МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»
Кафедра защиты информации

Факультет КСИС
Специальность ИиТП

Контрольная работа №1
по дисциплине «Основы защиты информации»

Выполнил студент: Драгун О.В.
группа 893551
Зачетная книжка № 2520050

Руководитель: Некрашевич Ирина Геннадьевна

Минск 2021

Оглавление

Введение

Цель и задачи исследования – вводное ознакомление и описание ключевых концепций ИБ, краткое описание современных комплексов по защите от случайных угроз, а также разработка и описание возможной политики ИБ некой организации.

Исследование получилось достаточно актуальным, претендующим на теоретическое ознакомление с угрозами и возможной политикой организации по защите от оных. По степени разработанности скорее поверхностный обзор ввиду ширины тем. Основным источником является сеть интернет

Угрозы информационной безопасности. Основные цели информационной безопасности

Классификация угроз безопасности по виду, происхождению, источникам и характеру возникновения. Примеры

Упрощенная классификация угроз выглядит следующим образом:

1. По свойству, против которого они направлены:
    a. физической и логической целостности, уничтожение или искажение информации (вирус-шифровальщик; вирус, дающий чрезмерное напряжение в плату; физическое воздействие на хранилище);
    b. конфиденциальности информации (раскрытие, передача третьим лицам, конкурентам);
    c. доступности, работоспособности (ddos-атака, блокировка на узлах);
    d. праву собственности.
2. По происхождению:
    a. случайные (отказы, сбои, ошибки, стихийные явления);
    b. преднамеренные (злоумышленные действия людей).
3. По Источникам:
    a. люди (персонал, посторонние);
    b. технические устройства;
    c. модели, алгоритмы, программы;
    d. внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).
4. По характеру
    a. естественные (стихийные бедствия; пожары; техногенные аварии)
    b. искусственные (- несанкционированный доступ к информации; перехват информации; хакерские атаки и т.д.)

Допустим существует практика ежемесячного сброса пароля, которая происходит автоматически. И некий сотрудник, чтобы не запоминать его, ежемесячно меняет его на один и тот же. В дополнение к этому с ним же регистрируется на сторонних ресурсах. С одного из ресурсов происходит утечка пар email-пароль. И злоумышленники получают доступ к внутренним ресурсам компании. Тогда реализовавшаяся утечка информации классифицируется так:

1. по свойству угроза конфиденциальности
2. по происхождению преднамеренная
3. по источникам человеческая
4. по характеру искуственная. С оговоркой, что если взять небрежность сотрудника и допустимость одинакового пароля за константу, то

подобная угроза когда-нибудь точно должна была произойти. То есть в некоторой степени по характеру – естественная.

Обеспечение доступности, конфиденциальности и целостности информации.

Доступность

Что же есть доступность?
Можно сказать, что информация должна быть доступна авторизованным лицам, когда это необходимо. Основными факторами, влияющими на доступность информационных систем, являются DoS-атаки, атаки программ-вымогателей, саботаж. Кроме того, источником угроз доступности являются непреднамеренные человеческие ошибки по оплошности или из-за недостаточной профессиональной подготовки: случайное удаление файлов или записей в базах данных, ошибочные настройки систем; отказ в обслуживании в результате превышения допустимой мощности или недостатка ресурсов оборудования, либо аварий сетей связи; неудачно проведённое обновление аппаратного или программного обеспечения; отключение систем из-за аварий энергоснабжения. Существенную роль в нарушении доступности играют также природные катастрофы, перечисленные ранее.
Во всех случаях конечный пользователь теряет доступ к информации, необходимой для его деятельности, возникает вынужденный простой. Критичность системы для пользователя и её важность для выживания организации в целом определяют степень воздействия времени простоя. Недостаточные меры безопасности увеличивают риск поражения вредоносными программами, уничтожения данных, проникновения из-вне или DoS-атак. Подобные инциденты могут сделать системы недоступными для обычных пользователей

Как обеспечить доступность информации?
Для обеспечения доступности информации в информационной системе необходимо использовать отказоустойчивые технические средства, выполнять резервирование технических средств, программного обеспечения и каналов передачи данных, а также резервное копирование критически важной информации. Также стоит упомянуть системы бесперебойного питания, резервирование и дублирование мощностей, планы непрерывности бизнес-процессов.

