Riigi Infosüsteemi Amet

ID-карта

CERT-EE

Digi Doc

eID

eesti.ee

X-tee

ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ ИНФОСИСТЕМЫ

Ежегодник 2020

RIHA

Э-голосование

ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ ИНФОСИСТЕМЫ
Ежегодник 2020

Издатель: **Департамент государственной инфосистемы,**
Пярну мнт., 139a, 11317, Таллинн

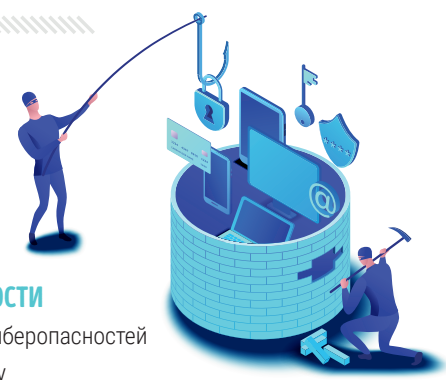
Оформление: **Мартин Милейко** (Profimeedia OÜ)
Иллюстрации: **Линда Вайномяэ** (Profimeedia OÜ)
Фотографии: **Нелли Пелло, Рене Рийсалу, Марек Метслайд**
Ecoprint

Содержание

ВВЕДЕНИЕ

ГОСУДАРСТВЕННЫЕ ИНФОСИСТЕМЫ

КИБЕРБЕЗОПАСНОСТЬ



МЕЖДУНАРОДНЫЕ КОММУНИКАЦИИ

КОЛЛЕКТИВ

Мы вместе формируем лучшее в мире ЦИФРОВОЕ ОБЩЕСТВО

МАРГУС НООРМАА
Генеральный директор Департамента государственной инфосистемы

В 2019 году в Департаменте государственной инфосистемы произошло множество изменений. По существу, наше учреждение получило новое правление, поскольку сменилась большая часть руководящего состава. Новые люди означают новые идеи, новое дыхание и новые направления, с помощью которых э-государству можно добавить размаха.

Мы видим, что цифровой и реальный мир между собой настолько тесно связаны, что их больше невозможно рассматривать по отдельности, и жители Эстонии понимают это все больше. Э-услуги в повседневной жизни становятся все важнее, и теперь уже часовое прерывание в работе э-услуг существенно нарушает жизнь людей.

В среде электронных услуг действуют также и киберпреступники, которые становятся всё более изощрёнными и находят новые способы, как использовать людей, не предчувствующих плохое. Таким образом, следует прилагать еще больше усилий, чтобы наши услуги работали при любой погоде и в любой ситуации. В то же время нельзя забывать о просвещении людей. Опасности цифрового мира изменяются, и все больше попадают под прицел также наши жители и предприятия. Задача государства – заблаговременно обнаруживать и сводить к минимуму опасности.

Всё важнее становится международное сотрудничество, поскольку киберпреступность не знает государственных границ. По оценке рапорта по безопасности Всемирного экономического форума 2020 года, из десяти основных рисков, с которыми сталкивается мир, три исходят из технологии и нашей неспособности ее защитить в достаточной мере.

Помимо этого, обычные люди также чувствуют всё больше опасностей виртуального мира и желают, чтобы государство помогло им справиться с ними. Таким образом, следует еще больше вкладывать в улучшение кибербезопасности, поскольку интернет и киберпреступники пришли, чтобы остаться. Цифровое государство держится в основном на доверии, и роль государства – создавать это доверие.

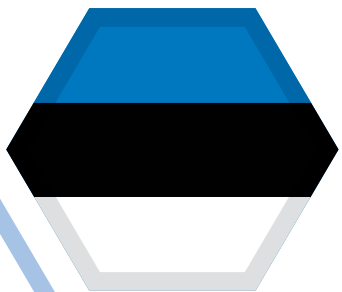
Безопасные решения требуют денег и инвестиций. Многие годы при разработке основных компонентов э-государства и других важных систем мы зависели от зарубежных дотаций, но это не стабильный источник финансирования. Мы работаем во имя того, чтобы сделать финансирование надежнее и стабильнее.

Помимо общего видения и денег нужны также компетентные и работящие люди. В действительности люди как раз и являются основным фактором достижения успеха. RIA желает быть достаточно привлекательным и достойным работодателем, чтобы самые светлые головы государства хотели бы здесь работать и создавать нечто по-настоящему грандиозное.

Работая во имя общей цели, как раз и рождаются результаты. Эстонское цифровое государство также было построено в тесном сотрудничестве публичного и частного сектора. В Департаменте государственной инфосистемы мы работаем единой командой, чтобы создавать и защищать лучшее в мире цифровое общество. Да, деньги заставляют колеса вращаться, но без компетентных людей от денег нет пользы. У нас хорошие люди, которые думают, как улучшить уже существующие системы, услуги и решения. В то же время мы работаем над новейшими системами, чтобы упростить жизнь цифровых граждан и упразднить излишнюю бюрократию.

Через увлекательные тернии к звездам!

ФАКТЫ ОБ ЭСТОНСКОМ Э-ГОСУДАРСТВЕ



Есть, что защищать и развивать.

1 354 000+
активных ID-карт

501 000+
пользователей Smart-ID

234 000+
учетных записей Mobiil-ID

20 МЛН
операций в месяц совершается через ID-карту

91,6%
жителей регулярно пользуется интернетом

87%
домохозяйств имеют компьютер

99,6%
банковских операций совершается в электронном виде

98%
подает налоговую декларацию в электронном виде

99%
рецептов электронные

3000+
э-услуг доступны через X-tee

66 000+
э-резидентов

5000+
э-услуг, где можно идентифицировать себя через ID-карту

46,8%
избирателей отдает свой голос в электронном виде

10 000+
предприятий принадлежит э-резидентам

КАК МЫ ЭТОГО

RIA сформировался в результате реорганизации и объединения нескольких учреждений. Фонд информатики Эстонии, сформированный в 1990 году в сфере управления Государственной канцелярии, с годами стал правительственным учреждением под ведомством Министерства экономики и коммуникаций со штатом сотрудников около 150 человек.

Руководители RIA

Маргус Ноормаа, генеральный директор с 22 апреля 2019 г. по …
Таймар Петеркоп, генеральный директор с 4 мая 2015 г. по 9 декабря 2018 г.
Яан Прийсалу, генеральный директор с 1 июня 2011 г. по 16 января 2015 г.
Эпп Йоаб, директор Центра развития государственных инфосистем с 26 мая 2003 г. по 31 мая 2011 г.

РУКОВОДИТЕЛИ ПРЕДШЕСТВУЮЩИХ ОРГАНИЗАЦИЙ

Имре Сийль, директор Эстонского центра информатики с 1997 г. по 2003 г.
Вяйно Сарнет, директор Центра государственных закупок с 15 ноября 2001 г. по 2 сентября 2002 г.
Устус Агур, исполнительный директор Эстонского фонда информатики с 1991 г. по 1 января 1997 г.

В ноябре 1989 года был сформирован Совет информатики Эстонии. В декабре 1990 года начал работу в сфере управления Государственной канцелярии в качестве ее рабочего органа Эстонский фонд информатики (EIF).

В марте 1993 года в составе Государственной канцелярии был образован отдел государственных инфосистем (RISO), важнейшим партнером которого являлся EIF.

28 января 2002 года была выдана первая ID-карта.

7 октября 2002 года была поставлена первая цифровая подпись, когда мэры городов Таллинна и Тарту скрепили цифровыми подписями договор о сотрудничестве.

12 марта 2003 года открылся информационный портал гражданина www.eesti.ee, который давал людям информацию об их правах и обязанностях, а также делился советами по практическому ведению дел с городскими учреждениями.

В мае 2003 года при слиянии Эстонского центра информатики и Центра государственных закупок был создан Центр развития государственных инфосистем (RIA).

10 декабря 2013 года премьер-министры Эстонии и Финляндии подписали цифровыми подписями в формате BDOC меморандум о сотрудничестве.

С 29 июня 2015 года круглосуточно работает мониторинговая группа отдела по обработке инцидентов службы кибербезопасности CERT-EE.

С июля 2016 года учреждения публичного сектора других стран Европейского союза акцептируют цифровые подписи, поставленные гражданами Эстонии. Аналогично государственные ведомства и учреждения местных самоуправлений Эстонии признают электронно-цифровые подписи других стран ЕС.

30 сентября 2016 года RIA и регистр народонаселения Финляндии заключили соглашение об объединении X-tee и его финского аналога (Palveluväylä).

С сентября 2019 года RIA использует в государственных службах в качестве средства аутентификации также Smart-ID.

ДОСТИГЛИ?

В 1996 году Эстонский фонд информатики был реорганизован в государственное учреждение под управлением Государственной канцелярии, которое получило название Эстонский центр информатики (EIK). Эстонский совет по информатике был преобразован в консультирующую правительство комиссию. Совет хотя и сохранил свое прежнее название, но стал выполнять новые задачи.

В 1997 году в состав Эстонского центра информатики вошел отдел передачи данных (ASO), действовавший ранее при институте кибернетики.

В 1998 году ASO стал одним из существенных администраторов и разработчиков магистральной сети передачи данных ReaTee.

В 2000 году был создан отдел государственных информационных систем (RISO) Министерства транспорта и коммуникаций. С 1 января 2001 года также Эстонский центр информатики перешел в сферу управления Министерства транспорта и коммуникаций в качестве управляемого государственного учреждения, где он продолжил деятельность в прежних основных направлениях.

В 2001 году RISO инициировал два государственных проекта, реформирующих ИКТ-инфраструктуру: слой обмена данными X-tee и eKodanik, из которых на сегодняшний день сформировался государственный портал, объединяющий э-услуги.

В августе 2004 года начала работать система мер безопасности инфосистем государственных учреждений и местных самоуправлений ISKE.

В 2006 году был создан центр обмена документами DVK, который объединил системы администрирования документами под государственным управлением.

1 марта 2006 года был создан отдел по обработке инцидентов кибербезопасности, который выполняет на государственном уровне задачи CERT Eesti.

1 июня 2011 года Центр развития государственных инфосистем был реорганизован в Департамент государственной инфосистемы (RIA).

1 октября 2009 года был создан отдел по защите жизненно важных инфосистем (KIIK).

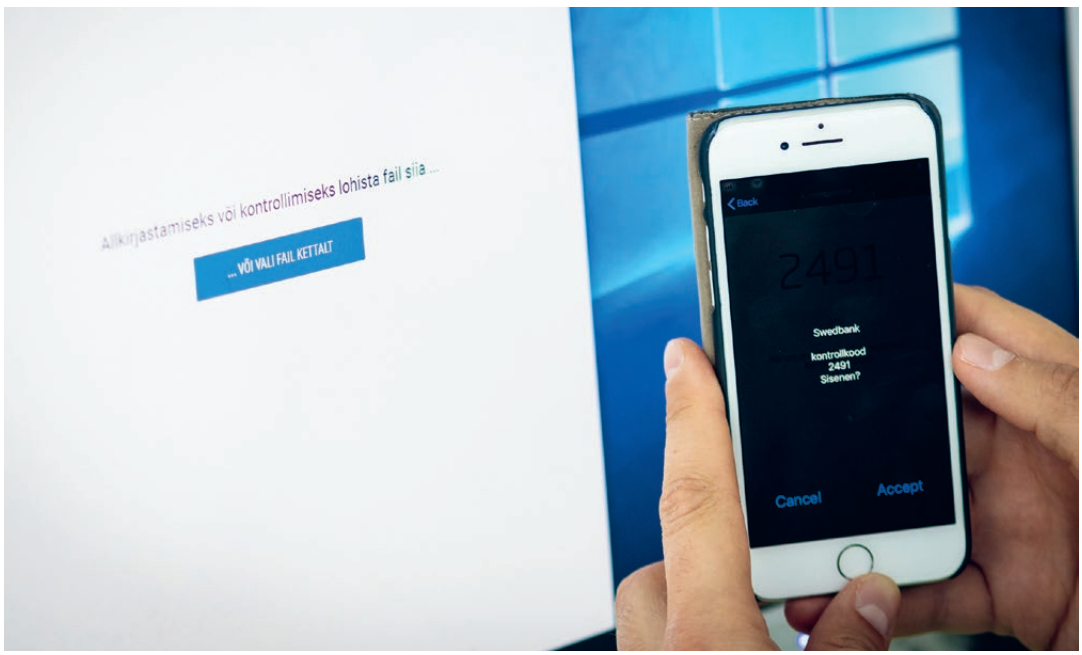
29 мая 2008 года начала работать система администрирования государственной инфосистемой (RIHA), цель которой – дать целостную картину государственных ИТ-ресурсов.

7 марта 2017 года министр предпринимательства и инфотехнологий Эстонии и министр по внешней торговли и развитию Финляндии подписали договор о сотрудничестве Эстонии и Финляндии, на основании которого формируется совместное недоходное объединение с целью общего развития X-tee.

30 августа 2017 года международная группа ученых проинформировала RIA об обнаружении риска безопасности, которому подвержены приблизительно 750 000 ID-карт. В октябре было выпущено обновление программного обеспечения для ID-карт, устраняющее их уязвимость.

В июле 2019 года был создан секретариат сети EU CyberNet, объединяющий в RIA экспертов Европейского союза по кибербезопасности. Секретариат координирует все проекты кибербезопасности Европейского союза, проводимые в третьих странах.

