления доступом, ко-

торая базируется на нескольких ранее изученных способах, совмещающих подходы DAC, MAC, RBAC и ABAC. Именно совмещение подходов позволяет гибко и вместе с тем безопасно решать задачу по управлению доступами.

В этой книге я познакомлю вас с тем, из чего строится доступ, практическими методами определения и формирования ролей, комбинирования, управления ими, их учета, а также с формированием доступа к информационным системам и учетом таких доступов, используя как простые методы, вроде учета в Excel (как универсального инструмента, который может быть преобразован в структуры баз данных), так и системы управления доступом на базе Active Directory и продуктов IDM.

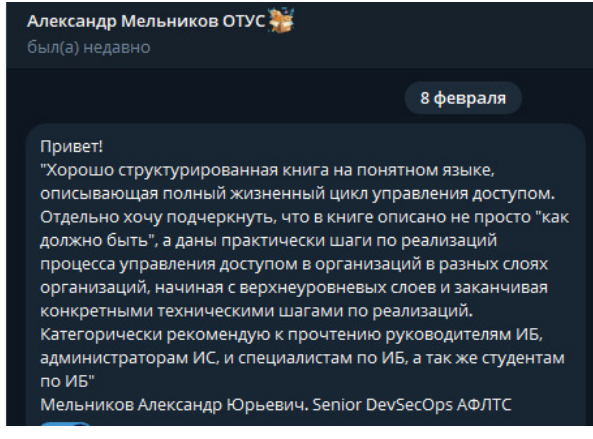
Изучив эту книгу, вы сможете понять, какая информация подлежит защите, где она хранится, как передается и как к ней обеспечивается доступ, что такое доступ, роли, их составляющие части, полномочия, как принимаются решения, вы сможете самостоятельно строить ролевые модели, вести учет и выполнять работы по автоматизации процессов или подойти к возможности внедрения системы класса IDM.

Отзывы читателей, участвовавших в закрытых чтениях рукописи:

«Книга написана доступным и понятным языком. Материал хорошо структурирован, простроены четкие взаимосвязи между всеми сторонами рассматриваемого вопроса. Даны практические рекомендации и предложены шаблоны необходимых документов. Актуальность книги обусловлена нарастающими темпами изменения ландшафта и количества киберугроз, а также требований регуляторов. Рекомендуется к прочтению как студентам специальностей, связанных с ИБ, так и преподавателям и действующим специалистам. Безусловно, рекомендована к прочтению Руководителями ИБ предприятий для упрощения выстраивания процессов».

Сергей Михайлович Терешин,
Руководитель и создатель курсов «Информационная

безопасность. Professional», «Внедрение и работа в DevSecOps», онлайн-университет Otus



«Хорошо структурированная книга на понятном языке, описывающая полный жизненный цикл управления доступом. Отдельно хочу подчеркнуть, что в книге описано не просто „как должно быть“, а даны практические шаги по реализации процесса управления доступом организаций в разных слоях организаций, начиная с верхнеуровневых слоев и заканчивая конкретными техническими шагами по реализации. Категорически рекомендую к прочтению руководителям ИБ, администраторам ИС и специалистам по ИБ, а также студентам по ИБ».

Мельников Александр Юрьевич.

Senior DevSecOps АФЛТС

"Книга Александра Захарова "В зоне доступа" выделяется на фоне литературы по информационной безопасности своей исключительной практической ориентированностью и системностью в раскрытии темы управления доступом.

Автор не ограничивается поверхностным обзором, а предлагает читателю детальную методологию: от анализа исходных требований и построения фундамента в виде ролевых моделей и матриц доступа (включая тонкости разделения обязанностей — SOD) до организации процессов их жизненного цикла, согласования, аудита и финального внедрения соответствующих систем.

Особую ценность представляют готовые регуляторные артефакты в приложениях: формулировки политик, регламентов и порядков, которые можно адаптировать для использования в организации.
Главы, посвященные пентесту доступов и внедрению систем, переводят теорию в плоскость реальных проектов.

Актуальность материалов обусловлена растущими требованиями Регуляторов и необходимостью противодействия инсайдерским угрозам через грамотное управление привилегиями.

Кому необходимо прочесть:

- Руководителям и архитекторам ИБ — для выстраивания или аудита процессов управления доступом
- Специалистам по внутреннему контролю и аудиту
- Студентам технических и управленческих специальностей в ИБ как образец структурирования сложного предмета

Книга заслуживает высокой оценки и является must-read для профессионалов, серьезно относящихся к построению эффективной системы безопасности.

Максим Вениаминович Чащин, Руководитель курса "CISO / Директор по информационной безопасности", онлайн-университет Otus"

сегодня в 18:12

«Книга Александра Захарова «В зоне доступа» выделяет-

ся на фоне литературы по информационной безопасности своей исключительной практической ориентированностью и системностью в раскрытии темы управления доступом.

Автор не ограничивается поверхностным обзором, а предлагает читателю детальную методологию: от анализа исходных требований и построения фундамента в виде ролевых моделей и матриц доступа (включая тонкости разделения обязанностей — SOD) до организации процессов их жизненного цикла, согласования, аудита и финального внедрения соответствующих систем.

Особую ценность представляют готовые регуляторные артефакты в приложениях: формулировки политик, регламентов и порядков, которые можно адаптировать для использования в организации.

Главы, посвященные пентесту доступов и внедрению систем, переводят теорию в плоскость реальных проектов.

Актуальность материалов обусловлена растущими требованиями Регуляторов и необходимостью противодействия инсайдерским угрозам через грамотное управление привилегиями.

Кому необходимо прочесть:

— Руководителям и архитекторам ИБ — для выстраивания или аудита процессов управления доступом.

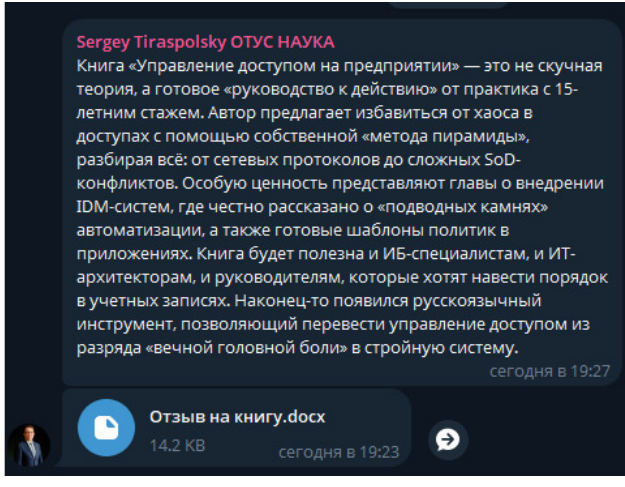
— Специалистам по внутреннему контролю и аудиту.

— Студентам технических и управленческих специально-

стей в ИБ как образец структурирования сложного предмета.

Книга заслуживает высокой оценки и является must-read для профессионалов, серьезно относящихся к построению эффективной системы безопасности».

Максим Вениаминович Чащин,
Руководитель курса «CISO / Директор по информационной безопасности»,
онлайн-университет Otus»



«В современном мире информационной безопасности сложилась парадоксальная ситуация: несмотря на огромное количество средств защиты (межсетевые экраны, SIEM,

DLP), наиболее уязвимым звеном остается сам процесс предоставления доступа сотрудникам к информации. Хаос в учетных записях, «плавающие» роли и неконтролируемые полномочия сводят на нет работу даже самых дорогих систем безопасности.

Книга Александра Захарова «Управление доступом на предприятии» — это не очередное перечисление терминов из стандартов, а, по сути, практическое «руководство к действию». Автор, обладающий более чем 15-летним опытом в сфере ИБ и инженерии, предлагает читателю не абстрактную теорию, а выстраданную на реальных проектах методологию.

Главное достоинство книги — ее системность. Автор предлагает отказаться от попыток управлять доступом «как получится» и внедряет четкую, иерархическую модель, которую он называет «методом пирамиды». Читателю предлагается пройти путь от фундамента — рекогносцировки активов и реестров систем — до самой вершины, где формируются удобные профили пользователей.

Особого внимания заслуживает язык изложения. В отличие от сухих академических трудов, книга читается легко. Автор не боится быть прямым, критикует устаревшие подходы и с юмором описывает типичные проблемы, с которыми сталкиваются специалисты на практике.