Конфиденциальность

Её можно определить как свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Конфиденциальность информации достигается предоставлением к ней доступа с наименьшими привилегиями исходя из принципа минимальной необходимой осведомлённости. Иными словами, авторизованное лицо должно иметь доступ

только к той информации, которая ему необходима для исполнения своих должностных обязанностей. Преступления против неприкосновенности частной жизни, такие, как кража личности, являются нарушениями конфиденциальности. Одной из важнейших мер обеспечения конфиденциальности является классификация информации, которая позволяет отнести её к строго конфиденциальной, или предназначенной для публичного, либо внутреннего пользования. Шифрование информации — характерный пример одного из средств обеспечения конфиденциальности

Целостность

Чёткое осуществление операций или принятие верных решений в организации возможно лишь на основе достоверных данных, хранящихся в файлах, базах данных или системах, либо транслируемых по компьютерным сетям. Иными словами, информация должна быть защищена от намеренного, несанкционированного или случайного изменения по сравнению с исходным состоянием, а также от каких-либо искажений в процессе хранения, передачи или обработки. Однако её целостности угрожают компьютерные вирусы и логические бомбы, ошибки программирования и вредоносные изменения программного кода, подмена данных, неавторизованный доступ, бэкдоры и тому подобное. Помимо преднамеренных действий, во многих случаях неавторизованные изменения важной информации возникают в результате технических сбоев или человеческих ошибок по оплошности или из-за недостаточной профессиональной подготовки. Например, к нарушению целостности ведут: случайное удаление файлов, ввод ошибочных значений, изменение настроек, выполнение некорректных команд, причём, как рядовыми пользователями, так и системными администраторами.

Для защиты целостности информации необходимо применение множества разнообразных мер контроля и управления изменениями информации и обрабатывающих её систем. Типичным примером таких мер является ограничение круга лиц с правами на изменения лишь теми, кому такой доступ необходим для выполнения служебных обязанностей. При этом следует соблюдать принцип разграничения полномочий[en], согласно которому изменения в данные или информационную систему вносит одно лицо, а подтверждает их или отклоняет — другое. Кроме того, любые изменения в ходе жизненного цикла информационных системы должны быть согласованны, протестированы на предмет обеспечения информационной целостности и внесены в систему только корректно сформированными транзакциями. Обновления программного обеспечения необходимо производить с соблюдением мер безопасности. Любые действия, влекущие изменения, должны быть обязательно протоколированы

Защита информации от случайных видов угроз.
Обучение сотрудников компании основным понятиям информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, исключить случайную установку потенциально опасного программного обеспечения на компьютер. Также в качестве меры предосторожности от потери информации следует делать резервные копии. Для того чтобы следить за деятельностью сотрудников на рабочих местах и иметь возможность обнаружить злоумышленника, следует использовать DLP-системы.
Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий

Классификация защит:

защита от нежелательного контента (антивирус, антиспам, веб-фильтры, анти-шпионы);
С точки зрения пользователя на рабочей машине должны быть предустановлено вышеуказанное ПО. С доступом или без него к правам администратора и возможностью/невозможностью удаления такого ПО в зависимости от квалификации специалиста.

сетевые экраны и системы обнаружения вторжений (IPS/IDS);
Отличия IPS и IDS систем
IPS — Intrusion Prevention System, а IDS — Intrusion Detection System. Это означает, что системы IPS отвечают за предупреждение и устранение атак, а IDS — за их обнаружение.
IDS не меняет сетевые пакеты и не предпринимает самостоятельных действий. А IPS наоборот предотвращает доставку пакета с подозрительным содержимым. Эта система запрещает сетевой трафик при обнаружении угроз. В IDS системе человек или другая система анализирует результаты мониторинга и определяет дальнейшие действия. Также, IPS имеет возможность менять содержание атаки и удалять инфицированный компонент. IPS, в каком-то смысле, расширение технологии IDS и обладает дополнительными возможностями для предотвращения атак при их выявлении. Каждая IPS содержит модуль IDS.