В декабре 2018 года поступили в обращение ID-карты нового поколения с новыми защитными элементами и бесконтактным интерфейсом.



eID: ключ к э-услугам

У каждого человека есть физическая идентификация. Почти у всех жителей Эстонии помимо этого имеется также электронная идентификация (eID), с помощью которой мы можем себя аутентифицировать электронным образом, ставить электронно-цифровые подписи и шифровать файлы.

Важность eID сложно переоценить: без нее у нас не было бы любимых э-услуг, цифровой подписи и возможности вести дела с госучреждениями по интернету. Официальное общение велось бы на бумаге и занимало бы намного больше времени.

ЧТО ЭТО ТАКОЕ?

Электронная идентификация – это набор данных, который связывает лицо в электронной среде с его физической идентификацией. У всех нас есть в физическом и цифровом мире только одна официальная идентификация, но носителей электронной идентификации, или мест, где сохранены данные eID, у одного лица может быть несколько. В Эстонии имеется три крупных носителя eID: ID-карта, Mobiil-ID и Smart-ID. В дополнении к ним электронными признаками пользователя являются также карта вида на жительство, дипломатический ID, диги-ID и диги-ID э-резидента, хотя их доля мала. Банки выдают своим клиентам разные средства аутентификации, но в общем случае их можно использовать только в услугах самого банка или по банковской ссылке в других услугах.

Что делает **RIA**?

- Мы формируем видение и стратегию развития сферы eID. Мы являемся ее представителем и формирователем мнений в Эстонии.
- Отвечаем за безопасность носителя секретного ключа средств eID и содержащегося в нем программного обеспечения, а также за их соответствие требованиям.
- Отвечаем за функционирование, разработку и администрирование программного обеспечения ID (приложение DigiDoc), направленного на конечного пользователя.
- Отвечаем за разработку, функционирование и администрирование программного обеспечения eID, направленного на разработчиков и поставщиков э-услуг.
- Отвечаем за совместные возможности международных электронных идентификаций, то есть за разработку, функционирование и администрирование международного решения программного обеспечения.
- Участвуем в эстонских и международных рабочих группах, а также вносим вклад в развитие государственной сферы PKI.
- Обеспечиваем поддержку пользователей в вопросах по базовому программному обеспечению для ID-карты.
- Обеспечиваем поддержку разработчиков.

КАК ЭТО РАБОТАЕТ?

В Эстонии основанием электронной идентификации является инфраструктура открытого ключа, или PKI (public key infrastructure). Модель PKI основывается на двух связанных между собой ключах – секретном и открытом. Как следует из самого названия, секретный ключ защищен, и его может использовать только человек, которому он выдан. Открытый ключ доступен всем.

Такая модель секретного и открытого ключа позволяет безопасно входить в электронные услуги, или аутентифицироваться цифровым способом и ставить электронно-цифровую подпись. С ее помощью можно также безопасно (в зашифрованном виде) передавать данные. Все операции, связанные со средствами eID (аутентификация, подпись, шифрование и расшифровка), защищены PIN-кодами, то есть для активации секретного ключа следует ввести PIN1 или PIN2.

НОВАЯ ID-КАРТА ПОЛУЧИЛА ОДОБРЕНИЕ

ID-карта – самый распространенный носитель eID. Она является обязательной для всех граждан и постоянных жителей Эстонии с возраста 15 лет.

В обращении находится свыше 1,3 млн действующих ID-карт. В электронном пользовании из них находится приблизительно 930 000. С их помощью ежемесячно совершается в среднем около 20 млн электронных действий (пользователи ставят цифровые подписи и входят в э-услуги).

В ЭСТОНИИ ИМЕЕТСЯ ТРИ КРУПНЫХ НОСИТЕЛЯ EID: ID-КАРТА, MOBIIL-ID И SMART-ID.

Несмотря на то, что популярность Mobiil-ID и Smart-ID – решений eID, работающих в смарт-устройствах – постоянно растет, сегодня ими пользуется примерно половина жителей Эстонии. ID-карта – это первичный носитель eID, без которого нельзя активировать ни Mobiil-ID, ни Smart-ID.

С конца 2018 года Департамент полиции и погранохраны выдает ID-карты с новым оформлением, новыми элементами безопасности и функциями. На новой карте имеется цветная фотография и многие свойственные Эстонии элементы оформления.

Чип новой ID-карты имеет больший объем, что позволяет в будущем добавить в него новые приложения, например, электронный билет общественного транспорта или какую-либо иную справку, выдаваемую

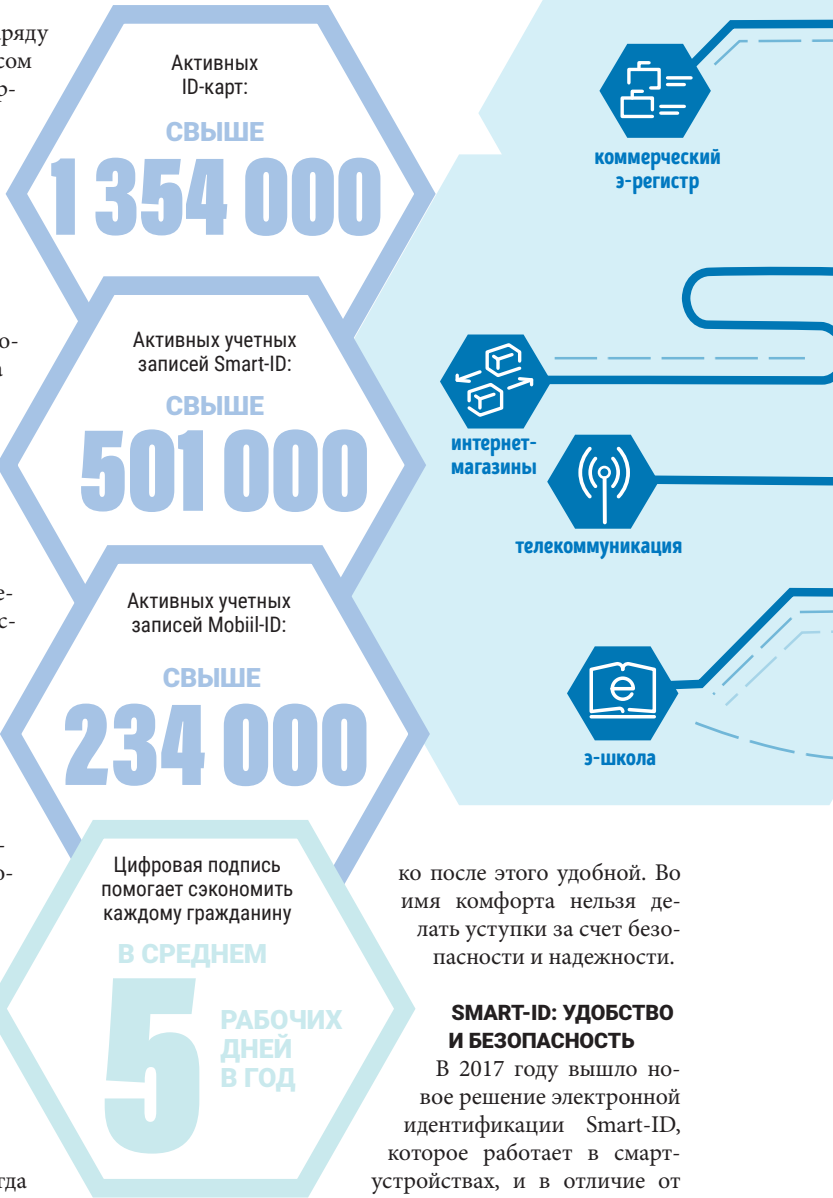
в электронном виде. У новой карты наряду с обычным контактным интерфейсом имеется также бесконтактный интерфейс, который позволяет ее использовать аналогично банковским бесконтактным картам. По соображениям безопасности проставление электронно-цифровой подписи и аутентификация первоначально возможны только с помощью контактного чипа.

В марте 2019 года наша ID-карта получила высокое признание, когда на конференции High Security Printing, проходившей на Мальте, были вручены награды лучшим новым документами и купюрам. В категории ID-карт победу одержала Эстония. Экспертная комиссия высоко оценила оформление карты, защитные элементы, чип и новые решения – QR-код и возможность бесконтактных операций.

В 2020 году мы разработаем возможность удаленного обновления ID-карты, чтобы при необходимости мы могли обновлять программное обеспечение и сертификаты, содержащиеся на чипе. Это одно из тех решений, где мы надеемся, что в подобном никогда не возникнет необходимости, но как показал связанный с ID-картой кризис 2017 года, мы должны быть готовы к неожиданностям.

На чипе ID-карт, выдаваемых с июля 2021 года, помимо файлов с личными данными владельца карты, должна быть фотография и отпечатки пальцев. Мы ведем подготовительную работу в этом направлении.

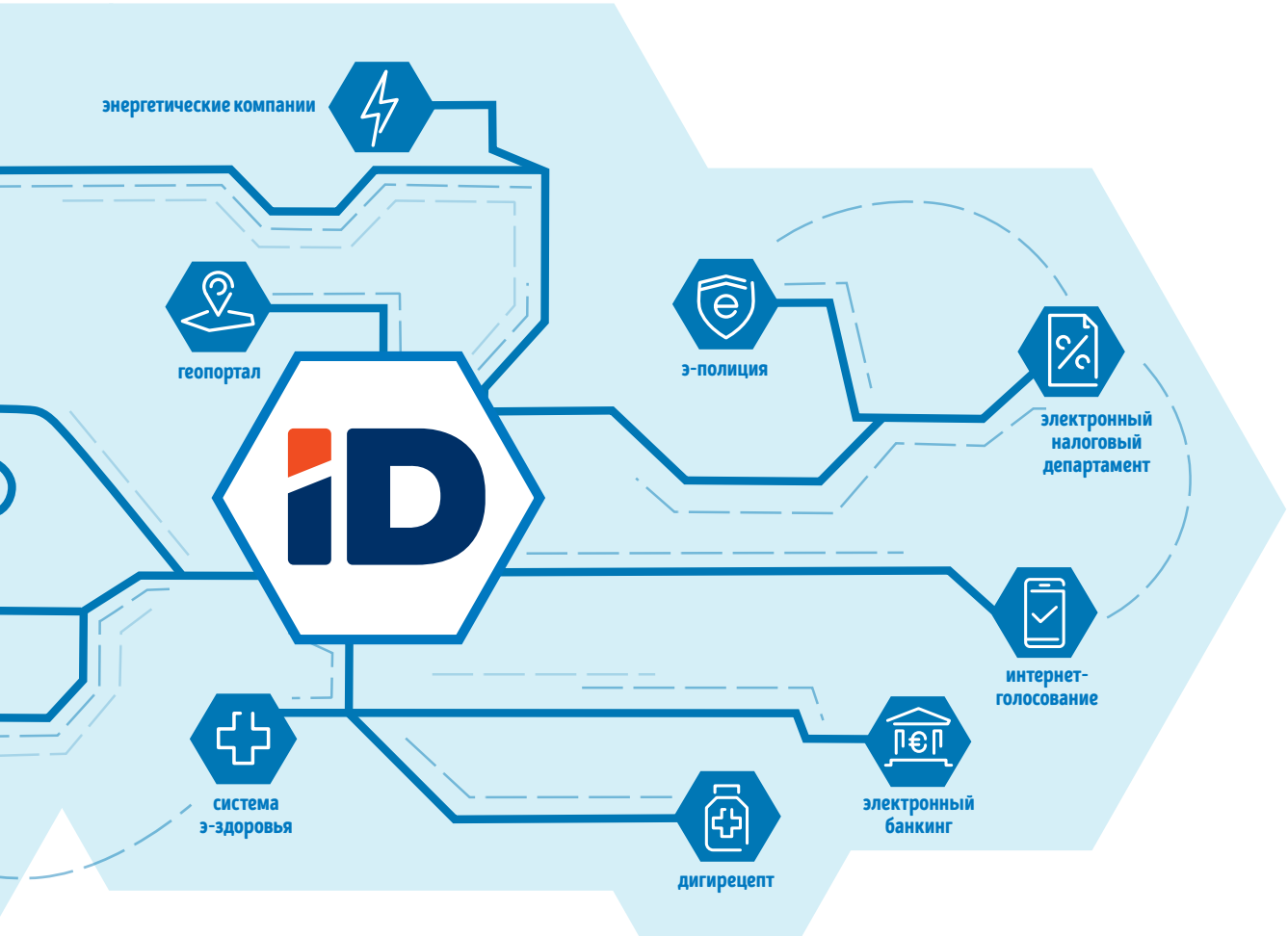
Нас неоднократно спрашивали, когда мы заменим PIN-коды ID-карты отпечатком пальца или распознаванием лиц. Это позволило бы ускорить идентификацию лица и проставление цифровой подписи, а также повысить удобство пользования. К сожалению, с этим придется подождать, поскольку сегодня ни одно решение биометрической идентификации не является достаточно безопасным, чтобы связать его с нашей электронной идентификацией. Без особого усилия можно обмануть считыватели отпечатков пальцев и систему распознавания лиц. eID должна быть в первую очередь безопасной и защищенной, и только после этого удобной. Во имя комфорта нельзя делать уступки за счет безопасности и надежности.