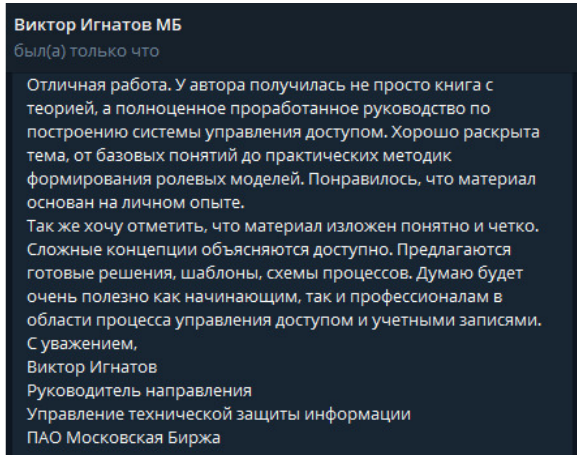
Отдельно хочется отметить наличие в конце книги готовых шаблонов (Приложение 1 и 2) — «Политики управле-

ния доступом» и «Порядка управления ролевыми моделями». Это бесценный материал для любого ИБ-специалиста или ИТ-руководителя, который можно брать и адаптировать под реалии своей компании, экономя месяцы на разработку документации с нуля».

Тираспольский Сергей Александрович

Заместитель декана: *НИУ ВШЭ в Нижнем Новгороде / Факультет информатики, математики и компьютерных наук*

Доцент: *НИУ ВШЭ в Нижнем Новгороде / Факультет информатики, математики и компьютерных наук / Кафедра информационных систем и технологий*



«Отличная работа. У автора получилась не просто книга с теорией, а полноценное проработанное руководство по построению системы управления доступом. Хорошо раскрыта тема, от базовых понятий до практических методик формирования ролевых моделей. Понравилось, что материал основан на личном опыте.

Также хочу отметить, что материал изложен понятно и четко. Сложные концепции объясняются доступно. Предлагаются готовые решения, шаблоны, схемы процессов. Думаю, будет очень полезно как начинающим, так и профессионалам в области процесса управления доступом и учетными записями».

Виктор Игнатов
Руководитель направления
Управление технической защиты информации
ПАО Московская Биржа

Термины и определения

Термин	Определение
Информация, подлежащая защите (Защищаемая информация)	Информация, которую требуется защищать от воздействий внешнего нарушителя, так и информация, которая должна быть доступна только отдельным категориям сотрудников для выполнения прямых обязанностей.
Доступ к информации	Возможность для физических и юридических лиц получать, использовать и обрабатывать информацию. Это включает в себя поиск, получение, передачу и распространение информации любым законным способом.
Доступ в систему	Доступ в систему в контексте информационной безопасности означает возможность пользователя или процесса взаимодействовать с ресурсами системы, такими как данные, приложения или оборудование. Это включает в себя аутентификацию (подтверждение личности) и авторизацию (предоставление прав доступа к конкретным ресурсам). Системы контроля доступа, будь то физические или логические, обеспечивают безопасность, регулируя, кто и как может получить доступ к ресурсам.
Несанкционированный доступ (НСД)	Несанкционированный доступ к компьютерной информации, или неправомерный доступ – это получение доступа к информации, хранящейся в компьютерной системе, без разрешения ее владельца или законного пользователя. Это нарушение правил разграничения доступа, при котором лицо, не имеющее права на получение данных, получает к ним доступ, используя штатные средства вычислительной техники или автоматизированных систем. Является нарушением, преследуемым по УК РФ, Статья 272.

Термин	Определение
Роль в информационной системе	Набор прав и привилегий, определяющий, какие действия пользователь или группа пользователей могут выполнять в системе. Роли часто соответствуют бизнес-ролям сотрудников и используются для разграничения доступа к различным ресурсам и функциональности системы.
Системная роль (атомарная)	Атомарные (неделимые) составляющие доступа. Полномочия в системе или наборе подсистем в ее составе. То есть это конкретные настройки системы, ее инфраструктуры или параллельных систем, которые необходимы пользователю для выполнения бизнес-операций.
Бизнес-роль	Комбинированные роли на основании системных ролей, которые более понятны пользователям и которые определяют набор системных ролей для конкретного набора прав и функций в системе. То есть это роли как виртуальные, так и реально запрограммированные в системе, которые содержат в себе целый набор доступов в системе с понятным описание функций, которые проще выбрать.
Профиль пользователя	Набор бизнес-ролей разных систем (допускается и системных, если комбинировать возможность отсутствует ввиду особенностей системы), закрепляемых за функциональной группой пользователей. То есть это виртуальные сущности пользовательской группы (определенные именно для «живых» потребителей), которые дают возможность сделать рабочее место определенной группы работников, используя готовые наборы разных систем, что позволяет назначать такие роли автоматически либо более простым способом, чем бизнес-роли и тем более системные.
Пререквизит роли	Составная часть более комплексной роли. Например, пререквизитами Бизнес-роли является одна или несколько системных ролей, а пререквизитами Профиля пользователя является набор

Глава 1. На чем строится доступ? Рекогносцировка информации, сетей, ресурсов и систем

Чтобы что-то защищать, надо сначала это увидеть, перечислить и учесть!

Настоящая глава расскажет о том, на чем базируется построение доступа, как определить, что такое «**защищаемая информация**», обрабатывающие ее ресурсы, процессы и системы, как их учесть, чтобы затем ими корректно управлять.

Начнем с главного — понимания, на чем строится доступ.

Что есть в любой компании — **информация, подлежащая защите (далее защищаемая информация)**. Это информация, которую требуется защищать от воздействий внешнего/внутреннего нарушителя, так и информация, которая должна быть доступна только отдельным категориям сотрудников для выполнения прямых обязанностей.

Защищаемая информация может быть определена законами РФ или отраслевыми стандартами как подлежащая защите в организации, так и информация определенного вида, защищать которую необходимо в соответствии с распоряжением руководства и внутренними нормативными докумен-

тами. Подробнее об этом мы поговорим чуть позже.

В начале есть информация, которую нужно защищать. Чтобы ее хранить, используют базу данных, хранимую, в свою очередь, на сервере. С учетом того, что информация и база данных с сервером нужны не одному работнику, могут использоваться несколько серверов. Для удобства использования вашей информации и базы данных используют серверы приложений и веб-серверы, которые красиво вам ее предоставят и позволят легко управлять, не мешая другим работникам. Несколько серверов объединяются в автоматизированную систему, которая работает быстрее и позволяет выполнять не все сразу, а разные функции.

Автоматизированная система, в свою очередь, может быть не одна, а вступать в интеграцию с другими системами, чтобы получать/отдавать необходимую ей дополнительную защищаемую и иную информацию и в итоге предоставлять сервис вашей компании. Разумеется, это упрощенная позиция, в которой не описано множество особенностей, но тут важен смысл и понимание природы доступа.

Упрощенно изучим это на схеме 1.

Как вы можете убедиться, для того чтобы добраться до необходимой информации, необходимо преодолеть немалый путь, включающий разные технологии, сети, протоколы, серверы, автоматизированные системы, базы данных и файловые ресурсы.

Тут сделаем ремарку, что на пути пользователя, помимо

всего вышеуказанного, есть еще и ограничители — такие как аутентификация (механизм определения пользователя, а именно, что он тот, за кого себя выдает), авторизация (механизм соотнесения введенной информации о логине/пароле с возможностью доступа) и средства защиты, которые в случае нарушения правил просто заблокируют или ограничат действия в системе или на пути к ней.

Весь этот путь по узлам и сквозь технологии и средства защиты, стоящие на пути от вашего рабочего места до необходимой вам в работе информации, **и есть доступ**, включающий **инструкции и правила прохода каждого из узлов** в согласованном порядке.

Составные части доступа, которые входят в него, но могут быть частями обеспечивающих подсистем (например, сетевые устройства и правила экранирования, файловые хранилища и т. д.), называются **— пререквизитами доступа.**