Таким образом, главное отличие IPS от IDS системы в том, что IPS — это система управления, а IDS — система мониторинга.

Что выбрать?
Выбор системы с точки зрения компании зависит от:

требуемого уровня защиты сети;
сферы деятельности компании;

подготовки специалистов;
бюджета организации.
Первое, на что стоит обратить внимание — масштаб систем: работает только с конкретным хостом или трафиком всей сети. Второй момент — позиционирование продукта. IPS и IDS могут быть как отдельными системами, так и частью программного обеспечения или аппаратного устройства.

Стоит отметить, что IPS систему необходимо регулярно настраивать под организацию и сеть, чтобы избежать сбоев и ложных срабатываний. Иначе, можно пропустить атаки и повредить сервисы компании. В случае с IDS системой, важным фактором будет удобство интерфейса для специалиста, который будет использовать систему. При использовании IDS нужно учитывать, что они с трудом работают в сетях с большим трафиком. 50 тысяч пакетов в секунду в 100 Мбит сети — это предел данной системы.

Наиболее эффективным способом защиты корпоративных сетей будет совместное применение IPS и IDS систем. Это UTM-системы (Unified Threat Management). Они являются комбинацией технологий IPS и IDS и предоставляют полный набор функций в одном устройстве. Таким образом, сокращая расходы на ресурсы. Важно обратить внимание на надежность системы от отказов.

Traffic Inspector Next Generation объединила в себе IDS/IPS технологии.

управление учетными данными (IDM) или Identity management;
комплекс подходов, практик, технологий и специальных программных средств для управления учётными данными пользователей, системами контроля и управления доступом (СКУД), с целью повышения безопасности и производительности информационных систем при одновременном снижении затрат, оптимизации времени простоя и сокращения количества повторяющихся задач.

контроль привилегированных пользователей (PAM);
Контроль действий привилегированных пользователей достигается за счёт идентификации сессий, требующих расширенного набора прав, и авторизации их инициаторов через специальный защищённый шлюз. В дальнейшем PAM-решение регистрирует все действия привилегированных клиентов, а также анализирует их поведение по ряду параметров. Сейчас для реализации этой функции всё чаще применяют искусственный интеллект и методы машинного обучения. В случае некорректных действий со стороны привилегированной учётной записи система может отправить уведомление ответственному лицу, ограничить набор прав или полностью разорвать соединение.

Ещё несколько лет назад большинство PAM-продуктов представляло собой одну из подсистем комплексных решений для управления процессом идентификации пользователей — Identity and Access Management (IAM). Такой идеологии до сих пор придерживаются многие крупные игроки, старающиеся закрыть максимум потребностей потенциальных клиентов. Например, у One Identity есть отдельное PAM-решение с возможностью интеграции между IDM и PAM. В результате на выходе клиенты могут получить «комбайн» PAG (Privileged Access Governance).

Но наблюдается и обратный процесс — продукты, ранее сфокусированные на решении относительно узкой задачи контроля привилегированных пользователей, приобретают всё больше функций, ранее им несвойственных. Помимо мониторинга сессий многие PAM-системы обеспечивают защищённое хранение паролей и криптоключей, интеграцию с SIEM-продуктами, фильтрами безопасности и CRM-системами. Некоторые разработки способны выступать в качестве надстройки для других решений, обеспечивая двухфакторную аутентификацию и управление DevOps-средами.

защита от DoS;

Полностью защититься от DDoS-атак на сегодняшний день невозможно, так как совершенно надёжных систем не существует. Здесь также большую роль играет человеческий фактор, потому что любая ошибка системного администратора, неправильно настроившего маршрутизатор, может привести к весьма плачевным последствиям. Однако, несмотря на всё это, на настоящий момент существует масса как аппаратно-программных средств защиты, так и организационных методов противостояния.