SMART-ID: УДОБСТВО И БЕЗОПАСНОСТЬ

В 2017 году вышло новое решение электронной идентификации Smart-ID, которое работает в смарт-устройствах, и в отличие от Mobiil-ID, для него не требуется SIM-карта. Smart-ID – по популярности второй носитель eID, у которого насчитывается в Эстонии свыше 501 000 пользователей (по состоянию на март 2020 г.). С ноября 2018 года со Smart-ID можно также ставить цифровую подпись.

Несмотря на то, что услуга была радушно принята, в 2019 году над ней сгустились тучи проблем. Мошенники подделали пару десятков эстонских учетных записей Smart-ID. С ID-картой и Mobiil-ID такого ни разу не случалось. С 1 июля 2019 года



активация Smart-ID немного усложнилась, но стала существенно надежнее в отношении мошенничества.

Мы все хотим, чтобы вход в э-услуги и проставление электронно-цифровых подписей были по возможности простыми и быстрыми. Так же незаметно могла бы осуществляться активация носителя eID. Однако на другую чашу весов мы должны поставить безопасность – если ее нет, то пропадет доверие, а вместе с ним и э-услуги.

Мы убедились, что нельзя создавать комфорт за счет безопасности. Если дополнительная просьба к пользователю сделать пару нажатий на экране или щелчков мышкой существенно повысит безопасность носителя eID, то это следует сделать.

ЧТО БУДЕТ С MOBIIL-ID?

Из средств eID третье место по популярности занимает Mobiil-ID. Услугой, выпущенной в 2007 году и работающей на основе SIM-карты, пользуется свыше 234 000 человек. 22% идентификаций личности при использовании государственной услуги аутентификации выполняется с помощью Mobiil-ID. Договор поставки Mobiil-ID завершается в 2021 году. Что случится после этого?

Точного ответа мы дать пока не можем. Нам известно, что государство должно выдать каждому гражданину два альтернативных средства eID. По крайней мере, в течение следующих пяти лет одним из них по-прежнему будет ID-карта. Каким будет второй выдаваемый государством носитель электронной идентификации, сегодня еще неясно. Это может быть, но не обязательно, Mobiil-ID.

СКОЛЬКО НОСИТЕЛЕЙ EID НАМ НУЖНО?

С одной стороны, можно сказать, что чем больше у нас носителей электронной идентификации, тем лучше. В этом случае лучше будут рассредоточены риски: если один из них перестанет работать, остальные продолжат функционировать и наше э-государство будет работать дальше. В то же время создание, разработка и администрирование каждого средства eID несут с собой дополнительные расходы для поставщиков средства и для э-услуг. Три столпа – сейчас ими являются ID-карта, Mobiil-ID и Smart-ID – это разумный компромисс. Риски достаточно минимизированы, и у всех имеется достаточное количество пользователей.

DIGIDOC4 CLIENT: программное обеспечение, окрыляющее ID-карту

ID-карта без программного обеспечения – это простой документ удостоверения личности. Электронные возможности ID-карты раскрывает программное обеспечение DigiDoc, которое установлено уже приблизительно в 600000 компьютерах и с помощью которого ежемесячно ставится полмиллиона цифровых подписей. Если раньше через программу DigiDoc можно было совершать операции с ID-картой и Mobiil-ID, то в январе 2020 года добавилась также поддержка Smart-ID.

ЧТО ЭТО ТАКОЕ?

DigiDoc – это программное обеспечение, которое позволяет ставить электронно-цифровые подписи, открывать документы с цифровой подписью, проверять действие подписей, шифровать файлы и снова переводить зашифрованные данные в читаемый вид, то есть расшифровывать их.

Помимо этого, с DigiDoc можно связать э-почту @eesti.ee, проверять работу своей ID-карты и действие сертификатов, изменять PIN-коды и PUK-коды, и при необходимости отменять блокировку сертификатов.

DigiDoc работает в операционных системах Windows, macOS, Linux, iOS и Android, а также его можно загрузить с сайта id.ee или из магазинов приложений Android и Apple.

ТРИ В ОДНОМ

В июле 2018 года пользователи получили программу DigiDoc4 client с более простым и современным интерфейсом пользователя. Если раньше для основных функций требовалось устанавливать в компьютер три отдельных приложения – средство управления ID-картой, DigiDoc3 client для подписания и DigiDoc Krüpto для шифрования – то теперь с DigiDoc4 можно все действия совершать в одном интерфейсе пользователя и в компьютер нужно устанавливать только одно приложение.

В ходе установки ID-программы в ваш компьютер устанавливается DigiDoc4 client, а также приложения и драйверы, необходимые для аутентификации и подписания в интернете.

TERA СТАВИТ ШТАМПЫ

В действительности в ваш компьютер устанавливается еще одно нужное приложение: приложение «Цифровой штамп» – TeRa. Что оно делает и зачем оно нужно?

Поскольку компьютерные мощности и средства, находящиеся в распоряжении людей с плохими намерениями, постоянно развиваются, то наши цифровые конверты в формате DDOC больше не являются такими безопасными, как десять лет назад. TeRa создает новый конверт в формате ASICS, соответствующий современным требованиям безопасности и запечатанный меткой времени, куда закладывается старый оригинал.

НА ПРОСТАВЛЕНИЕ ЦИФРОВЫХ ШТАМПОВ В НЕСКОЛЬКИХ СОТНЯХ ДОКУМЕНТОВ УХОДИТ ДО ДВУХ МИНУТ.

Новый конверт с меткой времени помогает установить время открытия и изменения старого конверта. Если у участников имеются разные версии одного и того же документа, то с помощью метки времени можно доказать, какая версия является оригиналом.

Пользователям, в чьем компьютере много файлов в формате DDOC, действие которых нужно в дальнейшем проверить и удостоверить, рекомендуется с

Программное обеспечение DigiDoc установлено приблизительно в **600 000** компьютеров.

С его помощью ставится ежемесячно приблизительно **500 000** цифровых подписей.

DigiDoc работает в операционных системах **WINDOWS, MACOS, LINUX, IOS и ANDROID.**

С начала 2020 года DigiDoc поддерживает помимо **ID-КАРТЫ и MOBIIL-ID также SMART-ID.**

Что делает **RIA**?

- **Мы обновляем ID-программы** по меньшей мере два раза в год, чтобы идти в ногу с развитием операционных систем, веб-браузеров и опорных программ, а также предлагать пользователями новые возможности.
- **Обеспечиваем поддержку пользователя ID-карты:** если у вас возникнут проблемы при использовании ID-карты, программного обеспечения DigiDoc4 client или TeRa, то вы найдете решение по адресу id.ee.
- **Разрабатываем** приложение TeRa и **управляем** им.
- **Посредничаем в оказании услуги метки времени** для учреждений публичного сектора.

помощью приложения TeRa повысить их стойкость к взлому. Это выполняется легко и быстро: TeRa после запуска отыскивает в компьютере устаревающие цифровые подписи (в формате DDOC) и помещает их в новый контейнер, криптографически более надежный к взлому. Все старые файлы сохраняются в том же месте, где они находились первоначально, но наряду с ними возникают новые файлы ASICS, которые можно открыть с помощью приложения DigiDoc4. На проставление цифровых штампов в нескольких сотнях документов уходит до двух минут.

БЛАГОДАРЯ Э-РЕЗИДЕНТАМ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ DIGIDOC С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ ИСПОЛЬЗУЕТСЯ ПО ВСЕМУ МИРУ.

X-TEE: артерии э-государства

Многие из нас в учебнике биологии или в кабинете семейного врача видели иллюстрации кровообращения человека. Рассматривая их, мы понимаем, как человек живет и функционирует. «Кровообращение» э-государства мы можем визуализировать аналогично со своим, но имеется одно важное отличие. Сердце, без которого человек не может жить, у э-государства полностью отсутствует. Наше цифровое государство рассредоточено.

ВСЕ ЯЙЦА ПО РАЗНЫМ КОРЗИНАМ

В отношении любой базы данных существует риск, что произойдет утечка ее содержания. Если бы государство собрало всю имеющуюся у него информацию в общий склад данных, то достаточно было бы одной атаки или человеческой ошибки, чтобы все данные утекли. Не говоря уже о том, что центральное управление такой базой данных было бы затратным и сложным.

Эстония свела к минимуму этот риск так, что каждое учреждение и министерство заботится о своих данных самостоятельно. В регистре народонаселения имеется информация о месте жительства человека, а в коммерческом регистре – о предприятии, у Департамента шоссейных дорог – информация об автомобилях. Если одна база данных окажется «под ударом», то других это не коснется.

Как учреждения выполняют свои задачи, если информация о людях, предприятиях, автомобилях, образовании, здоровье, участках земли и поступлении налогов распределена по всей Эстонии?

НА ПОМОЩЬ ПРИХОДИТ X-TEE

На помощь спешит слой обмена данных X-tee, начавший работать в Эстонии в 2001 году. Это решение, которое помимо прочего помогает купить в аптеке лекарство по дигирецепту, проверить с помощью устройства э-полиции данные об автомобиле и его владельце, помогает серверам министерства обороны запрашивать из регистра народонаселения, принадлежащего министерству внутренних дел, информацию о новых военнослужащих срочной службы. Примеров, которые уменьшают бюрократию и добавляют эффективности, можно привести тысячи.

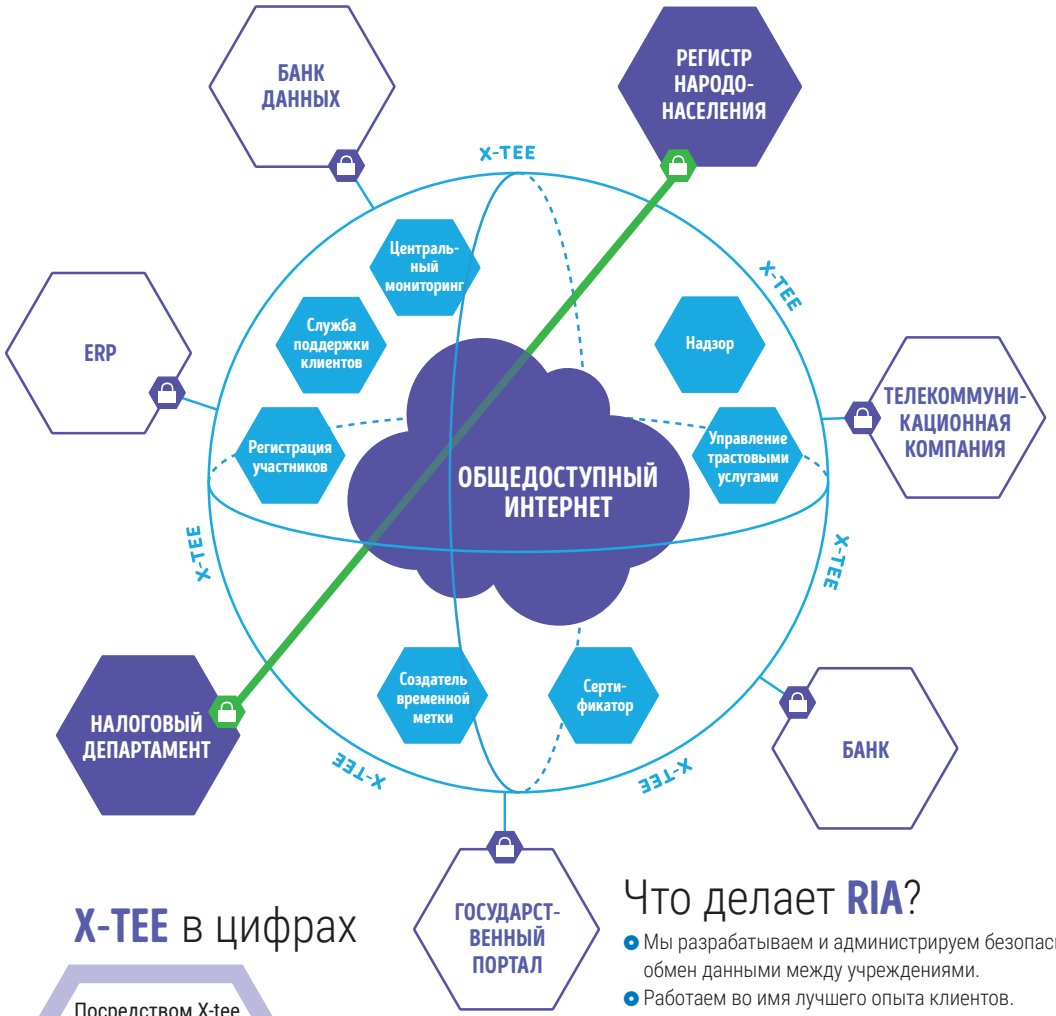
Важно понимать, что X-tee – это только средство для безопасного обмена данными, которое создает для этого общий протокол. Если бы X-tee не было, каждое учреждение должно было бы самостоятельно разрабатывать протокол и решать вопросы безопасности. Целостности данных ничего не угрожает, поскольку данные в архитектуре X-tee не сохраняются. Без X-tee актуальность данных представляла бы постоянную головную боль, поскольку если каждое учреждение хранит на своем сервере копии, то очень затратно по времени и тяжело выяснить, какая из них самая новая и правильная.

РАЗРАБОТКИ ПОДДЕРЖИВАЮТ ЗДОРОВЬЕ Э-ГОСУДАРСТВА В ПОРЯДКЕ

X-tee – главное решение в Эстонии, с помощью которого публичный сектор может обмениваться данными между собой и с частным сектором обмениваться данными. Нам доставляет радость, что количество членов, услуг и запросов X-tee увеличивается. Чтобы максимально упростить вступление в члены X-tee, мы разрабатываем среду самообслуживания. Предприятия и государственные учреждения, которые еще не используют X-tee, могут удобно и с минимальным усилием присоединиться в будущем.