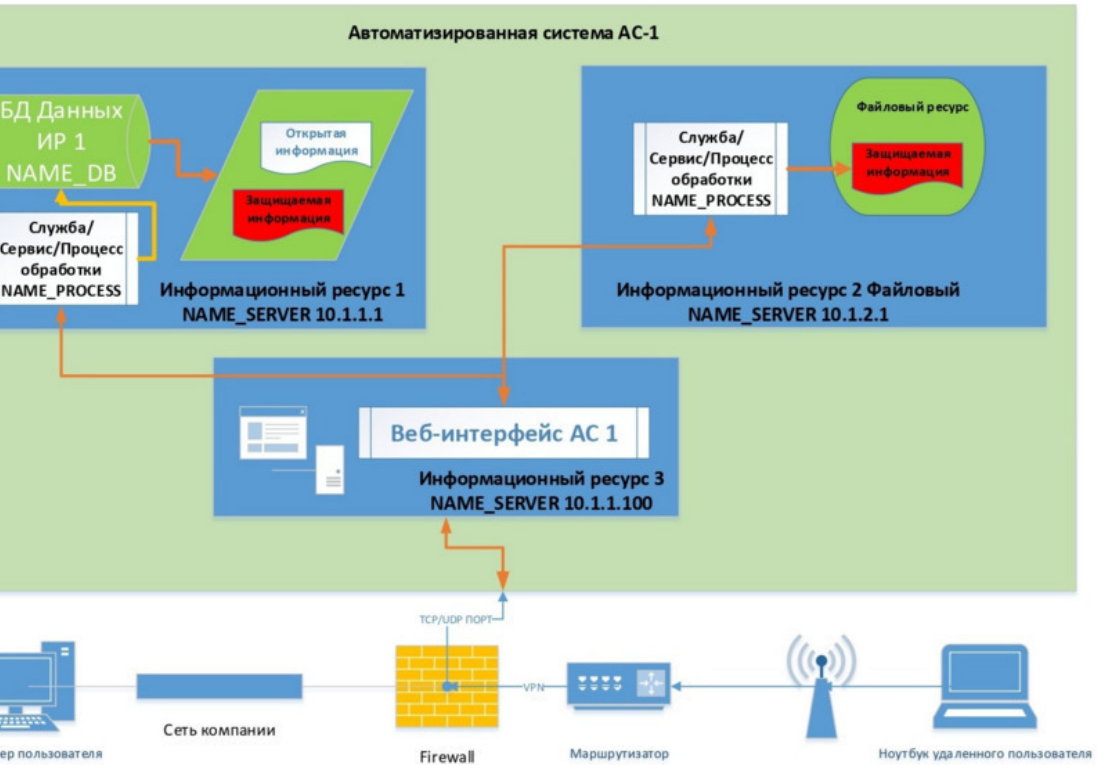

Автоматизированная система АС-1
БД Данных
ИР 1
NAME_DB
Открытая информация
Защищаемая информация
Служба/
Сервис/Процесс
обработки
NAME_PROCESS
Информационный ресурс 1
NAME_SERVER 10.1.1.1
Служба/
Сервис/Процесс
обработки
NAME_PROCESS
Файловый ресурс
Защищаемая информация
Информационный ресурс 2 Файловый
NAME_SERVER 10.1.2.1
Веб-интерфейс АС 1
Информационный ресурс 3
NAME_SERVER 10.1.1.100
TCP/UDP ПОРТ
VPN
Сеть компании
Firewall
Маршрутизатор
Ноутбук удаленного пользователя

Схема 1

Важно заметить, что доступ относится к разным составным частям, которые завязаны как на возможностях работы человека с компьютером, так и взаимодействиях систем друг с другом. Именно поэтому доступ не может быть основан только на работе систем, в нем непременно в опосредованной форме присутствует человек. Однако поскольку человека нельзя напрямую подключить к системе, используется его идентифицируемый реквизит — Учетная запись.

Учетная запись — совокупность данных, которая идентифицирует пользователя в компьютерной системе или ином ресурсе.

Учетные записи формируются в соответствии с правилами компании на основании ФИО работника и любых дополнений к этой информации (например, нумерации), чтобы сделать имя учетной записи абсолютно уникальным. Это особо важно, так как у одного сотрудника может быть не одна, а несколько учетных записей с разным уровнем привилегий (например, он разработчик или администратор системы), или же система/системы подразумевают формирование учетных записей строго локально, не ориентируясь ни на какие каталоги доступа.

Именно учетным записям на узлах или глобальной учетной записи, на которую «смотрят» эти узлы, присваиваются права доступа в рамках формируемого пути к системе и

взаимодействия человека с системой. Если же речь идет о машинном взаимодействии, то к учетной записи также добавляется необходимая информация о способах взаимодействия, местонахождении ресурсов и т. д. (например, адрес ресурса, идентификаторы машины, с которой нужно разрешить подключение на средствах обеспечения безопасности).

Чтобы защищаемую информацию никто, кроме ответственных работников, не изменил, не удалил или она не попала к не допущенным лицам, должны быть разработаны правила доступа к информации и способы управления таким доступом (выдавать и блокировать) в нужное время.

Различают **4 основных общепринятых подхода к управлению доступом**, которыми мы будем пользоваться частично или полностью для решения задачи:

Мандатное управление доступом (англ. Mandatory access control, **MAC**) — разграничение доступа субъектов к объектам, *основанное на назначении метки конфиденциальности для информации*, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

Дискретное (избирательное) управление доступом (англ. discretionary access control, **DAC**) — управление доступом субъектов к объектам *на основе списков управления доступом или матрицы доступа*. Также используются названия дискреционное управление доступом, контролируе-

мое управление доступом и разграничительное управление доступом.

Управление доступом на основе ролей (англ. Role-based access control, **RBAC**) — ограничивает доступ пользователей к системам, сетям и дополнительным ресурсам, предоставляя им только то, что необходимо для выполнения их конкретной роли. По сути, RBAC использует принцип наименьших привилегий (PoLP), чтобы пользователям предоставлялся доступ только к тому, что им нужно для эффективной работы.

Управление доступом на основе атрибутов (англ. Attribute-based access control **ABAC**) — определяет, кто может получать доступ к системам, сетям и данным на основе атрибутов, связанных со стандартами безопасности, ресурсами организации и средой пользователя. В отличие от RBAC, ABAC выходит за рамки роли пользователя и для авторизации доступа к ресурсам учитывает факторы, не относящиеся к его личности, например, его характеристики, среду и устройство.

И вроде кажется, что по отдельности эти методы уже перекрывают потребности в управлении доступом, но ровно до тех пор, пока вы не столкнетесь с ограничениями каждого из таких подходов, скудностью в описании учета и «серыми» зонами в принятии решений по тем или иным заявкам.

Разработанный мной метод включает в себя лучшее из всех 4 подходов и выстраивает единую удобную концепцию,

позволяющую сохранить гибкость и при этом высокий уровень информационной безопасности.

Тем не менее до использования в том или ином виде методов управления доступами *необходимо определить классификацию защищаемой информации и где она обрабатывается и хранится, прежде чем защищать ее и предоставлять к ней доступ*.

Как это сделать?

Как было указано ранее, в большинстве случаев основные категории уже продиктованы действующими законами или отраслевыми стандартами, а все остальное зависит от взгляда руководства на данное направление.

К защищаемой информации точно могут быть отнесены в любой компании:

• Персональные данные работников/клиентов/партнеров и т. д. компании (определяется законом 152-ФЗ РФ и подзаконными актами, а также документами ФСТЭК России);

• Коммерческая тайна (определяется законом 98-ФЗ РФ — перечень такой информации формируется самостоятельно, за исключением категорий информации, определенной законом, которые не могут таковыми быть).

Если ваша компания работает в отдельных сферах (напри-

мер, связи, финансовой сфере, сферах производства и иных областях), то к защищаемой информации необходимо отнести требования отраслевых стандартов или регуляторов (Роскомнадзора, ФСБ, ФСТЭК).

Так, например, для банковской и финансовой сферы регулятором является Банк России, а принимаемые им стандарты и постановления обязательны для исполнения всеми финансовыми организациями, начиная от микрофинансовой организации и ломбарда, заканчивая гигантами банковской сферы.

Стандартами в финансовой сфере являются на сегодняшний день:

- 683-П — постановление Банка России, определяющее требования к защите информации;
- ГОСТ 57580—1,2 — описывает обязательные требования по защите информации и соответствующих процедурах их обеспечения;
- PCI-DSS — международный стандарт по защите информации банковских карт и данных об их владельцах.

Если компания работает в сферах, связанных с обороной государства, или взаимодействует с ведомствами, связанными с обороной государства или обеспечением безопасности, то также может присутствовать информация, составляющая государственную тайну.

Также может присутствовать информация в соответствии с деятельностью компании и соответствующим процессом ведения бизнеса и получения доходов. Полный перечень нормативных документов могут предоставить юристы либо руководители подразделений вашей компании после изучения данного вопроса.

Для простоты понимания в данной книге мы будем оперировать теми видами защищаемой информации, обеспечение безопасности которых наиболее популярно.

Исходя из сказанного выше, следует вывод, что прежде, чем приступить к управлению доступом и тем более к его защите, необходимо сначала собрать информацию о том, какую информацию защищать, где она хранится и как она передается/обрабатывается.

***Рекогносцировка* — работа, связанная с инвентаризацией положения от информации к системам и механизмом, участвующим в ее обработке.**

Он делится на несколько важных этапов, в рамках которых разрабатываются жизненно важные для дальнейшей работы процессы и документы, подразумевающие под собой определение «где-что-как-зачем обрабатывается».

На первом этапе рекогносцировки следует начать именно с *перечисления всех видов информации*, утеря/компрометация которой может вылиться в штраф, в потерю заработка для бизнеса либо уголовную ответственность руководства.

Может показаться, что руководство подразделения или подразделение ИТ знает все. Зачем тогда писать ненужную бумагу? Однако вы будете удивлены, когда к ним подойдете с этим вопросом или попытаетесь узнать детали. В 90% случаев никто ничего не знает, а действует по интуиции и в абсолютном бардаке. Поэтому составить и утвердить перечень — жизненно важно. Сбор данной информации — это предмет аудита, о проведении которого в данном контексте я углубляться не буду, остановимся лишь на его результате.