Меры противодействия DDoS-атакам можно разделить на пассивные и активные, а также на превентивные и реакционные. Ниже приведён краткий перечень основных методов.

Предотвращение. Профилактика причин, побуждающих тех или иных лиц организовывать и предпринять DDoS-атаки. (Очень часто кибератаки вообще являются следствиями личных обид, политических, религиозных и иных разногласий, провоцирующего поведения жертвы и т. п.). Нужно вовремя устранить причины DDoS-атак, после этого сделать выводы, чтобы избежать таких атак в будущем.

Ответные меры. Применяя технические и правовые меры, нужно как можно активнее воздействовать на источник и организатора DDoS-атаки. В настоящее время даже существуют специальные фирмы, которые помогают найти не только человека, который провел атаку, но даже и самого организатора.

Программное обеспечение. На рынке современного программного и аппаратного обеспечения существует и такое, которое способно защитить малый и средний бизнес от слабых DDoS-атак. Эти средства обычно представляют собой небольшой сервер.

Фильтрация и блэкхолинг. Блокирование трафика, исходящего от атакующих машин. Эффективность этих методов снижается по мере приближения к объекту атаки и повышается по мере приближения к атакующей машине. В этом случае фильтрация может быть двух видов: использование межсетевых экранов и списков ACL. Использование межсетевых экранов блокирует конкретный поток трафика, но не позволяет отделить «хороший» трафик от «плохого». ACL списки фильтруют второстепенные протоколы и не затрагивают протоколы TCP. Это не замедляет скорость работы сервера, но бесполезно в том случае, если злоумышленник использует первостепенные запросы.

Обратный DDOS — перенаправление трафика, используемого для атаки, на атакующего. При достаточной мощности атакуемого сервера позволяет не только успешно отразить атаку, но и вывести из строя сервер атакующего.

Устранение уязвимостей. Не работает против флуд-атак, для которых «уязвимостью» является конечность тех или иных системных ресурсов. Данная мера нацелена на устранение ошибок в системах и службах.

Наращивание ресурсов. Абсолютной защиты, естественно, не дает, но является хорошим фоном для применения других видов защиты от DDoS-атак.

Рассредоточение. Построение распределённых и дублирование систем, которые не прекратят обслуживать пользователей, даже если некоторые их элементы станут недоступны из-за DoS-атаки.

Уклонение. Увод непосредственной цели атаки (доменного имени или IP-адреса) подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью атаки.

Активные ответные меры. Воздействие на источники, организатора или центр управления атакой, как техногенными, так и организационно-правовыми средствами.

Использование оборудования для отражения DDoS-атак. Например, DefensePro® (Radware), SecureSphere® (Imperva), Периметр (МФИ Софт), Arbor Peakflow®, Riorey, Impletec iCore и от других производителей. Устройства

развёртываются перед серверами и маршрутизаторами, фильтруя входящий трафик.

Приобретение сервиса по защите от DDoS-атак. Актуально в случае превышения флудом пропускной способности сетевого канала.

Также компания Google готова предоставлять свои ресурсы для отображения контента вашего сайта в том случае, если сайт находится под DDoS-атакой. На данный момент сервис Project Shield находится на стадии тестирования, но туда могут быть приняты сайты некоторых тематик. Цель проекта — защитить свободу слова.

защита веб-приложений (WAF);

Файрвол веб-приложений. совокупность мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение. WAF относятся к прикладному уровню модели OSI.

Веб-приложение может быть защищено силами разработчиков самого приложения без использования WAF. Это требует дополнительных расходов при разработке. Например, содержание отдела информационной безопасности. WAF вобрали в себя возможность защиты от всех известных информационных атак, что позволяет делегировать ему функцию защиты. Это позволяет разработчикам сосредоточиться на реализации бизнес-логики приложения, давая больше времени на закрытие уязвимостей

анализ исходного кода;

Проверка кода программного обеспечения, производимая с использованием методов статического и динамического анализа, осуществляется на этапе создания и перед вводом ПО в эксплуатацию. Данный анализ позволяет выявить критически опасные уязвимости, недекларированные возможности или ошибки, которые могут быть использованы как внутренними, так и внешними злоумышленниками с целью мошенничества, несанкционированного доступа к информации, с целью кражи данных и финансовых средств.