ИЗ СОВМЕСТНОГО ЭСТОНСКО-ФИНСКОГО ПРОЕКТА ВЫРОС X-ROAD

X-tee, используемый в Эстонии, представляет собой государственную платформу по обмену данными. Если же речь идет об англоязычной версии X-Road, то здесь имеется в виду технология, которую совместно разрабатывают Эстония и Финляндия с 2015 года. В феврале 2020 года была достигнута важная веха – коммерческие регистры Эстонии и Финляндии впервые поделились данными посредством X-Road.



X-TEE в цифрах

Посредством X-tee можно пользоваться

ПОЧТИ **2700**

услугами.

За 19 лет в X-tee было совершено приблизительно

6 МЛРД

запросов.

Ориентировочно 3% из них совершили люди.

У эстонской системы X-tee насчитывается свыше

500

учреждений ...

...и почти

1200

подключенных инфосистем.

Что делает **RIA**?

- Мы разрабатываем и администрируем безопасный обмен данными между учреждениями.
- Работаем во имя лучшего опыта клиентов. Цель – упростить и ускорить внедрение X-tee.
- Мы делимся опытом X-tee с другими странами. X-Road или его компоненты используют страны по всему миру, например, Финляндия, Канада, Мексика, Уругвай, Израиль, Исландия, Норвегия, Шотландия, Испания, Япония и Вьетнам. https://x-road.global/xroad-world-map

В 2019 году мы закрыли 5-ю версию X-tee, использовавшуюся с апреля 2011 года, и на международном уровне разрабатываем следующую, 7-ю версию X-Road, являющуюся основой X-tee.

КРУПНЕЙШИЕ ПОЛЬЗОВАТЕЛИ X-TEE

За 19 лет в X-tee было совершено приблизительно 6 млрд запросов. Мы предполагаем, что из них 3% совершили люди. Предполагая, что щелчки в интернете экономят в среднем 15 минут времени человека (он не должен идти в Департамент шоссейных дорог, Налоговый департамент или больницу, чтобы забронировать время приема), эти запросы сэкономили только в прошлом году в общей сложности 1100 лет рабочего времени.

EESTI.EE: наша дверь в э-государство

Государственный портал eesti.ee, открывшийся весной 2003 года – это быстрый и практичный контактный пункт, где жители и предприятия Эстонии получают достоверную информацию о предлагаемых государством услугах. Помимо этого, государственные учреждения и местные самоуправления могут через него безопасно общаться с людьми. На портале имеется информация об э-услугах и событиях жизни, а государственная э-почта помогает государству безопасно информировать людей.

МЫ ПРИВЕЛИ В ПОРЯДОК ДАЛЬНЮЮ КОМНАТУ

В 2019 году пользователи государственного портала даже и не заметили существенных изменений, поскольку большая часть разработок была направлена на приведение в порядок дальней комнаты eesti.ee (back-end). В этом году мы по большей части завершим эту работу. Далее мы приступим к обновлению портала, предусмотренного для предпринимателей.

ПОЧТОВЫЙ ЯЩИК EESTI.EE

RIA работает над тем, чтобы почтовый ящик eesti.ee стал в ближайшие годы основным каналом для обмена информацией с государством. Почтовый ящик работает уже много лет, но сейчас ведется дискуссия о возможных изменениях, которые позволили бы считать извещение доставленным, если оно поступает к получателю в почтовый ящик государственного портала. Идея находится только на стадии формирования, и еще нет полной уверенности, как это будет работать в будущем.

Общение через бумажные письма не исчезнет, но больше не будет основным способом информирования людей, поскольку цифровой обмен информацией происходит быстрее, удобнее и дешевле. В будущем все извещения государственных учреждений или местных самоуправлений будут поступать в почтовый ящик eesti.ee и будут там всегда доступны.

Извещения можно направлять также на внешний адрес э-почты, но почтовый ящик государственного портала – это место, где все предыдущие э-письма сохраняются. Поэтому не нужно беспокоиться, что из-за ошибки самого человека (удаление письма) или поставщика услуги (перебой в работе услуги) сообщение не поступит в его почтовый ящик. Историческая память об общении между государством и гражданином сохраняется в почтовом ящике eesti.ee.

ПОЯВЛЯЕТСЯ ВИРТУАЛЬНЫЙ СОБЕСЕДНИК

В настоящее время около 25 государственных учреждений используют для передачи важной информации почтовый ящик eesti.ee. Цель заключается в том, чтобы продвинуться настолько далеко, чтобы к услуге присоединились все учреждения. Помимо этого, в стадии разработки находятся календарь, который будет сообщать человеку о важных событиях, и виртуальный собеседник (чатбот), который помогал бы ему проще общаться с государством.

История EESTI.EE

Государственный портал eesti.ee был открыт 12 марта 2003 года. Портал дает людям информацию об их правах и обязанностях в Эстонии. Помимо этого, здесь делятся советами по практическому ведению дел с государственными учреждениями.

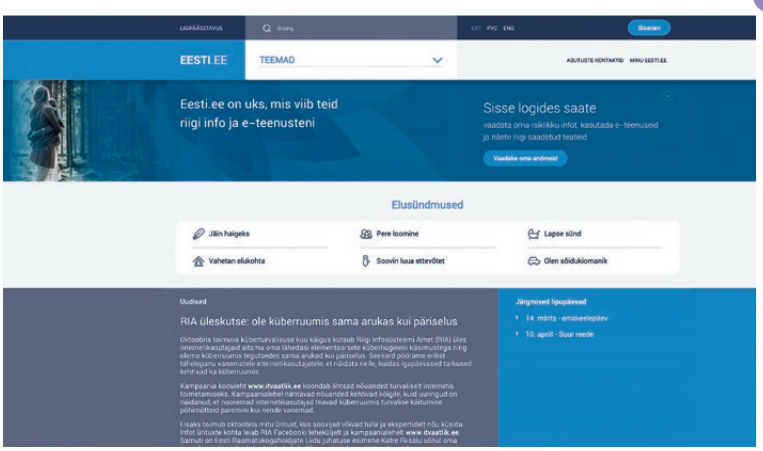
В 2005 году на портале появляются статьи на английском и русском языках. Дизайн сайта становится более удобным для пользователя и логичным. Предприятия начинают использовать адрес э-почты @eesti.ee.

В 2007 году появляется прародитель нынешнего государственного портала. Новый государственный портал объединяет в себе предыдущий информационный портал и портал гражданина, а информация распределена по блокам для гражданина, предпринимателя и чиновника. Eesti.ee становится центральным государственным порталом, который за месяц посещает 110 000 человек, из них 8000 иностранцев. Почтовым ящиком @eesti.ee пользуются 19 000 человек и 17 000 предприятий.

С 2008 года на портал можно войти через Mobiil-ID.

В 2009 году eesti.ee получает новый и до сих пор наиболее узнаваемый зеленый логотип.

В 2011 году выходит часть для предпринимателя с



Что делает **RIA**?

- **В нашем ведении находится** государственный портал eesti.ee.
- **Мы собираем на нем э-услуги** государственных учреждений.
- Через eesti.ee **мы предоставляем контактные данные** учреждений и информацию о предлагаемых государством услугах.
- Каждому человеку с личным кодом Эстонии **мы обеспечиваем** на государственном портале собственный адрес э-почты в виде личный_код@eesti.ee. Предприятиям мы предлагаем адрес в виде регистрационный_код@eesti.ee и название_предприятия@eesti.ee.

более полным содержанием, чем ранее. На портале насчитывается 200 услуг, 400 статей и 2500 контактов.

С 2013 года пользователь при входе в систему видит на главной странице свои личные данные и события.

В 2015 году в eesti.ee насчитывалось 815 э-услуг. В течение 2014 года портал посетили пользователи примерно из 200 стран и 9000 городов. Чаще всего пользователи смотрят меню «Мои дела », входят в SAIS, заполняют листы нетрудоспособности и просматривают свои рецепты.

В ДЕКАБРЕ 2015 года изменяются условия пользования извещениями eesti.ee. Направлением на свой адрес @eesti.ee человек дает согласие, что государственные учреждения присылают ему на этот адрес официальные документы и передают сообщения.

В 2017 году в eesti.ee на эстонском, русском и английском языках было в общей сложности 1330 статей, 154 услуги и 2866 контактов.

С КОНЦА 2018 года портал eesti.ee работает в своем нынешнем оформлении.

ГОСУДАРСТВЕННАЯ СЕТЬ: быстрая и безопасная передача данных публичному сектору

Государственная сеть предлагает государственным учреждениям и местным самоуправлениям услугу интернета и передачи данных более чем в 1400 местах в Эстонии. К государственной сети подключилось 97% учреждений публичного сектора. В исключительном случае могут подключиться также юридические лица, оказывающие публичную услугу от имени государства.

ГОСУДАРСТВЕННАЯ СЕТЬ – БЫСТРАЯ

Предлагаемая конечному клиенту скорость загрузки и отправки данных составляет максимально 1 Гбит/с, но мы можем предложить также соединение с максимальной скоростью 10 Гбит/с. Основой государственной сети является магистральная сеть, скорость которой должна в ближайшее время повыситься до 200 Гбит/с. При этом как минимум 30% ресурсов мы храним в резерве, чтобы обеспечить плавную работу магистральной сети даже в ситуациях, когда нагрузка временно возрастает.

ГОСУДАРСТВЕННАЯ СЕТЬ – БЕЗОПАСНАЯ

За ее работой круглосуточно следит CERT-EE, занимающийся не только выявлением и решением киберинцидентов, но и их предупреждением. С весны 2019 года у соединений государственной сети с зарубежными странами имеется защита от распределенной атаки типа «отказ в обслуживании» (DDoS). В случае атак внутри Эстонии мы способны быстро выйти на след злоумышленников.

Государственная сеть управляет дублирующей узловой интернет-точкой RTIX, которая соединяет между собой интернет-сети Эстонии и цель которой – обеспечить движение между сетями даже в том случае, когда соединение с зарубежными странами нарушено.

ПОМОЩЬ РЯДОМ

При решении неисправностей мы ведем сотрудничество с центром инфотехнологий и развития Министерства внутренних дел (SMIT). Если, например, в Валга или Курессааре какое-либо сетевое устройство понадобится заменить в срочном порядке, то техник RIA не должен для этого приезжать на место из Таллинна, вместо этого мы можем попросить помощи у техников SMIT, которые в большинстве случаев находятся поблизости. Так государство получает от этого выгоду, поскольку мы избегаем дублирования, а клиент государственной сети – удобство, поскольку помощь прибывает на место быстрее.

ЧТО ЖДЕТ В БУДУЩЕМ?

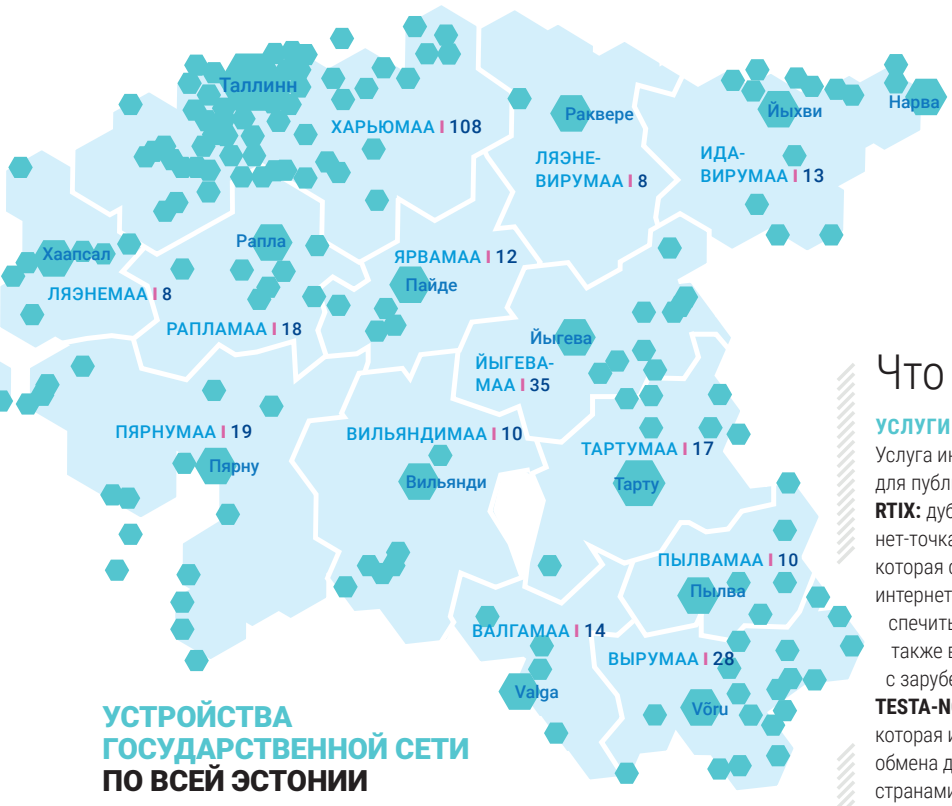
Мы каждый день работаем над развитием сети и прилагаем усилия, чтобы сократить время, затрачиваемое на создание клиентского соединения. Мы расширяем магистральную сеть и увеличиваем ее способность – ставим своей целью повысить скорость до 200 Гбит/с.

