Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информатики и веб-дизайна

Разработка политики информационной

безопасности ЖЭС

Выполнил студент 2 курса 10 группы

Помоз Даниил Сергеевич

Минск 2022

# Введение

В XXI веке – веке информатизации, происходит формирование и развитие информационного общества. Роль информации в современном мире огромна. Информация становится ключевым ресурсом, поэтому без решения задач информационной безопасности не может продолжать работу ни одно из предприятий. В любой организации, как большой, так и маленькой, возникает проблема безопасного хранения, передачи, использования информации.

Обеспечение информационной безопасности автоматизированной системы управления технологическими процессами необходимо для повышения уровня устойчивости ее функционирования, стабильности исполнения реализуемых технологических процессов путем предотвращения и/или снижения возможного ущерба от несанкционированных воздействий на объекты защиты автоматизированной системы управления технологическими процессами.

Вместе с развитием информационных технологий, развиваются и технологии передачи информации. Объемы передаваемой и принимаемой информации увеличились в десятки раз за сравнительно небольшой промежуток времени. Огромное количество обрабатываемой и передаваемой информации повышают риск потери, искажения или кражи информации. Кроме того, увеличилось число возможных путей кражи информации злоумышленниками. Каждый день обнаруживаются все новые и новые уязвимости в информационных системах, которые постоянно исправляются, но некоторый промежуток времени информационные системы остаются уязвимыми для злоумышленников. Поэтому роль защиты информации на сегодняшний день значительно возросла и так же будет возрастать в дальнейшей перспективе.

Роль защиты информации велика в любой компании, но некоторые компании нуждаются в защите информации на высшем уровне. К таким компаниям относят те, сфера деятельности которых напрямую связана с информацией и те, для которых принципиально важна безопасность передачи информации. К первым можно отнести компании, работающие в сфере информационных технологий, ко вторым же – банки и различные компании, работающие в юридической и финансовых сферах.

Защищаемая информация имеет следующие признаки:

* имеются законные пользователи, которые имеют право владеть этой информацией;
* имеются незаконные пользователи, которые стремятся овладеть этой информацией с тем, чтобы обратить ее себе во благо, а законным пользователям во вред;
* со стороны незаконных пользователей существуют различные виды угроз для защищаемой информации: угроза разглашения информации, подмена информации, имитация информации и др.

Для обеспечения информационной безопасности создаются политики информационной безопасности. Политики информационной безопасности – это формальное изложение правил поведения лиц, получающих доступ к конфиденциальным данным в корпоративной информационной системе.

Целью данной работы является разработка политики безопасности для жилищно-эксплуатационной службы. Данная служба нуждается в разработке документов по обеспечению безопасности стандартов, процедур, регламентов должностных инструкций.

# Общие положения

Политика безопасности разрабатывается в соответствии с законодательством Республики Беларусь и нормами права в части обеспечения информационной безопасности. Политика безопасности является документом, доступным любому пользователю, и представляет собой официально принятую руководством систему взглядов на проблему обеспечения информационной безопасности.

Основным объектом защиты информации в данной компании является автоматизированная система управления технологическими процессами, под которой понимается система, состоящая из персонала и комплекса средств автоматизации его деятельности и формирующая управляющее воздействие на технологические процессы.

Актуальность и необходимость внедрения политик информационной безопасности для компаний объясняется необходимостью создания механизма управления и планирования информационной безопасности. Также политики информационной безопасности позволяют совершенствовать следующие направления деятельности компании:

* поддержка непрерывности работы службы;
* повышение уровня доверия к службе;
* минимизация рисков с помощью защиты своих интересов в информационной сфере;
* повышение качества деятельности по обеспечению информационной безопасности;
* снижение издержек.

Естественно, что совершенствование направлений деятельности организации зависит от грамотности составления политики безопасности.