Пример того, как нужно минимально собрать информацию в виде таблицы-перечня со следующими столбцами:

- **№** — порядковый номер.
- **Название защищаемой информации** — Краткое название информации, подлежащей защите.
- **Цель обработки** — Описать, с какой целью производится обработка защищаемой информации по ее типу.
- **Требование по защите** — Указать прямую ссылку на закон, положение, постановление, ИСО/ГОСТ и т. д. или ваш внутренний документ.
- **Виды документов** — Описать все формы и виды документов, в которых есть защищаемая информация.
- **Метка** — Обозначение в документе, файле и/или ином носителе, дающее определение находящейся там защищаемой информации.
- **Где обрабатывается/хранится** — Указать либо поме-

щения, либо подразделения, либо автоматизированные системы.

• **Критичность** — определяется в соответствии с риск-ориентированным подходом, моделями угроз и нарушителей, а также проверкой «что будет, если».

• **Ответственный за обработку** — лицо, назначаемое приказом на должность ответственного за обработку отдельного вида или подвида информации. Данное лицо будет влиять в дальнейшем на маршруты согласования.

Пример заполнения может быть следующим (Таблица 1):

№	Название защищаемой информации	Цель обработки	Требование по защите	Виды документов	Метка	Где обрабатывается/ Храниться	Критичность	Ответственный за обработку
1	Персональные данные работников ...	Кадровое делопроизводство	152-ФЗ, 21 приказ ФСТЭК России	Личные дела работников, личные дела в рамках ИС 1С ЗУП и т.д. ...	ПД	Адрес ... Помещение 1, Автоматизированная система 1С ЗУП	Высокая (жалобы в Роскомнадзор, штрафы)	Иванов И. И.
2	Персональные данные клиентов ...	Обслуживание клиентов по договорам ...	152-ФЗ, 21 приказ ФСТЭК России	Файлы на файловом сервере ...	ПД	Адрес .. Помещение 2, Подразделение продаж, Автоматизированная система 1С CRM	Критичная (жалоба в Роскомнадзор, штрафы, проверки, остановка бизнеса)	Иванов И. И.

Таблица 1

Дополнение таблицы информацией о критичности информации облегчит жизнь работникам безопасности и руководству, которые будут точно знать, что охранять и насколько критичны могут быть инциденты, связанные с такой ин-

формацией.

В любом учете **никогда не скупитесь на достаточную понятность информации или набора данных**. Лучше потратьте время и сделайте красиво и понятно, чем искать выходы во время активных действий или инцидентов безопасности. Любые доступные примеры таблиц дополняйте нужной вам информацией в дополнительных столбцах, заранее определяя, как их правильно заполнять.

На втором этапе рекогносцировки определяются процессы, в рамках которых производится обработка защищаемой информации по ранее составленному перечню.

Пример того, как нужно минимально собрать информацию в виде таблицы со следующими столбцами (Таблица 2):

- **№ —** Порядковый номер.
- **Название защищаемой информации —** Краткое название информации, подлежащей защите.
- **Процесс —** Описать процесс, в котором фигурирует защищаемая информация.
- **Владелец процесса —** Указать подразделение-владельца процесса или ФИО и должность ответственного лица.
- **Актив (физический/виртуальный) —** Описать используемые для этого активы и ресурсы (например, системы и серверы, файловые ресурсы и реальные физические хранилища накопителей информации, соответственно).

№	Название защищаемой	Процесс	Владелец процесса	Актив Физический	Актив Виртуальный
1	Персональные данные работников	Кадровое делопроизводство	Иванова И.И Директор по работе с персоналом	Шкафы с картотекой в помещении 303 по адресу...	Сервер WS_FS_1C_01 (либо указатель на учет реестра ресурсов и активов)
				...	Система 1С-ЗУП (либо указатель на учет реестра автоматизированных систем)
					...

Таблица 2

Говоря о физических активах, при формировании всегда стоит пользоваться принципом минимизации функции каждого ресурса и актива. То есть если в шкафу вы храните защищаемую информацию в виде персональных данных, то не стоит хранить там же не связанную с ней общедоступную информацию, например, флаеры на скидку по услугам для раздачи. Во-первых, потому что в таком случае вам будет трудно обеспечить конфиденциальность таких данных, поскольку за флаерами на скидку может подойти неуполномоченный сотрудник, во-вторых, потому что цели работы с персональными данными и с флаерами абсолютно разные, а закон запрещает хранение и обработку не связанной разнородной информации. Аналогичное требование и к серверам обработки защищаемой информации и серверам хранения. (Пример — Федеральный закон №152-ФЗ «О персональных дан-

ных» обязывает операторов принимать все необходимые меры для защиты персональных данных от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий, что невозможно без разделения).

Придерживайтесь принципа «все по полочкам», и проблем будет значительно меньше.

На третьем этапе рекогносцировки мы определяем все ресурсы и системы (как внутренние, так и внешние), где производится обработка защищаемой информации. Это нужно как для наглядности, так и для конструирования и метки контуров защиты информации и отделения друг от друга тех или иных ресурсов и систем, чтобы обеспечить гранулированный к ним доступ в дальнейшем, а также нужный уровень защиты.

Составляются 5 основных документов, на основании которых строятся буквально все информационные технологии и информационная безопасность:

- Реестр автоматизированных систем (АС).
- Реестр информационных ресурсов (ИР).
- Реестр сегментов сети (VLAN).
- Реестр протоколов.
- Реестр портов/служб взаимодействия.

Стоит жестко контролировать, чтобы информационные

ресурсы (включая сети, протоколы, службы) были включены в автоматизированные системы. Множество «висячих» и «бесцельных» ресурсов создают засоренность и не позволяют корректно работать с доступом, кроме того, являются сборщиком причин уязвимостей, что в конечном счете приводит к инцидентам информационной безопасности и утечкам защищаемой информации. Это недопустимо и при обнаружении должно быть немедленно устранено путем консультации с подразделением информационных технологий и выведения ресурса из эксплуатации, либо его учет в целевой автоматизированной системе и последующей миграции в соответствующий контур безопасности. Также необходимо блокировать те ресурсы, которые у вас появились без регистрации в реестрах. Во-первых, это могут быть действия злоумышленников, во-вторых, такие узлы и ресурсы создают «серые» зоны в сети предприятия и увеличивают риски неправомерных действий.

Подробнее о документах (описание наполнения представлено в минимально-необходимом объеме для использования в дальнейших методиках построения моделей):

• **РЕЕСТР АВТОМАТИЗИРОВАННЫХ СИСТЕМ (далее Реестр АС) —** это перечень комплексных систем с точными их названиями, включенными в их комплекс подсистемами и информацией, позволяющей описать цель работы системы и ответственных лиц.

Благодаря такому учету можно понять цель системы, какая защищаемая информация обрабатывается в ее ресурсах, кто заинтересован в ее работе и кто является администратором. Информацию можно получать путем ведения простого EXCEL-файла в комплексе с приказами на введение систем. Желательным является внедрение систем инвентаризации или Enterprise Asset Management (EAM).

В рамках реестра должны определяться как *внутренние системы*, так и *внешние системы*.

• **№ —** порядковый номер учета, либо идентификатор системы.

• **Дата введения —** дата занесения в реестр по документам.

• **Автоматизированная система —** точное название основной системы, утвержденной документами.

• **Подсистема —** точное название вложенной (дочерней) системы в составе Автоматизированной системы.

• **Версии названий —** если система переименовывалась, то необходимо учесть предыдущие версии названий.

• **Описание —** описание целевого назначения системы.

• **Класс системы —** описательный класс системы, подразумевающей отнесение к общей классификации автоматизированных систем (например, CRM, ERP, СЗИ и т. д.).

• **Наличие защищаемой информации —** указатель на наличие в системе критичной информации по Реестру ЗИ.

• **Размещение —** место размещения систем и их ресур-

сов, если присутствует несколько площадок такого размещения.

• **Контуры системы** — контур (или в аналогичном смысле используется «полигон») системы, подразумевающий развертывание системы в одной или нескольких версиях для целей модернизации, тестирования и других вариантов модификации перед внедрением в продуктивную среду с применением соответствующих правил и ограничений информационной безопасности. Вариативность контуров будет рассмотрена в главе 8.

• **Статус системы** — указатель текущего статуса (в эксплуатации, внедрение, разработка, тестирование и т. д.).

• **Критичность системы** — показатель рассчитанной критичности системы (критичность должна определяться экспертным путем, риск-ориентированном подходом «что будет, если» либо наличием защищаемой информации или выполнением основополагающих бизнес- или технологических функций).

• **Владелец системы** — указатель на конкретного владельца или подразделение-владельца.

• **Администратор системы** — указатель на группу сопровождения или конкретного администратора системы.