Выполняя все это, мы отдаем себе отчет, что государственная сеть – словно Таллинн, строительство которого никогда завершится. Технология развивается, и государственная сеть должна идти с ней в ногу.

Предлагаемая клиенту скорость передачи данных составляет обычно до **1** Гбит/с

но мы можем предложить также **10** Гбит/с

Цель – повысить скорость магистральной сети до **200** Гбит/с



УСТРОЙСТВА ГОСУДАРСТВЕННОЙ СЕТИ ПО ВСЕЙ ЭСТОНИИ

Кто является **КЛИЕНТОМ** государственной сети?

Приблизительно

1000

ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ:

министерства и их подведомственные учреждения, а также учреждения с государственным участием

По состоянию на конец 2019 года мы находимся в

46

местных самоуправлениях

Всего приблизительно в

356

учреждениях

55 библиотеки

71 местные самоуправления (волостные дома, административные центры и др.)

138 образовательные учреждения (школы и детские сады)

84 народные дома, молодежные комнаты, дома престарелых и пр.

Данные по состоянию на декабрь 2019 г.

Что делает **RIA**?

УСЛУГИ ГОСУДАРСТВЕННОЙ СЕТИ

Услуга интернета и передачи данных для публичного сектора.

RTIX: дублирующая узловая интернет-точка, управляемая государством, которая соединяет между собой интернет-сети Эстонии. Ее цель – обеспечить движение между сетями также в том случае, если соединение с зарубежными странами нарушено.

TESTA-NG: услуга передачи данных, которая используется для безопасного обмена данными между институтами и странами-участниками Европейского союза. Цель – перевести все решения по безопасному обмену данными между странами-участниками ЕС в сеть TESTA.

DNS: система доменных имен, благодаря которой для входа на желаемый сайт мы можем написать в адресной строке веб-браузера вместо IP-адреса (комбинации цифр) доменное имя.

DNSSEC: набор безопасных расширений системы доменных имен, который гарантирует, что пользователь направляется на тот сайт, адрес которого он ввел в веб-браузер, а не на поддельный сайт, созданный мошенниками.

NTP: служба точного времени. Для ее использования своим первичным источником времени следует определить сервер времени ASO (ntp.aso.ee). Для предложения услуги мы используем NTP-серверы класса STRATUM 1 на базе GPS, которые продублированы между собой и физически находятся в разных местах.

CACHE: клиенты государственной сети могут использовать буферные серверы, которые помогают быстрее доставлять запрошенные данные.

97% учреждений публичного сектора подключились к государственной сети.

В 2019 году мы инвестировали в обновление оборудования государственной сети **1** миллион евро

Э-ГОЛОСОВАНИЕ
Мы являемся первопроходцами

Выборы в местные самоуправления, состоявшиеся в октябре 2005 года, были особенными: Эстония стала первой в мире страной, которая на государственных выборах применила э-голосование.

В то время проголосовавших электронным способом было всего 9317 человек, что составило 1,9% от участвовавших в выборах. На выборах в Рийгикогу 2019 года свои голоса электронным образом отдали уже 247 232 человека, то есть 43,8% от участвовавших в выборах.

ЧТО ЭТО ТАКОЕ?

Электронное голосование проходит посредством электронного устройства. Э-голосование позволяет отдать голос из любого места, где имеется компьютер с подключением к интернету и ID-карта, Mobiil-ID или digi-ID с действующими сертификатами. Проголосовать электронным способом можно в период предварительного голосования, но не в день выборов.

Цель э-голосования – упростить выборы и сделать их удобными для избирателей и организаторов.

КАК ЭТО РАБОТАЕТ?

Для э-голосования нужно загрузить в компьютер приложение избирателя. После идентификации личности приложение проверяет, имеете ли вы право голоса, и в случае положительного ответа выводит на экран список кандидатов.

После того, как вы выбрали кандидата и подтвердили свой отданный голос цифровой подписью, приложение избирателя отправляет голос на сервер сбора голосов. Услуга регистрации добавляет к каждому голосу временную метку, которая позволяет впоследствии проверить, все ли голоса поступили на сервер-сборщик. Если вы желаете проверить, засчитался ли отданный вами голос кандидату, которого вы выбрали, то это можно сделать с помощью специального телефонного приложения.

Все э-голоса засекречиваются. Для этого используется алгоритм шифрования, спецификацию которого определяет государственная избирательная служба перед каждыми выборами. Голос шифруется с помощью двух ключей. Приложение избирателя использует для засекречивания голоса открытый ключ. Для открытия голоса необходим секретный ключ, к которому имеется доступ только у членов государственной избирательной комиссии.

КАК ЭТО КАСАЕТСЯ RIA?

Процедуру э-голосования избирательная служба организует в сотрудничестве с Департаментом государственной инфосистемы (RIA). Сотрудничество началось за несколько лет до того, как мы создали хостинг для системы э-голосования, и с этого времени оно постоянно расширялось. Желание избирательной службы и RIA заключается в том, чтобы в будущем за разработку и администрирование всех инфосистем, связанных с выборами, отвечал RIA.

В 2019 году ответственность за информационную безопасность выборов перешла от избирательной службы к RIA. Мы задействовали дополнительные серверы, усилили брандмауэр, обеспечили государственную сеть защитными мерами против распределённых атака типа «отказ в обслуживании» (DDoS) и протестировали инфосистемы выборов. Помимо этого, мы организо-

НА ЗАМЕТКУ

Когда можно будет выбирать по мобильному телефону?

Мы хотим сделать выборы доступными в том числе в мобильных телефонах, которые мы с каждым днем используем всё больше и больше. Мы надеемся, что возможность м-выборов добавиться уже к выборам в местные самоуправления 2021 года, но прежде мы должны быть убеждены в их безопасности.

ДОЛЯ ПРОГОЛОСОВАВШИХ ЭЛЕКТРОННЫМ СПОСОБОМ
лиц среди всех избирателей

На последних выборах в Европейский Парламент каждый второй голос был отдан электронным способом.

ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ
в цифрах

Время, затрачиваемое на электронное голосование

3

МИНУТЫ

На выборах в Рийгикогу 2019 года свой голос электронным способом отдали

247 232

ЧЕЛОВЕКА,...

...это

43,8%

от общего числа участвовавших в выборах.

Что делает RIA?

- **Мы организуем проведение э-голосования:** обеспечиваем необходимое для этого аппаратное и программное обеспечение.
- **Разрабатываем и управляем инфосистемой выборов (VIS):** она позволяет регистрировать кандидатов, определять результаты выборов, а также активность голосования и выборов и делиться этой информацией с общественностью.
- **Отвечаем за информационную безопасность выборов**: тестируем инфосистемы выборов; защищаем их от возможных атак, обучаем кандидатов и группы по проведению кампаний.

вали учебные курсы по кибергигиене для кандидатов и групп по проведению кампании, протестировали веб-страницы кампании и партий, а также создали должность руководителя ведомственной охраны.

ЧТО ЖДЕТ В БУДУЩЕМ?

С 2019 года RIA отвечает также за разработку инфосистем выборов. Мы работаем над новой версией, или VIS3. Она принесет несколько изменений, которые сэкономят рабочие часы организаторов выборов и кандидатов и увеличат прозрачность.

До сих пор список избирателей распечатывался на бумаге, и член избирательного участка водил пальцем, проверяя, имеется ли в списке человек, пришедший на участок. VIS3 в свою очередь сделает списки избирателей электронными. Это и поправка к Закону о выборах являются предпосылкой для проведения электронного голосования до конца предварительного голосования, и в день выборов избиратель может изменить свой электронный голос, проголосовав на избирательном участке с бумажным бюллетенем.

Если до сих пор информация по активности выборов поступала перед выборами один раз в день и в день выборов три раза, то новая инфосистема выборов будет передавать ее чаще.

Новую инфосистему смогут использовать также кандидаты и партии: для представления списка кандидатов им не нужно будет приходить в избирательную службу, они смогут сделать это с помощью системы и одновременно оплатить необходимые государственные пошлины.

С новой инфосистемой выборов мы сэкономим тысячи рабочих часов на организацию и проведение выборов.

Когда версия VIS3 будет готова, мы опубликуем ее код, чтобы все интересующиеся могли изучить его структуру.

ГОСУДАРСТВЕННАЯ УСЛУГА АУТЕНТИФИКАЦИИ: безопасная дверь в э-услуги

Если вы желаете войти в какую-либо государственную э-услугу, то вам следует в первую очередь себя аутентифицировать, то есть удостоверить свою личность. Аутентификация должна быть достоверной и безопасной, поскольку никто не хочет, чтобы к его данным имели доступ посторонние или чтобы от его имени совершал сделки злоумышленник.

Для учреждений публичного сектора и других исполнителей общественной задачи здесь приходит на помощь государственная услуга аутентификации, где для идентификации лица можно использовать ID-карту, Mobiil-ID, Smart-ID и/или международную аутентификацию. Их можно комбинировать или использовать по отдельности.

АУТЕНТИФИКАЦИЯ ДОЛЖНА БЫТЬ ДОСТОВЕРНОЙ И БЕЗОПАСНОЙ.

ЗАЧЕМ ЭТО НУЖНО?

В Эстонии насчитывается несколько сотен предлагаемых э-услуг публичного сектора, которые обязаны идентифицировать пользователя. И хотя большинство из них уже поддерживает аутентификацию по ID-карте, а большая часть также по Mobiil-ID, тем не менее было предусмотрено добавление средств eID и возможности, что эти э-услуги будут способны идентифицировать не только жителей Эстонии, но и граждан других стран Европейского союза.

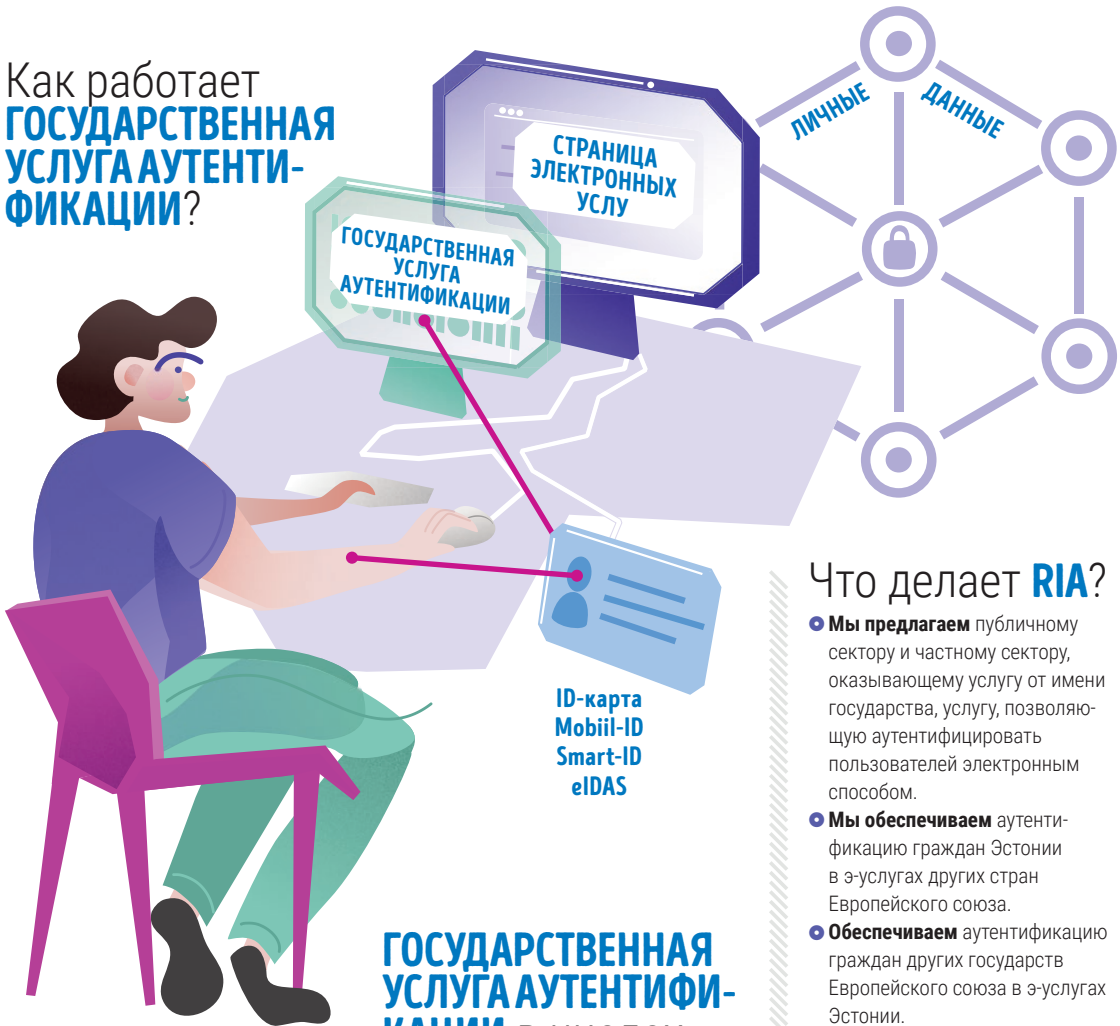
Поскольку новые разработки и требования приносят каждому поставщику услуги дополнительный расход, то родился план создать центральную услугу аутентификации, которой могут пользоваться все учреждения публичного сектора и за разработку и надежность которой отвечает RIA. Поставщики услуг в свою очередь могут сосредоточиться на своей основной деятельности.