В соответствии с определением политики информационной безопасности и рекомендациями международных стандартов в области планирования и управления политиками информационной безопасности, политики должны содержать:

* определение предмета задач и целей;
* условия применения и их ограничения;
* отражение позиции руководства в отношении выполнения политики информационной безопасности и создания комплексной системы информационной безопасности;
* определение прав и обязанностей сотрудников;
* определение границ ответственности сотрудников за выполнение политики информационной безопасности;
* порядок действий в случае нарушения политики безопасности.

Основные положения информационной безопасности и позиция руководства компании прописываются в концепции информационной безопасности. Концепция информационной безопасности реализуется в частных политиках информационной безопасности, процедурах, руководствах и стандартах, обеспечивающих детальную интерпретацию положения концепции информационной безопасности для сотрудников, партнёров и клиентов компании.

Таким образом политика информационной безопасности является неотъемлемой частью систем установления режима информационной безопасности и контроля за ним систем информационной безопасности и систем управления информационной безопасности соответственно.

# Структура предприятия

Для того чтобы разработать план по информационной безопасности ЖЭС нужно сначала понять, что из себя представляет ее структура информации. Информация представляется в бумажном и электронном виде.

Так как в ЖЭС хранится большая и важная документация, то доступ к информации имеется в зависимости от прав работника. Права работника назначаются в зависимости от должности.

Структура предприятия представляет собой:

* генеральный директор;
* главный бухгалтер;
* бухгалтерия;
* главный инженер;
* производственный отдел;
* отдел землеустройства и капитального ремонта дворовой территории;
* планово-экономический отдел;
* отдел по информационно-общественной деятельности;
* отдел кадров;

Необходимо введение разделения пользователей на группы с различным уровнем доступа к информации. Обычные пользователи могут только просматривать информацию, а привилегированные пользователи могут вносить какие-либо изменения. Так как важность документов очень велика, то доступ ко всей информации не может быть скопирован ни одним из уровней пользования. Такая же система работает как с электронными, так и с бумажными вариантами документации, которая хранится в архиве.

# Оценка рисков

В информационной безопасности методики оценки рисков появились с целью прогнозирования возможного ущерба, связанного с реализацией угроз, и соответственно оценки необходимого размера инвестиций на построение систем защиты информации.

Методики расчета делятся на количественные и качественные. Количественный расчет рисков в настоящее время нереализуем, это связано в первую очередь с отсутствием достаточного объема статистических данных о вероятности реализации той или иной угрозы. В результате наибольшее распространение получила качественная оценка информационных рисков.

До сих пор ведутся споры на тему оценки информационных рисков или экономического обоснования инвестиций в информационную безопасность. В настоящее время идет активное накопление данных, на основании которых можно было бы с приемлемой точностью определить вероятность реализации той или иной угрозы. К сожалению, имеющиеся справочники опираются на зарубежный опыт и потому с трудом применимы к нашим реалиям.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Под актуальными угрозами безопасности понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать их уничтожение, изменение, блокирование, копирование, предоставление, распространение и т.п.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

– по природе возникновения:

а) антропогенные;

б) техногенные;

в) естественные;

– по размерам наносимого ущерба:

а) общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);

б) локальные (причинение вреда отдельным частям объекта безопасности);

в) частные (причинение вреда отдельным свойствам элементов объекта безопасности);

– по аспекту информационной безопасности, на который направлены угрозы:

а) угрозы конфиденциальности (неправомерный доступ к информации);

б) угрозы целостности (неправомерное изменение данных);

в) угрозыдоступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы);

– по расположению источника угроз:

а) внутренние (источники угроз располагаются внутри системы);

б) внешние (источники угроз находятся вне системы);

– по степени преднамеренности действий:

а) случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия);

б) преднамеренные (умышленные действия, например, шпионаж и диверсии);

– по степени воздействия на информационную систему:

а) пассивные (структура и содержание системы не изменяются);

б) активные (структура и содержание системы подвергается изменениям).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей. преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Главпочтамта могут быть как внешними, так и внутренними.