• **Дата ввода в эксплуатацию** — фактическая дата ввода в эксплуатацию.

• **Дата вывода из эксплуатации** — фактическая дата вывода из эксплуатации.

• **РЕЕСТР ИНФОРМАЦИОННЫХ РЕСУРСОВ (далее Реестр ИР)** — это перечень серверов и рабочих станций в сети предприятия. По реестру ИР можно с легкостью определять ресурсы в составе информационных систем, ответственных лиц, адресацию и определить уровень защиты.

Благодаря такому учету появляется возможность видеть контур информационных технологий и ресурсов на предприятии. Информацию можно получать как путем ведения простого EXCEL-файла в комплексе с любым свободно распространяемым сканером сетей, так и путем внедрения систем инвентаризации ресурсов с возможностью сканирования и обновления информации в автоматическом режиме.

Реестр целесообразно заполнять для всех внутренних ресурсов, DMZ-ресурсов, физического оборудования.

• **№** — порядковый номер учета, либо идентификатор системы.

• **Дата введения** — дата занесения в реестр по заявке.

• **Имя ресурса** — фактическое точное имя.

• **IP-адрес —** фактический статический IP (целесообразно дополнить MAC-адресы в отдельное поле, если вы собираетесь делать фильтрацию по MAC).

• **Описание функции** — описание целевого назначения ресурса (не рекомендуется совмещать функции на одном ресурсе, следует придерживаться правила — «один ресурс — одна функция»).

• **Класс сервера** — отнесение к общей классификации сервера, сформированной в организации (например, Сервер системы защиты, Сервер АСУ ТП, Сервер ИСПДн и т. д.).

• **Контур** — определение контура, в котором размещается ресурс.

• **Автоматизированная система** — Указатель на Реестр автоматизированных систем, на систему, в рамках которой развернут ресурс (напоминание — необходимо максимально уйти от принципа «висячих» ресурсов, т. е. без определения конкретной системы).

• **Критичность ресурса** — показатель рассчитанной критичности ресурса (критичность должна определяться экспертным путем, риск-ориентированном подходом «что будет, если», либо наличием защищаемой информации или выполнением основополагающих бизнес- или технологических функций).

• **Владелец ресурса** — указатель на конкретного владельца или подразделение-владельца.

• **Администратор ресурса** — указатель на группу сопровождения или конкретного администратора системы.

• **Средства защиты и исключения** — описание установленных средств защиты или исключения из такой установки и альтернативных сценариев обеспечения информационной безопасности.

• **Дата вывода из эксплуатации** — фактическая дата вывода из эксплуатации.

• **Статус ресурса** — указатель текущего статуса (в эксплуатации, выведен и т. д.).

• **РЕЕСТР СЕГМЕНТОВ СЕТИ** (далее Реестр сегментов сети (VLAN)) — это перечень подсетей и контуров вычислительной сети, в рамках которых располагаются ресурсы и системы в соответствии с целью применения и защиты информации.

Благодаря такому учету появляется простота и наглядность в определении сети предприятия, подсетей, из которых она стоит, и зонах ее топологии. Информацию можно получать как путем ведения простого EXCEL-файла в комплексе с любым свободно распространяемым сканером сетей (например, NMAP или Netdiscover).

• **№** — порядковый номер учета, либо идентификатор системы.

• **Дата введения** — дата занесения в реестр по заявке.

• **Подсеть учета** — адресация IPv4 или IPv6 с указанием маски (например, 10.10.10.0/24), либо адресация иного протокола (если таковые используются, целесообразно добавить поле, относящееся к иным протокольным соединениям).

• **VLAN** — рекомендуется брать номера длиной 3—5 знаков, подразумевающих описание устройства, номер порта устройства и номер VLAN (т. е. 112 будет означать 1 — главный маршрутизатор, 1 — номер порта на нем 1, 2 — VLAN №2).

• **Описание** — Краткое описание, для чего используется VLAN. Рекомендуется делить VLAN в соответствии с контурами, однотипными устройствами, либо целевым назначением типов хранимой информации, либо узлов.

• **Контур** — Указатель контуров, указанных в реестрах выше.

• **Размещение** — Флаг указания отношения к отдельным сегментам (набор сегментов следует определять самостоятельно, минимально выделяют LAN — локальная сеть, DMZ — демилитаризованная зона и OI — открытые сети интернет).

• **Маршрутизатор** — указание на головной маршрутизатор сети.

• **Разрешения** — указатель на номера VLAN, с которыми разрешены соединения (разрешения соединений не подразумевают правила FireWall, а вообще возможность ходить из одного VLAN в другой, к не указанным в списке должна быть выставлена блокировка).

• **РЕЕСТР ПРОТОКОЛОВ** — это перечень сетевых протоколов, используемых в сети для взаимодействия информационных ресурсов и систем по модели ISO/OSI (взаимодействия открытых систем).

Благодаря такому учету появляется понимание, какие протоколы доступа используются для взаимодействия в вашей сети, а какие можно ограничить или закрыть, чтобы они

не могли быть использованы злоумышленниками в случаях появления в них уязвимостей.

Информацию можно получать путем ведения простого EXCEL-файла.

• **№ —** порядковый номер учета, либо идентификатор системы.

• **Дата введения —** дата занесения в реестр по заявке.

• **Уровень модели OSI —** подразумевает указатель на один из 7 уровней модели OSI.

• **Наименование протокола —** в соответствии с заводским названием.

• **Статус —** разрешение или запрет.

• **Описание статуса —** условия, при которых протокол может быть разрешен или запрещен.

• **РЕЕСТР ПОРТОВ И СЛУЖБ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ —** это перечень портов и служб, закрепленных по умолчанию, их перераспределение для нужд предоставления доступа и использования системами и протоколами при работе информационных ресурсов.

Благодаря такому учету появляется понимание, какие технологии используются в вашей компании, а также какие порты необходимо открыть на сетевых устройствах класса Firewall, чтобы приложения и системы работали стабильно и правильно.

Информацию можно получать как путем ведения просто-

го EXCEL-файла, так и с помощью систем NetFlow или сканеров канального и сетевого уровней модели OSI.

• **№ —** порядковый номер учета, либо идентификатор системы.

• **Дата введения —** дата занесения в реестр по заявке.

• **Протокол —** указатель на реестр протоколов.

• **Номер порта и служба —** указание службы и номера порта (сам по себе порт ввода-вывода не является уязвимым, однако стартующая под ним уязвимая служба и является причиной несанкционированного доступа). Ввиду невозможности перенастройки или отключения отдельных службы рекомендуется исключать порты и службы соответственно.

• **Статус —** разрешение или запрет.

• **Информация об уязвимости или вредоносном распространении —** ссылки на открытую информацию об уязвимости порта+службы или распространении через них вредоносных программ

В каждый из реестров целесообразно добавлять информацию по заявкам, на основании которых производится введение или ссылки на артефакты, с помощью которых получена информация.

Разумеется, объем полей может быть увеличен и обогащен любой необходимой для понимания руководства компании и работников информацией, тем не менее рекомендую

не сильно расширять рабочие документы в целях их удобного использования.

Требования к наименованию систем и ресурсов, а также наполнению полей реестров определяются работниками подразделений управления информационными технологиями совместно с информационной безопасностью.

После учета всех ресурсов и систем глобальный контур компании считается «замкнутым», а служба информационной безопасности получает право на блокировку любых неучтенных в реестрах ресурсов и систем, а также реагирования/расследования инцидентов при появлении неучтенных объектов в сети. При таком подходе крайне важна связь и взаимодействие между подразделением информационных технологий и подразделением информационной безопасности.

Рекомендацией в этой ситуации является создание приказа и положения, на основании которых производится работа по инвентаризации и учету информационных ресурсов и автоматизированных систем и ведение указанных выше реестров, а также разделение зон ответственности каждой из сторон.

Следует обратить внимание, что ***указанные выше и подобные реестры сами по себе являются защищаемой информацией, т. к. описывают структуру компании***. Поэтому хранение таких данных следует производить в секрете и допускать только отдельных уполномоченных лиц.

Ведение таких реестров является постоянной работой, которую следует производить совместными усилиями с подразделением информационных технологий. Желательным является ведение реестров в специализированных системах с уровнями подобной инвентаризации либо в EXCEL-файлах с интеграцией с помощью скриптов Visual Basic, Python и BASH, с инструментами постоянного сканирования и выявления неучтенных элементов. Такая интеграция возможна, например, с Nessus, NMAP.

Глава 2. Потребность в управлении доступом

Стоит определиться на берегу — зачем вообще управлять доступом к системам и информации?

В современных компаниях потребность в управлении доступами появляется, когда происходят проверки, либо случаются инциденты с утечками или действиями злоумышленников, парализующими бизнес-процессы, и редко, когда руководитель понимает, что в его компании должен быть порядок, а доступы должны предоставляться доверенным людям, безопасные и контролируемые.