Зачастую отдается сторонним сервисам в угоду экономии, что само по себе является угрозой информационной безопасности.

антифрод;

Система, предназначенная для оценки финансовых и не финансовых событий (карточных транзакций, действий пользователя в ДБО, операций с баллами лояльности и проч.) на предмет подозрительности с точки зрения мошенничества и предлагающая рекомендации по их дальнейшей обработке. Как правило, сервис антифрода состоит из стандартных и уникальных правил, фильтров и списков, по которым и проверяется каждая транзакция.

С точки зрения юзера источник боли и страданий, особенно при нахождении за рубежом без достаточного кол-ва денег наличными. С точки зрения банков-уменьшение потерь от мошенничества.

защита от таргетированных атак;

Таргетированные атаки используются для вредоносного воздействия на инфраструктуру компаний и государственных структур. Перед атакой киберпреступники тщательно изучают средства защиты атакуемой организации. Нападению могут быть подвергнуты не только привычные информационные системы компании, но и автоматизированные средства управления технологическими процессами (АСУ ТП). Антивирусные продукты не в силах предотвратить целевую атаку, так как вредоносные программы в таких случаях разрабатываются специально под конкретную инфраструктуру — в том числе с учетом используемого защитного ПО.

Для предотвращения таргетированных (целевых) атак необходима комплексная защита на всех уровнях, как на аппаратно-программном, так и на организационном.

управление событиями безопасности (SIEM);

Обычно, SIEM-система разворачивается над защищаемой информационной системой и имеет архитектуру «источники данных» — «хранилище данных» — «сервер приложений». SIEM-решения представляют из себя интегрированные устройства (all-in-one) либо двух-трехкомпонентные комплексы. Распределенная архитектура чаще всего предполагает большую производительность и лучшие возможности по масштабированию, а также позволяет развернуть SIEM-решение в IT-инфраструктурах с несколькими площадками.

Агенты выполняют первоначальную обработку и фильтрацию, а также сбор событий безопасности.
Передача информации от источников данных может осуществляться несколькими способами:

- источник сам инициирует передачу событий (например, отправляет по syslog-протоколу);
- события с источника забираются пассивно.

Рассмотрим использование этих способов на практике.

С первым вариантом все достаточно просто: на источнике указывается IP-адрес устройства, осуществляющего сбор событий (коллектора), и события отправляются адресату.

Второй вариант включает агентный или безагентный сбор информации, причем в некоторых SIEM-системах для части источников доступны оба способа. Агентный способ предполагает использование специальной программы-агента, безагентный - настройки источника событий, такие как создание дополнительных учетных записей, разрешение удаленного доступа и/или использования дополнительных протоколов.
Собранная и отфильтрованная информация о событиях безопасности поступает в хранилище данных, где она хранится во внутреннем формате представления с целью последующего использования и анализа сервером приложений.
Сервер приложений реализует основные функции защиты информации. Он анализирует информацию, хранимую в репозитории, и преобразует ее для выработки предупреждений или управленческих решений по защите информации.

Исходя из этого, в SIEM-системе выделяются следующие уровни ее построения:

- сбор данных: осуществляется от источников различных типов, например, файловых серверов, межсетевых экранов, антивирусных программ
- управление данными: данные, хранящиеся в репозитории, выдаются по запросам моделей анализа данных
- анализ данных: результатом являются отчеты в предопределенной и произвольной форме, оперативная корреляция данных о событиях, а также выдаваемые предупреждения

системы обнаружения аномального поведения пользователей (UEBA);

User and Entity Behavior Analytics (UEBA, «поведенческий анализ пользователей и сущностей») — технология выявления киберугроз, основанная на анализе поведения пользователей, а также устройств, приложений и иных объектов в информационной системе.
Основная задача UEBA — своевременно обнаруживать целевые атаки и инсайдерские угрозы. Решения UEBA обрабатывают большой объем данных из различных источников, определяют нормальные модели поведения для каждого пользователя и объекта и уведомляют ИБ-специалистов, если замечают отклонения от этих моделей.