На основании оценивания рисков выбираются средства, обеспечивающие режим информационной безопасности. Ресурсы, значимые для нормальной работы организации и имеющие определенную степень уязвимости, считаются подверженными риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

Основными источниками внутренних и внешних угроз являются:

* сотрудники (бывшие и нынешние);
* бизнес-партнеры и люди, имеющие доступ к внутренней информации;
* программное обеспечение;
* аппаратные средства.

Основными угрозами информационной безопасности автоматизированной системы управления технологическими процессами являются:

– несанкционированное вмешательство в управление технологическими процессами;

–нарушение функционирования автоматизированная система управления технологическими процессами или ее отдельных элементов;

– несанкционированный доступ к информации, хранимой в базах данных автоматизированная система управления технологическими процессами и передаваемой по каналам передачи данных.

В результате реализации угроз информационная безопасность могут быть нарушены:

– целостность (утрата, уничтожение, модификация) информации;

– доступность (блокирование) информации и отдельных элементов автоматизированная система управления технологическими процессами;

– конфиденциальность (утечка, перехват, съем, копирование, хищение, разглашение) информации.

Обеспечение информационной безопасности автоматизированной системы управления технологическими процессами осуществляется по следующим направлениям, реализуемым организационно-техническими мерами защиты.

Физическая защита, включая:

– защиту технических средств обработки, хранения и передачи информации;

– защиту зданий, сооружений и помещений.

Обеспечение информационная безопасность при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов, включая:

– защиту от вредоносного программного обеспечения;

– резервирование серверов, сетевого оборудования, средств защиты и каналов передачи данных;

– обеспечение безопасности сетевой инфраструктуры;

– защиту программного обеспечения;

– регистрацию и учет событий информационная безопасность;

– организацию безопасного использования, преобразования, хранения и передачи информации;

– криптографическую защиту.

Контроль доступа, в том числе:

– управление доступом пользователей;

– определение ответственности пользователей;

– контроль доступа к прикладным системам;

– контроль доступа к операционным системам;

– контроль сетевого доступа;

– обеспечение безопасности при использовании мобильных устройств;

– обеспечение безопасности в беспроводных сетях;

– контроль доступа к сетевому оборудованию.

Реализация организационно-технических мер обеспечения информационная безопасность автоматизированная система управления технологическими процессами достигается в первую очередь путем:

– корректного использования и администрирования встроенных механизмов безопасности технических средств обработки, хранения и передачи информации и средств защиты, входящих в состав автоматизированная система управления технологическими процессами;

– наделения пользователей автоматизированной системы управления технологическими процессами правами доступа и привилегиями по работе в автоматизированная система управления технологическими процессами;

– физической защиты технических средств обработки, хранения и передачи информации от неправомерного доступа к ним;

– контроля функционирования и настроек механизмов безопасности, а также соблюдения требований по информационной безопасности.

Обязанности пользователей автоматизированной системы управления технологическими процессами по обеспечению информационной безопасности зависят от занимаемой должности и определены в их должностных инструкциях.

# Разработка мер защиты

Защита технических средств обработки, хранения и передачи информации

В целях защиты информации от несанкционированного доступа и ее утечки, предотвращения хищения технических средств обработки и хранения информации и несанкционированного управления ими, а также простоев в функционировании автоматизированной системы управления технологическими процессами обеспечивается физическая защита входящих в нее технических средств. Серверное оборудование и критичное сетевое оборудование размещаются в запираемых шкафах с сигнализацией, располагаемых в специализированных помещениях (серверных), ограничивающих доступ к ним посторонних лиц. Перед утилизацией или передачей в ремонт технических средств выполняется гарантированное удаление информации с них. Кабельные сети прокладываются так, чтобы максимально ограничить несанкционированный доступ к ним. Для защиты от перебоев электричества в эксплуатацию вводятся централизованные системы бесперебойного питания. Система информационная безопасность включает в себя максимальное количество элементов, обеспечивающих эффективную защиту системы при критической нагрузке.