ЧТО ЖДЕТ В БУДУЩЕМ?

Если вы используете службы Google, то знаете, что для доступа к своим э-письмам, документам и фотографиям достаточно одного входа в систему. Однако при перемещении между э-услугами публичного сектора Эстонии нужно каждый раз снова себя аутентифицировать.

Мы хотим изменить эту традицию и протестировать, можно ли в государственной услуге аутентификации использовать разовую услугу входа (SSO). Как уже следует из названия, такое решение требует только одной аутентификации: если пользователь через государственную услугу аутентификации вошел в какую-либо э-услугу, то он может пользоваться и другими э-услугами, не идентифицируя в каждой из них повторно свою личность.

Как работает **ГОСУДАРСТВЕННАЯ УСЛУГА АУТЕНТИФИКАЦИИ**?

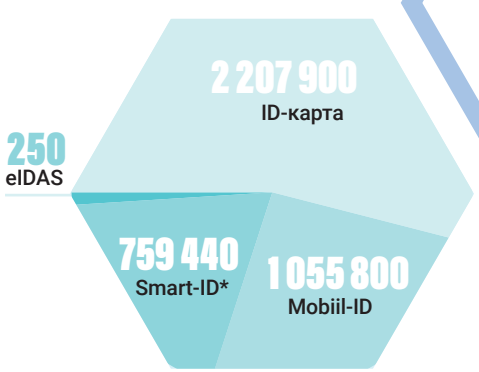


Что делает **RIA**?

- **Мы предлагаем** публичному сектору и частному сектору, оказывающему услугу от имени государства, услугу, позволяющую аутентифицировать пользователей электронным способом.
- **Мы обеспечиваем** аутентификацию граждан Эстонии в э-услугах других стран Европейского союза.
- **Обеспечиваем** аутентификацию граждан других государств Европейского союза в э-услугах Эстонии.
- **Обеспечиваем** надежность и безопасность государственной услуги аутентификации.
- **При необходимости мы добавляем** в государственную услуги аутентификации новые безопасные методы аутентификации (в октябре 2019 года добавился Smart-ID).

ГОСУДАРСТВЕННАЯ УСЛУГА АУТЕНТИФИКАЦИИ в числах

ЗНАЧИМОСТЬ МЕТОДОВ АУТЕНТИФИКАЦИИ в государственной услуге аутентификации, 29.03.–31.12.2019



* Smart-ID добавился в октябре 2019 года

Государственную услугу аутентификации использует

78 **Э-УСЛУГ,**

в том числе eesti.ee, e-MTA, э-услуги регистра народонаселения и э-услуги Кассы по безработице.

По состоянию на январь 2020 года к тестовой среде присоединилось

149

Э-УСЛУГ

УСЛУГА ПОДПИСИ: чтобы вы могли сфокусироваться на основной деятельности

Люди ставят подписи уже несколько столетий. Собственноручным написанием своего имени мы соглашаемся с содержанием или подтверждаем, что ознакомились с ним. Электронно-цифровая подпись является современным аналогом обычной подписи. С ее помощью можно совершать электронным способом операции, для которых раньше нам требовались бумага и ручка.

Цифровая подпись приравнена законом к собственноручной подписи, и все ведомственные учреждения Эстонии обязаны принимать документы с цифровой подписью. Так мы экономим время, деньги и бережем природу. Для подписания документов больше не нужно ехать в государственное учреждение или к договорному партнеру, а с подписанного файла можно сделать бесконечное число юридически равнозначных (запасных) копий. В то время как каждую копию бумажного документа следовало бы подписывать отдельно.

RIA предлагает всем исполнителям общественной задачи центральную услуги подписи, чтобы им не нужно было самим заниматься ее разработкой и управлением, и они смогли бы сосредоточиться на своей основной деятельности.

ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ ЯВЛЯЕТСЯ СОВРЕМЕННЫМ АНАЛОГОМ ОБЫЧНОЙ ПОДПИСИ.

ЧТО ЭТО ТАКОЕ?

Государственная услуга подписи предлагает услугу создания подписанных конвертов. Помимо проставления подписи с помощью услуги можно добавить к конверту временную метку, которая подтверждает, что подпись была поставлена именно в этот момент, и проверить действие поставленных подписей.

Если же для создания аналогичной функциональности исполнителя общественной задачи требуется заключать отдельные договоры для подписания с помощью Mobiil-ID, использования услуги подтверждения действия и услуги временной метки, то с предлагаемой RIA услугой эта процедура упрощается: один договор, одно подключение, и все перечисленные возможности имеются.

КАК ЭТО РАБОТАЕТ?

Государственная услуга подписи работает внутри других э-услуг. Когда вы заходите на государственный портал eesti.ee или какую-либо иную э-услугу, то с услугой подписи можете соприкоснуться, даже не замечая того.

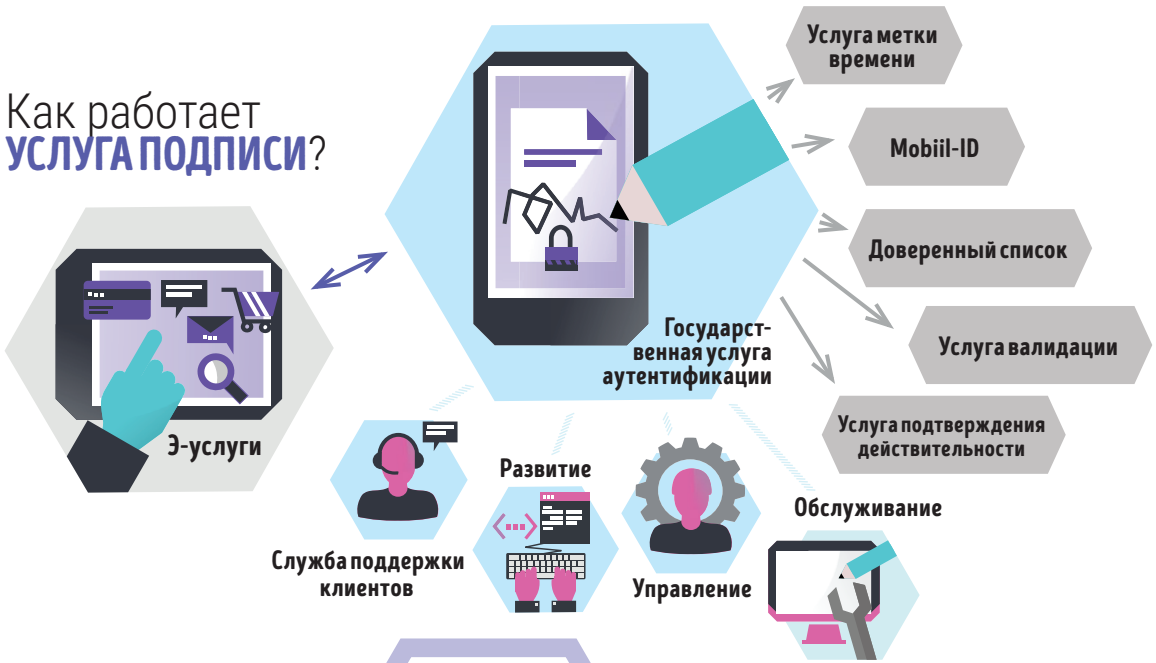
Когда вы загружаете в э-услугу документ и нажимаете на кнопку «Подписать», то она создает хеш документа, или цифровой отпечаток, и запрашивает от ID-карты или какого-либо другого носителя eID подпись, защищенную PIN-кодом.

Эти данные направляются к услуге подписи, которая формирует из них цифровой конверт, или контейнер ASICE, и отправляет его обратно к э-услуге. Затем э-услуга проверяет, совпадают ли отправленный вами файл и подпись с информацией, полученной от услуги подписи, и при положительном ответе помещает документ, требующий подписания, в контейнер ASICE. Последней операцией проверяется действие подписей. Если всё в порядке, то на экране вашего компьютера появится сообщение, что документ подписан.

В фоновом режиме идет активная деятельность, но весь процесс занимает меньше времени, чем вы успеете сказать «Департамент государственной инфосистемы».

Исполнителям общественной задачи RIA предлагает услугу подписи бесплатно. Программное обеспечение, являющееся ее основой, доступно в GitHub для всех желающих, и позволяет каждому оказывать подобную услугу.

Как работает **УСЛУГА ПОДПИСИ**?



В Эстонии насчитывается более **234 000** пользователей Mobiil-ID...

... пользователей Smart-ID более чем в два раза больше, **СВЫШЕ 501 000**

В Эстонии насчитывается **1,35 МЛН** активных ID-карт.

В Эстонии первую цифровую подпись поставили в **2002** году.

К концу января 2020 года было поставлено свыше **878 МЛН** цифровых подписей...

... и сделано свыше **900 МЛН** электронных идентификаций личности.

Что делает **RIA**?

- **Мы предлагае**м всем исполнителям общественной задачи центральную услугу подписи с помощью ID-карты и Mobiil-ID.
- **Мы гарантируем** безопасность услуги подписи, ее надежность, развитие и поддержку пользователям.
- Помимо проставления подписей и проверки их действия мы предлагаем через услугу подписания также услугу временной метки.
- **Мы сохраняем** необходимые для подписания технические компоненты на уровне, соответствующем современным требованиям.

УСЛУГА СОГЛАСИЯ RIA открывает экономику данных

Чтобы государство могло существовать как государство, требуются данные. Государству нужно знать, кто является его гражданином, где он живет, какую зарплату получает, сколько у него детей и принадлежит ли ему какой-либо участок земли или транспортное средство. От этого зависит, кто сколько платит налогов и в каком объеме получает от государства блага.

ПОЧЕМУ НУЖНА УСЛУГА СОГЛАСИЯ?

У государства имеется множество данных о здоровье, которые находятся в разных государственных базах данных, но представляют интерес также для других. Например, если человек соглашается на передачу своих данных о здоровье страховому предприятию, то он может получить полис страхования жизни по более низкой цене.

Уже не за горами и эпоха персональной медицины, когда для выписывания правильного лекарства будут использоваться наши генные данные и медицинская история. Чтобы необходимые данные могли по разрешению человека двигаться между разными участниками, как раз и нужна услуга согласия. При этом важно знать, что согласие, какие данные и кому передаются, дает сам человек. Аналогично этому он может в любой момент отозвать согласие и прекратить передачу информации.

Толчок для создания услуги согласия дала сфера здравоохранения, но этому способствует также Общий регламент по защите данных Европейского союза (GDPR), который расширяет контроль человека над своими данными.

ВАЖНАЯ ВЕХА

В декабре 2019 года мы показали партнерам публичного и частного сектора прототип услуги согласия и спросили у них отзывы. Мы получили подтверждение, что услуга была ожидаемой во всех отношениях и вызывает большой интерес в том числе за пределами сектора здравоохранения. Мы продолжаем разработку услуги, осознавая, что из нее сформируется универсальное решение с широким применением, входящее в ИТ-инфраструктуру государства.

Параллельно разработкам министерство социальных дел проводит анализ влияний, который оценивает воздействия, сопутствующие передаче данных о здоровье. Наряду с добавляющимися возможностями современный подход к передаче персональных данных таит в себе также определенные риски, которые следует четко описать и естественным образом сводить к минимуму.

МЫ ПРОДОЛЖАЕМ РАЗРАБОТКУ УСЛУГИ, ОСОЗНАВАЯ, ЧТО ИЗ НЕЕ СФОРМИРУЕТСЯ УНИВЕРСАЛЬНОЕ РЕШЕНИЕ С ШИРОКИМ ПРИМЕНЕНИЕМ, ВХОДЯЩЕЕ В ИТ-ИНФРАСТРУКТУРУ ГОСУДАРСТВА.

НАЧИНАЕМ СО ЗДРАВООХРАНЕНИЯ

Партнерами RIA в разработке услуги согласия наряду с министерством социальных дел являются Центр информационных систем здоровья и благополучия (TEHIK) и Больничная касса, в ведение которых находятся огромные массивы данных, содержащие информацию о здоровье. Также к участию в проекте привлечены различные поставщики услуг частного

Как работает **УСЛУГА СОГЛАСИЯ**?

сектора, многие из которых могли бы стать будущими пользователями услуги согласия.

Услуга согласия должна появиться в первом квартале 2021 года, за два месяца до запуска ее смогут протестировать ряд избранных пользователей, поставщиков услуг и баз данных.

После основательного анализа влияний, заземления рисков и преодоления трудностей Эстония получит уникальную в мире услугу согласия, поскольку у нашего э-государства имеются превосходные предпосылки для передачи данных от публичного в частный сектор. Это, в свою очередь, создает плодородную почву для рождения новых и уникальных услуг.

Что делает **RIA**?

- **Мы разрабатываем услугу согласия,** с помощью которой люди смогут делиться своими данными, содержащимися в государственных базах данных, с третьими сторонами.
- В декабре 2019 года **мы показали** партнерам публичного и частного сектора прототип услуги согласия. Отзывы были положительные.
- **Услуга согласия** начнет работать в первом квартале 2021 года.

RIHA путеводитель по инфосистеме Эстонской Республики

RIHA – это система администрирования государственной инфосистемой. Она словно путеводитель, благодаря которому мы знаем, что происходит в нашей государственной инфосистеме и на каких основаниях в ней совершаются операции. Без RIHA было бы очень сложно получить обзор, какие данные собирают учреждения. Помимо этого, RIHA помогает вновь использовать уже имеющиеся данные и услуги и тем самым уменьшить дублирование.