Начнем с логики и закончим требованиями разных стандартов и законов, что в свою очередь позволит обосновать эту необходимость на всех уровнях.

2.1. Логический взгляд на управление доступом к ресурсам сети вашей организации

Начнем с банального — рабочее место работника.

Если любому работнику компании, даже выполняющему функцию «сложить на компьютере 2 +2, используя калькулятор, и записывать результат в блокнот», дать права администратора, то он с огромной радостью поставит на этот компьютер World of Tanks, торрент, Телеграм и другие «веселые программы». Ведь никто это формально и физически не ограничивает, да и на его функцию сложения и записи это никак не влияет.

То есть отсутствие ограничений на доступ к установке программ ведет к неизбежному злоупотреблению полномочиями, так как при успешном выполнении задачи, пока начальство не смотрит, работнику нечего делать. А занять время как-то хочется.

Это еще самый безопасный сценарий.

А теперь представим, что работник не просто со скуки злоупотребляет вашим оборудованием, а инсайдер компании-конкурента, мошенник или злоумышленник-террорист. Такой человек запросто поставит необходимое ему программное обеспечение, с помощью которого запустит инже-

неров компании-конкурента или ОПГ, или будет тихонько сливать истинному работодателю вашу клиентскую базу. А затем еще и «анонимно» даст интервью о том, насколько ваша компания небезопасна.

Суммируя эти сведения, ваша компания из-за одного такого «засланного казачка» вполне может перестать существовать, так как ваши партнеры и клиенты не оценят такой подход к делу и информации, которой они с вами делятся в рамках рабочей деятельности.

Продолжим экстраполяцию и посмотрим на доступ в интернет.

По причине все той же скуки на рабочем месте часто работники ходят на совершенно отвлеченные от работы сайты, социальные сети или мессенджеры. Не трудно догадаться, что без ограничений на доступ в открытую незащищенную сеть работник, имеющий низкий навык работы в ней или попросту бескультурный, запросто полезет на ресурсы, например, содержащие порнографию, либо сериалы, либо нелицензионный взломанный софт, либо попросту пройдет на фишинговый сайт и сам не заметит, как впустит злоумышленника в сеть.

Заражение вредоносным программным обеспечением — дело нескольких дней.

Получается, что отсутствие ограничений в интернет — это прямая дорога злоумышленников в вашу сеть через безответственного или просто обнаглевшего пользователя и его

активность в такой сети.

Экстраполируя на злонамеренность работника, вариант утечки информации, используя даже самые примитивные инструменты вроде VPN и бесплатной почты, — это самая очевидная атака на информацию вашей компании.

Коснемся и информационных систем, где, собственно, и обрабатывается информация, которая является для компании ценной либо требующей защиты в связи с требованиями закона (например, персональные данные).

Не имея ограничений (т. е. права администратора) в такой системе, работник в самом очевидном случае может войти в раздел, где, например, будет фигурировать его зарплата, и увидит, что у него и у соседа по столу напротив она различается как минимум в 2 раза. Полагаю, будет трудно объяснить, почему соседний работник, складывающий 2 +2, делает это лучше.

Кроме того, информацию он может попросту скачать себе и затем использовать как угодно. Например, продать злоумышленникам из обиды и желания компенсировать недоплаченные средства. И никто ему в этом не сможет помешать. При проявленной хитрости и анонимизации доступа вы даже не сможете выйти на такого обиженного работника.

А теперь подумаем о том, что работник, имея неограниченный доступ и гуляя по системе, к примеру, получил доступ к секретной разработке вашей компании, на которой ваша компания планировала сделать ставку, вложилась в ре-

кламу и перестроила производство. Но вот он получил доступ и хохмы ради решил похвастаться «крутизной» вашей компании перед друзьями в социальных сетях. Вы скажете: «Ну и что?» Да все просто — поисковые запросы и открытые страницы пользователей социальных сетей индексируются поисковиками, а ваши конкуренты умеют пользоваться поисковыми запросами и dorks osint-запросами. Завтра они увидели пост вашего работника и сделали вашу работу быстрее вас, выйдя с новым товаром на рынок. Итог — прямые и существенные потери для бизнеса в виде неполученной выгоды.

Здесь я указал простые и понятные примеры, к чему может привести вседозволенность в доступах разного уровня. Управление доступами в компании — это не способ «накинуть ошейник на сотрудника» и контролировать каждый его шаг, а **инструмент недопущения глупости и обеспечения безопасности как сотрудников, так и компании**, например, как ограждение около опасной зоны с дикими зверями в зоопарке. Разумеется, способов намного больше, и они намного сложнее. Злоумышленник зачастую паразитирует на неопрятности работы вашей компании.

Как и в случае с реальной безопасностью на производстве, на информационную безопасность и управление доступами часто закрывают глаза. Работает — не трогай! Однако это ровно до той поры, пока не случится инцидент с утечками или остановками бизнеса. Потери из-за этого могут сделать

компанию банкротом либо в худшем случае — привести на скамью подсудимых как нарушителя, так и руководство.

2.2. Требования законов и стандартов

Именно в этой главе придется столкнуться с очевидной дырой в законодательстве на момент написания книги, дающей понять, что данная **область не регламентирует способы управления доступом в те или иные системы и не определяет методики, как это делать корректно и безопасно**. Таким образом, в частности, каждый работник информационной безопасности сталкивается с абсолютным непониманием, как ему вести это направление и как ограничивать доступ. Многие считают, что, ставя средство защиты в виде маршрутизатора с FIREWALL, оно само что-то там будет фильтровать и ограничивать действия злоумышленников. Однако это заблуждение, и без наведения порядка и введения четких правил разграничения доступа будет ситуация — либо «все доступно», либо «ничего не работает».

Давайте рассмотрим, а что вообще есть в этом направлении:

Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации»

«Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных

на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации».

Мы видим наличие требований предотвращения несанкционированного доступа, обнаружения фактов и предупреждать его, но при это не указано, как это делать. Тем не менее это фиксирует запрос законодательства в этом направлении хотя бы общими словами.

«ГОСТ Р 59383—2021 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ»

В своей основе описывает базовые понятия, аналогичные описанию в настоящей книге, однако не дает четкости построения моделей, форм, состава доступа и скорее годен для общего развития, чем для применения «как есть». Еще одним большим минусом является необязательность соответствия данному стандарту для компаний и государственных органов, а также применимость для конкретной защищаемой информации.

Закон 152-ФЗ (в соответствии с периодом написания книги), регламентирующий защиту персональных данных:

В его тексте говорится:

«Ограничение доступа:

Доступ к персональным данным должен быть ограничен кругом лиц, которым он необходим для выполнения их служебных обязанностей или для достижения целей, предусмотренных законом.

Согласие субъекта данных:

Обработка персональных данных, как правило, требует согласия субъекта персональных данных, за исключением случаев, когда обработка осуществляется на основании закона или международного договора.

Обеспечение безопасности:

Операторы персональных данных должны принимать необходимые меры для обеспечения безопасности персональных данных, включая защиту от несанкционированно-

го доступа, уничтожения, модификации, блокирования, копирования, распространения и других неправомерных действий».

Анализируя и этот закон, мы видим лишь то, что есть запрос на ограничение и контроль, но все абсолютно абстрактно и не содержит никаких явных инструкций.

Стоит обратить внимание на ГОСТ Защита информации СИСТЕМЫ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ И ПРАВАМИ ДОСТУПА Общие требования (который, правда, на момент написания книги был лишь проектом).

В целом является примером описания бизнес-процессов управления доступами через кадровые события и единый каталог (Схема 2). Также в нем сформированы базовые понятия системных и бизнес-ролей и взаимодействия с пользователем. В случае его утверждения настоящая книга в целом не только будет соответствовать требованиям стандарта, но и дополнять их недостающими сведениями об управлении доступом.