### Защита зданий, сооружений и помещений

В целях обеспечения безопасности технических средств автоматизированной системы управления технологическими процессами осуществляется защита зданий, сооружений и помещений автоматизированная система управления технологическими процессами. Здания и сооружения, в которых размещаются технические средства автоматизированная система управления технологическими процессами, обеспечиваются инженерно-техническими средствами охраны и средствами защиты от противоправных действий. Помещения, в которых размещаются критически важные технические средства автоматизированная система управления технологическими процессами, оборудуются средствами пожарной безопасности, вентиляции и кондиционирования. Доступ в такие помещения разрешается работникам только для выполнения должностных обязанностей по обслуживанию технических средств автоматизированная система управления технологическими процессами. Доступ в помещения ограничивается средствами контроля и управления доступом. При выполнении работ в помещениях, где размещаются критически важные технические средства автоматизированной системы управления технологическими процессами, лицами, чья деятельность не связана непосредственно с их обслуживанием, обеспечивается контроль их деятельности.

### Организация безопасной эксплуатации средств обработки, хранения и передачи информации

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных для этого работников. Изменения конфигурации средств обработки и хранения информации, а также изменения сетевой инфраструктуры, конфигурации сетевого оборудования выполняются администратором. Все изменения регистрируются в соответствующих журналах. Самостоятельное изменение конфигурации средств обработки, хранения и передачи информации пользователями автоматизированная система управления технологическими процессами запрещено. Использование съемных носителей информации в автоматизированной системе управления технологическими процессами запрещено. При размещении средств разработки, тестирования и эксплуатации обеспечивается их физическое или логическое разделение в целях снижения риска несанкционированного доступа или внесения изменений в систему.

### Защита от вредоносного программного обеспечения

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного программное обеспечение в автоматизированная система управления технологическими процессами применяются средства защиты от вредоносного программного обеспечения. Средства защиты от вредоносного программного обеспечения устанавливаются на серверном оборудовании и автоматизированное рабочее место операторов и специалистов автоматизированной системы управления технологическими процессами. Управление и обновление средств защиты от вредоносного программного обеспечения осуществляются централизованно. Разрешается использование только сертифицированных на соответствие требованиям безопасности информации средств защиты от вредоносного программного обеспечения. Администрирование средств защиты от вредоносного программного обеспечения осуществляется системным администратором. Настройки системы защиты от вредоносного программного обеспечения согласовываются и контролируются администратором информационная безопасность.

Используемая антивирусная система защиты имеет:

– стойкую систему самозащиты, которая не по­зволит неизвестной вредоносной программе нарушить нормальную работу автоматизированная система управления технологическими процессами и сделает возможным функционирование антивирусная система защиты до поступления обновления;

– систему обновлений, находящуюся под контролем системы самозащиты антивирусной системы и не использующую компоненты операционной системы, которые могут быть скомпрометированы;

– систе­му обновления, позволяющую мгновенно, по сигна­лу системы централизованного управления доставить на защищаемый антивирусом объект обновления для устранения активного заражения;

– дополнительные механизмы для обнаружения новых неизвестных вредоносных программ;

– проверяет все поступающие из локальной сети файлы до момента получения их используемыми приложениями, что исключает использование вредоносными приложениями неизвестных уязвимостей данных приложений;

– систему централизованного сбора информации с удаленных рабочих станций и серверов, позволяющую максимально быстро передавать в антиви­русную лабораторию всю необходимую для решения проблемы информацию.

### Обеспечение безопасности сетевой инфраструктуры

Для обеспечения непрерывного и устойчивого функционирования автоматизированная система управления технологическими процессами осуществляется защита ее сетевой инфраструктуры. Защита сетевой инфраструктуры обеспечивается:

– контролем логического доступа к сетевому оборудованию;

– контролем сетевых соединений;

– шифрованием каналов управления;

– защитой информации ограниченного доступа при ее передаче вне контролируемых зон;

– физической защитой сетевого оборудования и средств защиты;

– мониторингом подключаемых к локальная вычислительная сеть автоматизированной системы управления технологическими процессами сетевых устройств;

– обнаружением и предотвращением вторжений;

– использованием встроенных в сетевое оборудование средств защиты от подмены адреса (средств антиспуфинга);

– применением средств мониторинга и регистрации событий.