ОБНОВЛЯЮЩАЯ СИСТЕМА RIHA ПОМОГАЕТ ОТКРЫТЬ Э-ГОСУДАРСТВО

В Эстонии данные хранятся рассредоточено, то есть не существует одной центральной супербазы данных. У рассредоточения имеется много преимуществ, но оно несет также вызовы, поскольку данные распределены по всей стране. RIHA, конечно, дает сейчас обзор государственных инфосистем Эстонии, но целостная картина могла бы быть современнее и качественнее.

Для достижения этого мы хотим использовать в RIHA единые протоколы и стандарты, автоматизировать передачу метаданных из баз данных в RIHA. Это помогло бы в «путеводителе» точнее и легче находить, какие данные и услуги имеются у государства и как их можно повторно использовать.

А для этого нужно, чтобы все собственники баз данных использовали для описания собираемых данных, предлагаемых услуг и иных компонентов установленные стандарты. Таким образом, в будущем будет возможно эффективнее повторно использовать данные, уменьшить дублирование и тем самым снизить уровень бюрократии. Следовательно, у государства уменьшится потребность повторно запрашивать у людей и организаций одни и те же данные.

Потенциал и ценность RIHA трудно переоценить. Если мы знаем по возможности точно, какие данные, услуги и повторно используемые последовательности кодов имеются в государстве, то и государство, и частный сектор смогут предлагать совершенно новые услуги. Обновляющаяся система RIHA создает предпосылки, чтобы наше э-государство смогло совершить следующий скачок в развитии.

Из RIHA можно узнать:

- какие инфосистемы формируют государственную инфосистему
- какие данные собираются и обрабатываются и в каких инфосистемах это происходит
- кто является собственником, пользователем и контактным лицом инфосистем
- на каких правовых основаниях держатся инфосистемы и обрабатываются данные
- какие имеются компоненты, обеспечивающие совместные способности инфосистем, и повторно используемые компоненты (файлы XML, классификаторы).

ЧТО ДЕЛАЕТ RIA ДЛЯ ОБНОВЛЕНИЯ RIHA?

Первая система RIHA была практически тетрадью, содержащей информацию о тогдашних инфосистемах Эстонии, но на сегодняшний день она развилась в систему администрирования, которая дает обзор государственной инфосистемы Эстонии. Работа с RIHA продолжается, и в новой версии RIHA мы используем стандарт описания данных, разработкой которого

ДЕПАРТАМЕНТ ЗДОРОВЬЯ:
программное обеспечение для администрирования документами Delta

ЛЯЭНЕМААСКАЯ БОЛЬНИЦА:
подсистема X-tee

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ:
среда э-обслуживания регистра народонаселения

СПАСАТЕЛЬНЫЙ ДЕПАРТАМЕНТ:
служебный интерфейс OIS инфосистемы спасения

ГОСУДАРСТВЕННАЯ КАНЦЕЛЯРИЯ:
подсистема проектной инфосистемы

СИЛЫ ОБОРОНЫ:
портал Сил обороны

КАНЦЕЛЯРИЯ РИЙГИКОГУ:
подсистема VIS

RIHA в цифрах

В RIHA насчитывается
900
АКТИВНЫХ УЧРЕЖДЕНИЙ И ПРЕДПРИЯТИЙ

В RIHA насчитывается свыше
2600
зарегистрированных инфосистем и баз данных.

5
СОГЛАСУЕМЫХ УЧРЕЖДЕНИЙ

В 2019 году было инициировано согласование
24
баз данных и информационных систем

управляет Департамент статистики.

Мы всё больше сотрудничаем с клиентами, чтобы с помощью их отзывов сделать RIHA более удобной в пользовании и соответствующей их ожиданиям. Ведется также работа над анализом рассредоточенной системы RIHA и созданием прототипа.

Что делает **RIA**?

- **Мы управляем** системой администрирования государственной инфосистемы (RIHA).
- **Ведем учет** по государственной инфосистеме.
- **Даем обзор** по государственной инфосистеме (данные, участники, требования).
- **Собираем требования** государственной инфосистемы и позволяем оценить соответствие им.
- **Обеспечиваем посредством** RIHA удобное общение между собственниками и оценщиками инфосистем.

CERT-EE: государственное киберподразделение Эстонии

Когда нет крупного кризиса, рабочие помещения RIA остаются на ночь пустыми. Однако есть одно помещение, где свет и экраны компьютеров никогда не гаснут. В нем располагается отдел по обработке инцидентов службы кибербезопасности RIA (сокращенно CERT-EE), который круглосуточно следит за происходящим в киберпространстве Эстонии и оперативно решает киберинциденты даже посреди ночи.

CERT-EE – это государственная контактная служба Эстонии, с которой общаются аналогичные учреждения других стран, когда нужно сообщить об инцидентах, замеченных в киберпространстве Эстонии. CERT-EE в свою очередь отправляет сообщения группам реагирования на киберинциденты в других странах, а также хостинг-провайдерам и другим поставщикам услуг, если какой-либо замеченный в Эстонии фальшивый сайт продолжает ловить жертв.

ЧТО ТАКОЕ КИБЕРИНЦИДЕНТ?

Согласно Закону о кибербезопасности, киберинцидентом является происходящее в системе событие, которое угрожает или причиняет вред безопасности системы. Наиболее распространенные киберинциденты – переадресация на ложные сайты, прерывание услуги, распространение вредоносных программ и взлом учетных записей пользователей. Киберинцидентами являются также атаки программ-вымогателей, финансовые мошенничества и утечки данных.

Некоторые учреждения и предприятия обязаны сообщать нам об инцидентах (например, государственные учреждения, поставщики жизненно важных услуг или местные самоуправления), но зачастую о них сообщают также предприятия и частные лица, которые делают это из хороших побуждений или желания получить помощь.

Об отсутствии работы можно не беспокоиться, поскольку количество зарегистрированных случаев растет стремительно. Если в 2017 году мы зарегистрировали 10 649 и в 2018 году 17 440 случаев, то в 2019 году их было уже 24 369. Это составляет в среднем 67 сообщений в день или 3 сообщения в час.

Чем больше нас информируют, тем лучший мы имеем обзор и тем эффективнее мы можем защитить киберпространство Эстонии и предупредить опасности.

КАК ЭТО РАБОТАЕТ?

Большинство учреждений публичного сектора подключены к государственной сети. Роль CERT-EE – гарантировать, чтобы эта сеть была чистой, безопасной и защищенной. Для этого мы ведем круглосуточный мониторинг государственной сети, выявляя в ней признаки злонамеренной деятельности. Если мы их находим, то вмешиваемся.

Однако наша деятельность не ограничивается государственной сетью: мы ведем мониторинг также сетей некоторых поставщиков жизненно важных услуг. Для этого мы разработали автоматизированное решение мониторинга сети Suricata4All (S4A). Данная система помогает обнаруживать атаки, вредоносные программы, а в некоторых случаях также уязвимые места и проблемы с конфигурацией.

S4A состоит из центральной системы под управлением CERT-EE и датчиков, которые владельцы сетей могут установить в свои устройства. Центральная система задает датчикам правила, на основе которых можно обнаружить атаки. В соответствии с изменяющейся картиной угроз мы регулярно обновляем эти правила. Датчики в свою очередь отправляют центральной системе сообщения, если обнаружено вредоносное движение. S4A позволяет сохранять, индексировать и анализировать движение в сети.

Услуги CERT-EE

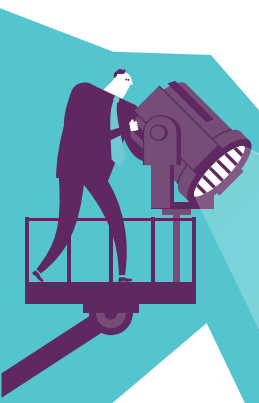
Среда передачи файлов: paste.cert.ee
Рабочий инструмент, с помощью которого можно отправить сомнительные файлы на анализ в CERT-EE. Подходит для передачи объемных журналов записей, фишинговых писем и присланных вместе с ними вкладок, примеров программ-вымогателей и т. п.

«Песочница» CERT-EE: cuckoo.cert.ee
Рабочий инструмент для анализа файлов, предназначенный для ИТ-специалистов. Позволяет в безопасной среде проверять, как операционные системы, работающие на разных виртуальных и физических платформах, ведут себя при запуске сомнительного файла.

Предупреждения и сообщения CERT-EE: twitter.com/cert_ee
Наиболее оперативный способ просмотра сообщений и предупреждений CERT-EE.

Автоматизированное решение мониторинга Suricata4All (S4A)
Решение, состоящее из центральной системы и датчиков, которое помогает обнаруживать атаки и вредоносные программы, а в некоторых случаях также уязвимые места и проблемы с конфигурацией.

Новостная рассылка по кибербезопасности
CERT-EE составляет ежедневную новостную рассылку по кибербезопасности, которая содержит итоги по новостям в сфере кибербезопасности и ИТ, публикуемым в открытых источниках. Для подписки на новостную рассылку отправьте э-письмо с темой «Subscribe» по адресу **certnews@cert.ee.**



Что делает RIA?

- **Мы следим** за ситуацией в сфере информационной безопасности в Эстонии. Для этого мы используем поступающие рапорты и сами собираем информацию о киберинцидентах.
- **Мы помогаем** предотвратить киберинциденты и уменьшить риски безопасности, прежде всего, с помощью повышения осведомленности о безопасности и информирования.
- **Мы оказываем** помощь учреждениям в вопросах по киберинцидентам и консультируем их, если они желают, чтобы правоохранительные органы начали расследование инцидента.
- **Мы организуем** решение кризисных ситуаций. При необходимости мы привлекаем партнеров

CERT-EE в числах

С 2015 года CERT-EE ведет
КРУГЛОСУТОЧНЫЙ
мониторинг происходящего в киберпространстве Эстонии.

В 2019 году в CERT-EE было сообщено о
24 369
СЛУЧАЯХ
в компьютерных сетях и сетях передачи данных Эстонии.

Это составляет в среднем
64 СООБЩЕНИЯ В ДЕНЬ
3 СООБЩЕНИЯ В ЧАС

О ситуации в киберпространстве: 2019 ГОД БЫЛ ГОДОМ ВЫЖИВАНИЯ

На основании сообщений, поступивших в отдел обработки инцидентов – CERT-EERIA – 2019 год можно назвать годом выживания. Конечно, больше всего мы зарегистрировали заражений ботнетами, однако количество известных нам заражений уменьшилось, в то время как количество поддельных веб-сайтов и мошеннических писем почти удвоилось.

ЗЛОУМЫШЛЕННИКИ В БАНКЕ

До 2019 года кибермошенники, чьим любимым трюком была кража денег из банков, жителей Эстонии в основном не беспокоили. Вероятно, причина заключалась в том, что здешние банки используют относительно безопасные способы аутентификации: ID-карту, Mobiil-ID и Smart-ID.

Однако в апреле был найден способ, как используя поддельные сообщения и сайты, создать от имени жертв новые учетные записи Smart-ID. На мобильный телефон пользователей от имени банка присылалось сообщение, которое с виду направляло на страницу входа в интернет-банк. Там жертву направляли войти в систему через Mobiil-ID. Когда жертва вводила на поддельном сайте свой признак пользователя, личный код и PIN-1, злоумышленники начинали одновременно фоном создавать новую учетную запись Smart-ID. После того, как это было сделано, злоумышленники от имени жертвы входили в банк и снимали оттуда деньги.

КРАЖИ ДАННЫХ ПО УЧЕТНЫМ ЗАПИСЯМ

Наряду с мошенническими письмами и поддельными сайтами, созданными для кражи денег, много ущерба причинили также мошеннические кампании, выуживающие данные учетных записей. Простое письмо, которое предупреждает о заполнении объема почтового ящика или просит поменять пароль, может на первый взгляд всего лишь дать злоумышленникам доступ к личным письмам и возможность распространять мошеннические письма дальше. Но зачастую за кражей таких данных учетной записи кроется долгосрочный план – по э-письмам найти деловых партнеров учреждения, вмешаться в переписку и в нужный момент отправить письмо, которое сообщает об изменении банковского счета, предусмотренного для совершения платежей.

В прошлом году мы неоднократно видели такие волны хакерских атак (фишинг), выуживающих данные учетных записей, которые помогла бы предотвратить многоступенчатая аутентификация. Жертвами таких атак стали работники местных самоуправлений, по меньшей мере трех крупнейших в Эстонии университетов, больниц, а также малых учреждений, как например, топливное предприятие и фирма по обслуживанию дорог.

Ликвидацию последствий инцидентов и выяснение масштаба утечки информации зачастую осложняет то, что у групп по инфобезопасности (если они вообще имеются) или у поставщиков услуг отсутствуют необходимые журналы записей, чтобы выяснить, содержание каких учетных записей и в каком объеме было скомпрометировано. Если учреждение желает понять, какого вида информация украдена, то аккуратное ведение журналов записей играет крайне важную роль.