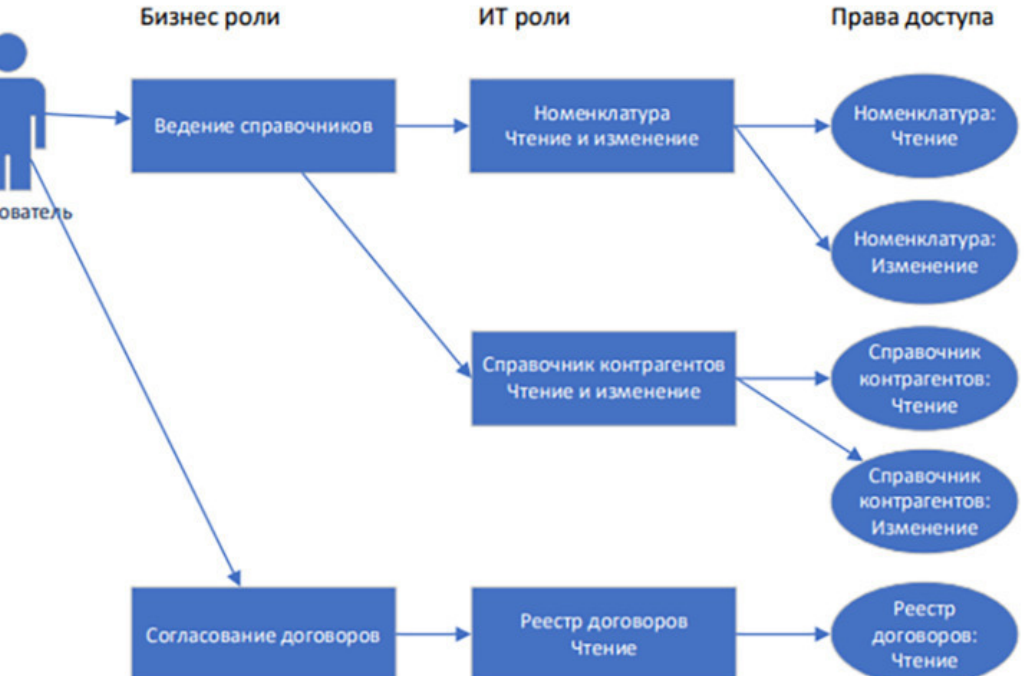

Бизнес роли
ИТ роли
Права доступа
ователь
Ведение справочников
Номенклатура
Чтение и изменение
Номенклатура:
Чтение
Номенклатура:
Изменение
Справочник контрагентов
Чтение и изменение
Справочник
контрагентов:
Чтение
Справочник
контрагентов:
Изменение
Согласование договоров
Реестр договоров
Чтение
Реестр
договоров:
Чтение

Схема 2

Используя методики, изложенные в настоящей книге, требования законов и даже стандартов будут выполнены, а злоумышленники столкнутся либо с действительно сложной защитой периметра, требующей высоких знаний, ловкости и дорогостоящих инструментов проникновения (0-day уязвимостей или систем действия на уровнях закладок или уязвимостей ядер систем), либо будут вычислены и остановлены при первых попытках проникновения в сеть, либо совершат критичные ошибки, при которых службы информационной безопасности смогут их вычислить и остановить до совершения задуманного.

2.3. Внутренние документы

Рассмотрим набор документов и их содержание для успешного управления доступом в дополнение к документам информационной безопасности и информационным технологиям.

В первую очередь набор документов должен быть расширением действий Политики информационной безопасности, принятой в компании.

Основным документом должен быть документ второго уровня — **Политика управления доступом к информационным ресурсам и автоматизированным системам** (или иногда Регламент, Порядок).

Разделы, которые следует отразить в данном документе, должны включать:

- **Предоставление доступа к информационным ресурсам —** описывает общий процесс доступа к информационным ресурсам на основании заявок. Как, что, где в какой форме.
- **Предоставление доступа к автоматизированным системам —** описывает общий процесс доступа к автоматизированным системам на основании заявок. Как, что, где в какой форме.
- **Оформление заявок на доступ в рамках создания**

нового рабочего места — описывает процесс создания рабочего места, ранний прием сотрудника, наличие базовых доступов.

• **Предоставление доступа к внешним информационным ресурсам и автоматизированным системам** — описывает процесс добавления в белый список ресурсов сети интернет, включая почту, подрядные организации и т. д.

• **Предоставление доступа к базам данных** — описывает процесс получения доступа к базам данных как пользователей, так и приложений (например, с помощью шин данных, API или иных подходов к гранулированному обмену информации).

• **Формирование учетных записей работников для доступа к информационным ресурсам и автоматизированным системам** (внешним, внутренним, локальным, привилегированным, техническим) — описывает процесс и стандартный общий подход к формированию имен и уникальных идентификаторов учетных записей на всех уровнях, а также учет таких учетных записей.

• **Инвентаризация учетных записей, информационных активов и доступа к ним** — детализирует процесс проверки, наследования новым владельцам технических учетных записей и доступов, соответственно, контрольные сроки, ограничения на использование и т. д.

• **Изменение и прекращение прав доступа** — процесс отзыва доступов либо его дополнения, изменения для всех

видов учетных записей.

• **Управление ролевыми моделями доступа** — процесс построения ролевых моделей для систем, их изменение, управление и утверждение, а также прекращение использования ролей и их отзыв, также процесс управления предоставления полномочий и принятия решений по всем видам заявок на доступ.

• **Предоставление удаленного доступа** — соответственно, процесс относительно всех видов удаленного доступа и управление им, подключение удаленных сервисов и пользователей.

• **Распределение ролей и ответственность** — обязательная часть в отношении лиц, являющихся как частью процесса управления доступом, так и частью согласовательного процесса для определения зон ответственности каждой стороны, а также описания нарушений и последствий.

При написании **Политики управления доступом** следует учесть все виды пользователей, механизм подачи/согласования/учета и контроля заявок на доступ, а также механизмы его предоставления и отзыва. Документ должен служить понятной инструкцией по определенным процессам управления к действию, поэтому следует делать его подробным и исчерпывающим. (Пример такого документа в Приложении 1.)

Простейшая политика управления доступом может опре-

делять почтовый адрес приема заявок, форму заявки и ее наполнение, время обработки, маршрут согласования и порядки выдачи и отзыва доступа, аудит и контроль и ответственность участников процесса.

При необходимости в документ можно вставить данные по формированию и управлению ролевых моделей описанные далее, однако настоятельно рекомендую сделать это в рамках отдельного регламента, поскольку это сильно увеличит объем Политики и потребует частого ее переутверждения ввиду подвижности процесса управления матрицами.

Разрабатываемые документы должны утверждаться приказом генерального директора по компании и выполняться всеми работниками, подрядчиками и т. д., определенными как целевая аудитория данного документа.

ВАЖНО! Довести и «переломить ситуацию» в следующих направлениях и запретить:

- согласовывать и предоставлять доступы пользователям «как у кого-то»;
- согласовывать доступ без обоснований или с пометкой «для выполнения должностных обязанностей», по звонку от руководителя сотрудника и т. д.;
- пользователям получать привилегии Администратора и совмещать административные функции в системе (и сопровождения) с выполнением бизнес-операций в системе;
- администраторам выполнять работу за пользователей;

• заставить пользователей всех видов выполнять требования парольной политики и наказывать за компрометацию паролей;

• разработчикам работать в продуктивном сегменте и применять изменения в неурочное время.

Чтобы это сделать, необходимо предоставить им информацию о доступах в удобном и понятном виде. Если говорить на более бытовом уровне — как меню в ресторане.

И здесь следует учитывать следующие аспекты:

• **Понятность** — сотруднику даже с низким уровнем компьютерной грамотности должно быть понятно, что он заказывает и хочет получить. Одновременно с этим описательная часть, скрывающаяся за кратким названием, должна быть достаточной для работы сотрудников ИБ и ИТ подразделений для выдачи такого доступа и его отзыва в дальнейшем.

• **Краткость** — сотруднику должен предоставляться небольшой набор выбора в соответствии с его целями, чтобы он не запутался. Одновременно с этим набор должен быть исчерпывающим относительно тех бизнес-функций, которые выполняет такой сотрудник.

• **Удобство** — сотруднику должен быть предоставлен удобный интерфейс с клиентским путем выбора, прозрачным согласованием и быстрым предоставлением доступа в кратчайший возможный срок после согласования. Все нуж-

ные составляющие части доступа уже должны быть включены в состав доступа для функционирования — «включил и работает». При этом удобство должно касаться и сотрудников обслуживания таких запросов.

• **Прозрачность —** сотрудникам должен быть предоставлен понятный и прозрачный процесс согласования доступа и принятия решений «согласовано/отклонено» на основании правил, однозначно определяющих процесс принятия решений.

• **Безопасность —** предоставляемые доступы должны быть гранулированы и обеспечены защитой как от сторонних манипуляций (например, выключения неуполномоченным лицом), так и прослушивания и утечки информации. Каналы, протоколы и службы предоставления доступа должны иметь встроенные механизмы конфиденциальности, целостности и доступности передаваемой информации. Также пользователь должен быть идентифицирован, аутентифицирован и авторизован.

Как же учесть набор таких аспектов с учетом их противоречивости?

Ответ: Используя настоящий авторский «Метод Пирамиды», включающий ранее указанные методики DAC, MAC, RBAC и ABAC. Подробнее о методе см. главу 4.

Набор сопутствующих документов, прилагаемые материалы которых будут служить информационными источника-

ми, следующий:

• **Политика сегментации сети —** описывает проектирование и использование сети и ведение реестра VLAN, реестров протоколов, портов и служб.

• **Политика инвентаризации автоматизированных систем, ресурсов и активов —** описывает процессы учета информационных ресурсов, активов и систем, а также ведение реестров автоматизированных систем, информационных ресурсов, файловых ресурсов и т. д.