Контроль сетевых соединений между локальная вычислительная сеть автоматизированная система управления технологическими процессами и подключаемыми к ней беспроводными сетями также осуществляется средствами межсетевого экранирования. Защита информации ограниченного доступа при ее передаче вне контролируемых зон осуществляется применением сертифицированных средств криптографической защиты информации (построением защищенных виртуальных сетей). Защита от вторжений в локальная вычислительная сеть автоматизированная система управления технологическими процессами осуществляется средствами обнаружения и предотвращения вторжений, размещаемыми на входе в локальная вычислительная сеть. Базы данных сигнатур средств обнаружения и предотвращения вторжений регулярно обновляются с сайта производителя применяемых средств. Категорически запрещается удаленное администрирование автоматизированная система управления технологическими процессами.

В целях поддержания работоспособности программное обеспечение осуществляются меры по устранению уязвимостей программное обеспечение, а также другие меры защиты от:

– умышленного либо неумышленного раскрытия, модификации или уничтожения защищаемых данных. В частности, это подразумевает использования средств ограничения доступа к различным ресурсам офисного контроля;

– установки средств защиты кем-либо, кроме администратора, несанкционированного внесения изменений в порядок функционирования системы защиты, изменения ее возможностей. Данное требование приводит к необходимости разграничения прав доступа к настройкам системы, защите ее от несанкци­онированного воздействия. Это подразумевает использование в локальной сети только программных продуктов, поддерживающих ролевой принцип доступа, а также применение функций офисного контроля. Средства защиты должны устанавливаться как на рабочие станции, так и на сервер. В организации, соответствующей требованиям стандарта, должна использо­ваться только защищенная почта, что вместе с требованием о наличии защиты от вирусов и спама подразумевает установку средств антивирусной фильтрации почтовых сообщений. В свою очередь доступ в сеть Интернет должен использоваться только для обеспе­чения банковской деятельности. Устранение уязвимостей программное обеспечение достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками программное обеспечение. Обновление операционная система, другого общесистемного и прикладного программное обеспечение осуществляется системными администраторами и администраторами прикладных систем. Обновления для программное обеспечение автоматизированная система управления технологическими процессами получаются с серверов обновлений, размещенных в информационно-управляющей системе.

## Контроль доступа

### Управление доступом пользователей

В целях устойчивого функционирования автоматизированной системы управления технологическими процессами и обеспечения безопасности информационных ресурсов осуществляется управление доступом пользователей к операционным и прикладным системам, а также сетевому оборудованию. Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на установленной в ЖЭС формализованной процедуре предоставления прав доступа. Права доступа и привилегии пользователей подлежат регулярному пересмотру. Каждый пользователь обеспечивается уникальным персональным идентификатором. Подтверждение подлинности идентификатора (аутентификация) пользователя осуществляется при помощи паролей и/или средств усиленной аутентификации. Длина, сложность и срок действия паролей устанавливаются в зависимости от степени критичности защищаемых систем.

# Заключение

Политика безопасности — совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На политике безопасности нельзя экономить, так как данные, которые могут быть подвержены хищению, копированию или изменению, могут стоить дороже, чем ресурсы, потраченные на ее разработку и осуществление.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность и общие меры предосторожностей.

Политика безопасности должна быть разработана таким образом, чтобы ее несанкционированный доступ к информации стоил дороже, чем сама информация.

Необходимо иметь в виду, что многие меры защиты требуют достаточно больших вычислительных ресурсов, что в свою очередь существенно влияет на процесс обработки информации.