защита АСУ ТП;

Автоматизированная система управления (АСУ) технологическим процессом (ТП) - собирательный термин, имеющий отношение ко всему многообразию управляющих компьютерных устройств и их объединений, которые имеют целью обеспечить управление разнообразными процессами. Первоначально системы АСУ ТП развивались на производстве, однако сходство технологических процессов с процессами работы самых различных механизмов

позволяет часто причислять к АСУ ТП системы, использующиеся в управлении транспортом, оружием, инженерными системами зданий и др.

защита от утечек данных (DLP);

Под DLP-системами принято понимать программные продукты, защищающие организации от утечек конфиденциальной информации. Сама аббревиатура DLP расшифровывается как Data Leak Prevention, то есть, предотвращение утечек данных.

Подобного рода системы создают защищенный цифровой «периметр» вокруг организации, анализируя всю исходящую, а в ряде случаев и входящую информацию. Контролируемой информацией должен быть не только интернет-трафик, но и ряд других информационных потоков: документы, которые выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываемые на принтере, отправляемые на мобильные носители через Bluetooth и т.д.

шифрование;

Про него можно писать отдельную диссертацию. Самый простой пример – проверка md5 хешей при передачи файлов для проверки их целостности. Позволяет убедится, что отправитель и приемник работают с одной и той же версией.

защита мобильных устройств;

Google и Apple активно работают в этом направлении. Мне, как разработчику android с каждой новой версией операционной системы становится всё сложнее и сложнее получить доступ к телефону пользователя. С точки зрения компании запрещать телефоны у сотрудников бесполезно. Лучшее решение = просвещать их про недопустимость и опасность использования перепрошивок, рутов, jailbreak-ов. Про проверку разрешений у приложений, и недопустимость установок непонятных файлов из непонятных источников.

резервное копирование;

Как говорится «системные администраторы делятся на тех, кто еще не делает резервное копирование и на тех, кто уже делает резервное копирование» Бэкап и возможность отката к старой версии = золотое правило и стандарт не только в системном администрировании, но и в разработке ПО.

системы отказоустойчивости

Отказоустойчивость определяется количеством единичных отказов составных частей (элементов) системы, после наступления которых сохраняется работоспособность системы в целом. Базовый уровень отказоустойчивости подразумевает защиту от отказа одного любого элемента. Поэтому основной способ повышения отказоустойчивости это избыточность. Наиболее эффективно избыточность реализуется аппаратно, путём резервирования. В ряде областей техники отказоустойчивость путём резервирования является

обязательным требованием, предъявляемым государственными надзорными органами к техническим системам.

Для технических систем повышенной опасности частным случаем отказоустойчивости является отказобезопасность — способность системы при отказе некоторых её составных частей переходить в режим работы, не представляющий опасности для людей, окружающей среды или имущества. В реальных системах эти два свойства могут рассматриваться совместно.

Политика информационной безопасности

Назначение и цель политики ИБ.

Основной целью, на достижение которой направлены все положения Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ. Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям законодательства РБ и договорным обязательствам в части ИБ;
- обеспечение непрерывности критических бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- изучение партнёров, клиентов, конкурентов и кандидатов на работу;
- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
- повышение деловой репутации и корпоративной культуры.

Содержание, структура, этапы разработки политики ИБ.