• **Политика использования систем вычислительной техники —** описывает процесс использования вычислительной техники, создания рабочих мест, особенности ее учета и внесения изменений в сети для ее подключения, жизненный цикл вычислительной техники.

• **Политика использования баз данных —** описание процесса создания и ведения баз данных, ведение реестра баз данных.

• **Политика использования электронной почты —** описывает процесс использования электронной почты, ее получение сотрудником и правил создания почтовых ящиков.

• **Политика учетных записей и паролей —** описывает правила создания учетных записей всех видов (пользовательские, административные, технические, локальные и т. д.), требования к паролям, жизненный цикл их смены.

• **Политика использования файловых ресурсов —**

описание процесса создания и ведения файловых хранилищ, ведение реестра файловых хранилищ.

Описать ли документ «все в одном» или же разбить его на множество отдельных небольших документов — необходимо решать самостоятельно. Огромные документы тяжело читать и править, однако обилие малых документов также будет проблемой для освоения пользователями.

Глава 3. Информационная безопасность и защита информации при управлении доступом

Если не определен «санкционированный доступ», то всякий доступ в компании является несанкционированным.

Новостные источники с завидной регулярностью сообщают о новых видах мошенничества и утечках информации, которые злоумышленники опубликовали в сети. Списывая все на неких «злых хакеров», которые день и ночь сидят за черными экранами и ломают системы. Тем временем ситуация на деле оказывается совсем другой. В 80—85% случаев «взламывать» ничего вообще не нужно, либо это делать минимально, поскольку неосмотрительность и банальная глупость администраторов/владельцев систем ставят крест на защите информации, и информация просто выкачивается без особых проблем прямо с ресурса.

Если речь идет о веб-ресурсах, то в первую очередь злоумышленники используют системы и роботизацию для автоматического поиска таких вещей, как:

• Доступность консоли администрирования извне (банальный метод перебора паролей, включая стандартные, например, Login ADMIN Pass ADM1N часто дает плоды в виде доступа в систему с правами администратора).

• SQL-инъекции — дописывание кода в поле ввода на сайте для прямого запроса базы (при такой возможности можно получить данные, используя легальный механизм запроса к базе, ничего вообще не взламывая и не имея никаких прав, кроме пользователя на сайте/в системе).

• Файловая доступность на ресурсе и сохраненные бэкапы, пароли, история.

• Доступность на ресурсе доступа во внутреннюю сеть напрямую или через «реверс-прокси» (т. е. реверсивный авторизованный метод доступа).

• Доступные уязвимости оборудования (в том числе маршрутизатора), операционной системы или сервиса.

Если речь идет о ресурсах внутренней сети (например, если барьер демилитаризованной зоны DMZ уже прорван), то речь, как правило, идет о такой информации, как:

• О структуре сети и способах в ней закрепиться и легально работать (например, доступные Wi-Fi-сети или Ethernet без фильтров и паролей, пингование узлов, трассировки, таблицы маршрутизации для спуффинга).

• Передаваемая в открытом виде (без шифрования) информации (например, по HTTP или FTP трафик).

• Сохраненные логины-пароли в открытом виде, их передача в почте/мессенджерах (например, на рабочем столе, в блокнотах, в письмах, папках, кодах).

• Структура каталога LDAP на домен-контроллерах (например, простым запросом PowerShell GetUsers).

• Файловые ресурсы, в особенности «файловые помойки» (часто там можно найти вообще все что нужно, чтобы захватить домены, всю инфраструктуру и базы данных либо прямые выгрузки данных).

• Почта без шифрования (например, протокол SMTP отправляет без шифрования письма, и по нему же можно сформировать поддельное письмо на любой адрес в компании, чем ввести пользователя в заблуждение).

• Выгрузки из БД в Excel, отчеты и т. д. на рабочих столах пользователей или в общем доступе.

Разумеется, это лишь то, что приходит на ум среднего специалиста-злоумышленника сразу без дополнительной разведки и подготовки. Список далеко не исчерпывающий, однако показательный, что, даже не имея целей что-то взломать, используя легальные доступные инструменты пользователя или несокрытие отдельной информации, можно позволить злоумышленнику ее получить и либо совершить проникновение далее, либо и вовсе получить все и сразу.

Не все проблемы решаются только управлением доступом, поэтому сфера информационной безопасности включа-

ет в себя множество направлений, которые ставят цель замедлить злоумышленника, спровоцировать его изобличение и детектирование, блокировать до совершения преступления либо хотя бы получить материалы о том, как он действовал, если проникновение и преступление совершено успешно. Однако управление доступом вместе с другими направлениями дает возможность сильно ограничить возможности потенциального или реального нарушителя.

Основные принципы информационной безопасности, гласящие о минимизации полномочий, сложных паролях и недопустимости их разглашения, политики чистого рабочего стола, актуальны всегда, но при управлении доступом они дополняются:

- Идентификацией каждого лица, скрывающегося за учетными записями и принадлежности к ним.
- Аутентификацией пользователя системы.
- Минимизацией сетевых доступов и протоколов.
- Проработкой наличия на ресурсе защищаемой информации и доступа к ней через отдельные роли или шифрование ее / недоступность выгрузки.
- Структуризацией наборов и порядка ролей и доступа.
- Структуризацией методов мониторинга и организации защиты с помощью систем предотвращения вторжений, межсетевого экранирования и фильтрации.
- Единым подходом к получению и прекращению доступа,

который можно автоматизировать и поставить на поток, при этом контролировать и периодически проверять.

Добавим к этому аспекты мониторинга событий информационной безопасности, антивирусной защиты, контроля и устранения уязвимостей, политики смены паролей, контроля установки/запуска разрешенного программного обеспечения, настроенную систему предотвращения вторжений и межсетевого экрана, открытого только для узких согласованных доступов — и злоумышленник обнаружит себя раньше, чем вообще что-то успеет сделать, и даже если успешно сможет появиться в сети, то будет заблокирован.

Суть описания дальнейших методов как раз в том, чтобы обеспечить механизм, при котором доступ может быть быстро предоставлен пользователю, был бы минимально ему необходимый, достаточно описанный, чтобы разобраться и предоставить по запросу, и также быть быстро отозван при выявлении проблем или подозрений у сотрудников ИБ в том числе.

Глава 4. Из чего строится доступ и его потребители

«Мне доступ как у дяди Васи! И побыстрее! Для исполнения служебных обязанностей».

«Доступ как дом, его тоже можно построить по кирпичикам!»

Определившись с защищаемой информацией, ресурсами, системами и сетью, а также потребностью управлять доступом, необходимо перейти к пользователям. Но прежде надо понять — кто такие «Пользователи»? И что нужно для их работы?

Итак, пользователи могут быть **внутренними сотрудниками компании, внешними потребителями, а также такими категориями, как партнеры и внештатные работники**.

Каждой категории пользователей может быть доступно одно и запрещено другое. Именно с этими правилами необходимо определиться сразу, а также с процессами, связанными с приемом таких работников и подключения их к системам, согласованию, а также недопустимым действиям и отзыву прав.

Давайте последовательно разберемся, из чего строится

доступ. Для этого мы возьмемся за формирование РОЛЕЙ в системах, включающих в себя как полномочия на конкретном «железе» (серверах, сетях, сервисах и т. д.), так и создадим сущности пользователей, позволяющие даже при плоской структуре компании получать доступы в соответствии с целями.

Ранее мы уже определились с процессом управления доступом в рамках Политики, однако формирование ролевых моделей и матриц — процесс более живой и органичный, поэтому его стоит вывести в отдельный документ (Порядок или Регламент), чтобы не переутверждать всю политику каждый раз при его дополнении.

В рамках такого документа мы формируем набор операций по определению матричных моделей (проще говоря, наборов таблиц с указанием всех необходимых составных частей доступа), а также форм таких моделей, методики их заполнения и правил, по которым роли в матрицах создаются и при этом не противоречат друг другу.

Пример такого порядка можно найти в Приложении 2. Особо рекомендуется его разработка и использование при внедрении систем автоматизации, таких как IDM.

Принцип построения доступов всегда строится от малого к большому. Для этого нужно хорошо пониматься, из каких частей он состоит, как группируется, а также что необходимо для функционирования, кто и как это выдает, кто его должен получать и что нужно, чтобы у потребителя все заработало.

Метод базируется на **3 базовых составных частях**:

- **Системные роли (или ИТ-роли, или Атомарные)**
- **Бизнес-роли (или Комбинированные)**
- **Профили пользователей (Комбинированные наборы ролей разных систем под единым признаком пользователя)**

Вложенность ролей друг в друга является одной из основных черт данного метода, что позволяет неограниченно расширять и при этом жестко контролировать наборы полномочий пользователей и доступы к ресурсам.

Ниже приведена схема идеального распределения ролей и доступов (Схема 3).

Конец ознакомительного фрагмента.