Содержание и структура политики ИБ

Кратко опишем положения, которые могли бы содержаться в политике ИБ некой организации

1. Структура документов.
   Разбитие документов на иерархию вида

Где полная политика является внутренним документом первого уровня. Инструкции, регламенты, порядки – документы, описывающие действия сотрудников по реализации документов первого и второго уровня. Третий уровень – отчётные документы о выполнении требований документов верхних уровней

2. Ответственность за обеспечение ИБ.
   Описание работы отдела ИБ. Задачи, права и обязанности сотрудников
3. Объект защиты.
   Сюда можно включить ответственность за ресурсы, классификацию информации по степени важности
4. Оценка и обработка рисков.
   Регламентация периодичности оценки, для учета изменений бизнес-требований и приоритетов, принятия во внимание новых угроз и уязвимостей, проверки актуальности реализованных средств.
5. Безопасность персонала.
   Условия найма, ответственность руководства, обучение ИБ, завершение или изменение трудовых отношений.
6. Физическая безопасность.
   Защищенные области с доступом у минимально необходимого кол-ва сотрудников, области общего доступа, утилизация или повторное использование оборудования, перемещение имущества.
7. Контроль доступа.
   Учетные записи с различным уровнем доступа. Регистрация и блокирование учетных записей. Управление паролями. Контроль прав доступа. Использование паролей. Пользовательское оборудование, оставляемое без присмотра. Мобильное компьютерное оборудование
8. Политика допустимого использования информационных ресурсов.
   Общие обязанности пользователя, использование ПО, ресурсов

локальной сети, электронной почты, работа в сети, использование мобильных устройств, защита от вредоносного ПО, обработка конфиденциальной информации

9. Приобретение, разработка и обслуживание систем.
   Требования безопасности для информационных систем, обработка информации, криптографические средства, электронные цифровые подписи, управление ключами, безопасность системных файлов, безопасность процесса разработки и обслуживания систем.
10. Управление инцидентами ИБ.
    Формализация процедур ввиду происшествий в области ИБ
11. Управление непрерывностью и восстановлением.
    Разработка контролируемого процесса для обеспечения и поддержки непрерывности бизнес-процессов Учреждения. Планы по восстановлению операций/уровня доступности после сбоев. Четкие условия начала использования плана и ответственные сотрудники.
12. Соблюдение требований законодательства
    Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Учреждения к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.
13. Аудит информационной безопасности
    Внутренние проверки через запланированные интервалы времени. Цели и задачи такого аудита

Этапы разаработки политики ИБ

Если подойти к вопросу достаточно формально, то можно выделить 4 этапа разработки:

- Исследование текущего состояния информационной среды и информационной безопасности организации;
- Анализ полученных сведений по результатам исследования;
- Формирование плана работ по разработке политики информационной безопасности;
- Разработка политика информационной безопасности организации.

В результате 4 этапов должен получиться следующий пакт документов:

- Политика информационной безопасности организации - высокоуровневый документ, описывающий основные принципы и правила, направленные на защиту информационных ресурсов организации;

- Регламенты информационной безопасности, раскрывающие более подробно процедуры и методы обеспечения информационной безопасности в соответствии с основными принципами и правилами, описанными в политике;
- Инструкции по обеспечению информационной безопасности для должностных лиц организации с учетом требований политики и регламентов;
- Прочие документы, представляющие собой отчеты, регистрационные журналы и прочие низкоуровневые руководящие документы.

Конкретные проекты необходимых документов каждого типа определяются в ходе обследования существующего уровня информационной безопасности Заказчика, её организационной структуры и основных бизнес-процессов.

Заключение

Рассмотренный материал дает обзорное представление о некоторых угрозах ИБ и возможных программных средствах для их предотвращения. А также представление о политике информационной безопасности, с которой наверняка придется столкнуться практически любому специалисту в IT-сфере, и не только в ней.

Использованная литература

1. Основы защиты информации и управления интеллектуальной собственностью Л.М. Лыньков, В.Ф.Голиков,Т.В.Борботько, 2013
2. Информационная безопасность Wikipedia
3. https://www.anti-malware.ru/threats/information-security-threats
4. Что такое ids/ips-системы
5. Что такое PAM
6. Защита от DoS
7. Политика ИБ НЦОТ
8. Пример политики ИБ государственного бюджетного учреждения Ярославской области «Электронный регион»
9. Другие открытые источники интернет-сети