BEC-СХЕМЫ ЖДУТ НОВЫХ ДАННЫХ

Проблемой 2018 года с самым большим влиянием были финансовые мошенничества, инициированные через скомпрометированные учетные записи электронной почты (англ. business email compromise, или BEC-схемы), которые причинили эстонским предприятиям ущерб на сумму не менее 600 000 евро. В 2019 году такие инциденты также находились под нашим вниманием, но, к счастью,

АНАЛИЗИРУЕМ тенденции в киберпространстве

В большей части именно на основании инцидентов, зарегистрированных CERT-EE, отдел по анализу и предупреждению, входящий в состав службы кибербезопасности RIA, анализирует тенденции в киберпространстве Эстонии. На основании поступившей информации отдел составляет недельные, месячные и квартальные обзоры. Также аналитики RIA при необходимости подробнее изучают разные единичные случаи или рассматривают непосредственно какой-либо крупный исследуемый вопрос, стоящий перед RIA. Недавно отдел взял на себя также курирование научно-исследовательской деятельности в сфере кибербезопасности.

мы узнали о существенно меньшем ущербе. По имеющимся у нас данным, наибольшая сумма, которая вследствие мошенничества была перечислена на неправильный банковский счет, составила 112 000 евро. На этот раз благодаря сотрудничеству между банками предприятие смогло вернуть потерянную сумму.

Важно отметить, что BEC-схемы не выбирают жертв, и вследствие выуживания данных по учетной записи может лишиться данных (а потом и денег) любое предприятие Эстонии, ведущее сотрудничество с зарубежными партнерами. В основном жертвами были импортеры каких-либо продуктов (инструменты, шины, промышленное оборудование, медицинская техника и т. д.), и потерянные суммы составляли от нескольких тысяч до 70 000 евро.

Однако наряду с удачными схемами мы слышали о некоторых схемах, которые обнаруживали внимательные бухгалтера или руководители и где ущерба удалось избежать. Также нас информировали о ситуациях, когда деловые партнеры Эстонии в других странах несли ущерб из-за подобных схем. Поэтому важно, чтобы эстонские предприятия, пережившие инцидент утечки данных по учетным записям, информировали своих зарубежных партнеров, которые могут стать следующей целью мошенников.

КОЛИЧЕСТВО ОБРАЩЕНИЙ В RIA ЗА ПОСЛЕДНИЕ ТРИ ГОДА

Инцидентами с влиянием мы считаем те, из-за которых были нарушены конфиденциальность, целостность или доступность информации или систем.
Обращением мы считаем все сообщения об инцидентах с влиянием и без влияния, о замеченных прерываниях в работе услуг, спаме, вопросах к CERT-EE, сводных рапортах партнерских учреждений и т. д.

ПЕРЕБОИ В РАБОТЕ ВАЖНЫХ УСЛУГ

В 2019 году мы написали в ежегоднике по кибербезопасности: «Поддержание кибербезопасности в Эстонии требует постоянной работы и внимания руководителей. Обновления важны, стандарты также, поэтому в обновления и стандарты необходимо инвестировать деньги и время. Чтобы мы могли в Эстонии и в дальнейшем избегать киберинцидентов с большим влиянием, необходимо проделать эту работу».

В 2019 году мы наблюдали в работе услуг существенные перебои, у которых могло бы быть масштабное влияние на жителей Эстонии: ошибка в программном обеспечении в сентябре на 20 минут отключила телефоны центра тревоги; из-за обрыва кабелей государственной сети, на который не обратили внимания, в ноябре несколько часов были недоступны дигирецепты и государственный портал, после этого дигирецепты в декабре были несколько раз недоступными из-за обслуживания устаревших систем. Переход Mobiil-ID на новые системы в мае на 24 часа отключил возможность аутентификации и подписания с помощью этой услуги; также с перебоями работали регистр народонаселения, государственная услуга аутентификации, новая версия X-tee и т. д.

Жители Эстонии настолько привыкли к цифровым услугам, что следует инвестировать в их доступность, проверять их работоспособность, тестировать системы, улучшать процедуры и еще раз тестировать.

Перебои в работе услуг в 2019 году были обусловлены по большей части человеческими ошибками, ошибками администрирования или природными причинами, однако уязвимые системы могут столкнуться со злоумышленниками и угрожающими лицами с государственными связями, которые не заботятся о нашей безопасности и нашем здоровье.

СНОВА ЭТИ БОТНЕТЫ

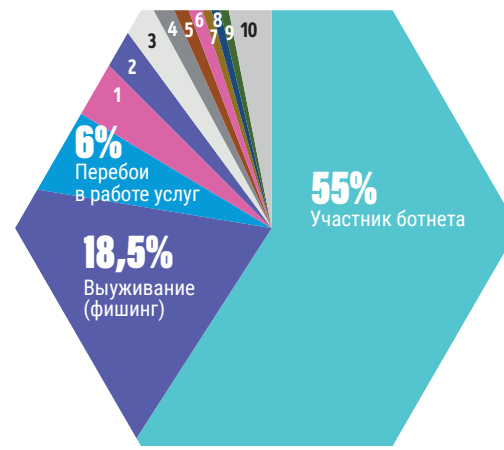
О ботнетах мы писали в предыдущие годы. Причиной большого количества зарегистрированных в прошлом году инцидентов, связанных с вредоносными программами, послужил, например, ботнет Avalanche. Его деятельность была остановлена в результате международной полицейской операции в декабре 2016 года, но вредоносные программы не удаляются из устройств автоматически, и их следует чистить отдельно, чтобы избежать последующего захвата той же инфраструктуры и их запуска для новых атак.

Другая большая часть зараженных устройств подключилась к ботнету Necurs, который использовали много лет, например, в атаках с целью сбоя

Год **ВЫУЖИВАНИЯ**

Удельный вес инцидентов, зарегистрированных в 2019 году, по видам

Инциденты, зарегистрированные CERT-EE. Наибольший удельный вес набрали сообщения о заражении ботнетами. Однако наряду с ними большой скачок совершило число фишинг-мошенничеств (выуживание информации), которое по сравнению с прошлым годом удвоилось.



1 Распространение/хранение вредоносных программ 3,9%
2 Компрометирование: 2,4%
3 Завладение учетной записью: 2,2%
4 Злонамеренная переадресация: 1,2%
5 Финансовое мошенничество: 0,9%
6 Программы-вымогатели: 0,9%
7 Добывание криптовалюты: 0,6% | **8 Утечка данных: 0,6%**
9 Атака с целью сбоя в работе услуг: 0,6% | **10 Иное: 3,1%**

в работе услуг, для распространения вредоносных программ (например, для кражи банковских данных), отправки спама и т. д. В марте 2020 года Microsoft сообщил о взятии сети под свой контроль. Несмотря на это, многие устройства в Эстонии еще заражены, но не представляют такой большой опасности для других.

В Эстонии имеется еще множество устройств, которые подключились к какому-либо ботнету, но управляющие серверы которых не находятся под контролем учреждений правопорядка и о которых мы не получаем регулярной информации. Все устройства «интернета вещей» (IoT), у которых не было обновлено программное обеспечение или не изменен пароль администратора по умолчанию, могут оказаться участниками подобных сетей и без ведома владельца отправлять подобные мошеннические письма или письма с вредоносными программами, которые в прошлом году причинили так много неприятностей.

Эстония получает новый СТАНДАРТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Все мы хотим, чтобы вода, которую мы пьем, еда, которую мы едим, и здания, в которых мы живем, соответствовали требованиям безопасности и качества. С точки зрения функционирования э-государства, информационные системы и передаваемые по ним данные настолько же важны, и поэтому мы должны гарантировать, чтобы эти системы были созданы и защищены таким способом, который обеспечивал бы их надежность и безопасность данных.

Информационная и сетевая безопасность государственных учреждений и местных самоуправлений должна быть выстроена в соответствии с установленными требованиями. Задача RIA – проверять выполнение этих требований. Помимо этого, мы осуществляем надзор над поставщиками жизненно важных услуг, то есть над энергетическими предприятиями, предприятиями водоснабжения, банками, телекоммуникационными фирмами и т. д.

ЧТО ТАКОЕ ISKE?

Конкретные требования и инструкции собраны в стандарт мер безопасности информационных систем (ISKE). В нем приведены три уровня безопасности: низкий (L), средний (M) и высокий (H). ISKE должны применять все государственные учреждения и местные самоуправления, которые являются ответственными обработчиками какой-либо базы данных.

RIA консультирует разработчиков и помогает им: мы делимся инструкционными материалами, организуем учебные курсы и отвечаем на вопросы. Мы создали портал ISKE (iske.ria.ee), где доступна вся необходимая информация. В то же время следует помнить, что RIA не применяет меры информационной безопасности за другие учреждения.

Сегодня уровень применения ISKE в государственных учреждениях в целом хороший. В большинстве из них аудиторские проверки проводились уже несколько раз, и существенных недостатков, как правило, нет. Местные самоуправления не обязаны проводить аудиторские проверки. В основном фокусе отдела стандартов и надзора RIA в 2019 году как раз и были местные самоуправления.

ЧТО ЖДЕТ В БУДУЩЕМ?

Сейчас согласно постановлению по ISKE, принятому на основании Закона о публичной информации, ISKE является единственным одобренным набором требований. В ближайшее время планируется добавить к нему также международно признанный и распространенный стандарт инфобезопасности ISO 27001. Многие учреждения проявили интерес к его применению.

Параллельно ведется разработка нового эстонского стандарта информационной безопасности. Новый стандарт содержит больше приближений на основе рисков и в будущем заменит ISKE. Новый стандарт не такой объемный и для пользователя более простой и гибкий, учитывает размер, особенности и возможности разных учреждений.

Что делает RIA?

- **Мы оказываем помощь и консультируем** при применении системы трехуровневой эталонной безопасности инфосистем ISKE.
- **Контролируем применение мер безопасности** в инфосистемах государственных учреждений и учреждений местных самоуправлений, поставщиков существенных и жизненно важных услуг, услуг связи, услуг доверия и цифровых услуг.
- Обновляем и дополняем применяемые требования в соответствии с изменившимися опасностями и окружающей обстановкой.

ПРОФИЛАКТИЧЕСКИЕ КАМПАНИИ против киберопасностей

Одной из важнейших задач группы по анализу и профилактики из службы кибербезопасности RIA является профилактическая деятельность. Из них наиболее яркими являются направленные на общественность информационные кампании, цель которых – ознакомить с возможными рисками в области кибербезопасности и предложить решения для их преодоления.

ПРОБЛЕМЫ ПОЖИЛЫХ ЛЮДЕЙ

RIA организует информационные кампании уже много лет. Например, кампания Nuti-Mati, проведенная в 2016 году вместе с целевым учреждением Vaata Maailma («Посмотри мир»), обращала внимание на безопасность смарт-устройств. В 2013 году с помощью кампаний мы попытались уменьшить число пользователей устаревшей операционной системы Windows XP.

Теперь пришло время рассмотреть информационную деятельность систематически. Используя результаты исследований Департамента статистики, Eurostat и других исследований, мы постарались точнее определить целевую группу информационных кампаний. Из исследований четко выделилась группа, у которой кибергигиена была неважной, но на которую в части кибербезопасности не обращали так много внимания – это пожилые жители.

Например, на молодых интернет-пользователей Союз защиты детей, Департамент полиции и погранохраны, а также несколько министерств вместе с ведомствами своей административной сферы в течение нескольких лет обращали довольно пристальное внимание. При этом пожилые люди должны были сами учиться и преодолевать трудности в меняющемся киберпространстве.

В связи с этим во второй половине 2019 года, делая акцент на базовые знания по кибергигиене, мы организовали информационную кампанию, основной целевой группой которой были жители в возрасте от 55 лет и старше. Наш медиапартнер Havas создал запоминающееся послание «Будь осмотрИТельным» («Ole IT-vaatlik») и организовал теле-, радио-, наружную и интернет-рекламу, которая осенью 2019 года хорошо бросалась в глаза благодаря сине-белому контрасту и оформлению в стиле ретро.

НА ПОМОЩЬ ПРИХОДЯТ БИБЛИОТЕКИ

В ходе кампании мы вели сотрудничество также с Союзом библиотекарей. На инфодне, состоявшемся в ноябре, у людей в разных уголках Эстонии была возможность прийти с вопросами по кибербезопасности в свою местную библиотеку и спросить совета. В инфодне приняли участие свыше ста библиотек, одной из целей которых было подчеркнуть послание, что местная библиотека как раз могла бы стать местом, где можно в дальнейшем получать помощь в части безопасности своих смарт-устройств.

Через рекламу и PR-деятельность сообщения кампании достигли по меньшей мере 80% целевой группы. Последовавшее затем исследование показало, что более четверти людей, видевших рекламу нашей кампании, осведомлялись о кибербезопасности дополнительно или сделали хотя бы один шаг, чтобы обеспечить для себя или близких более высокий уровень безопасности/приватности в интернете.

С одной стороны, кампанией для пожилых людей мы желали подчеркнуть важность кибербезопасности, с другой стороны – мы побуждали об-

ОТЦЫ И ДЕТИ

48% **людей в возрасте от 15 до 24 лет** использует в разных местах разные пароли

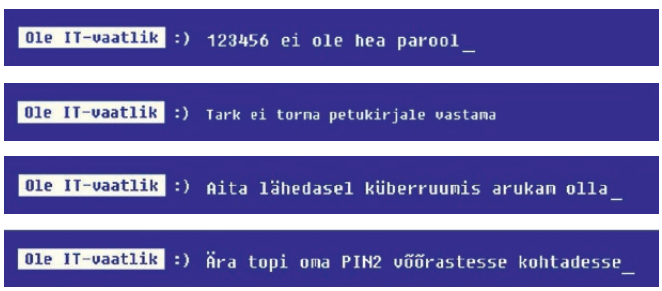
11% **людей в возрасте от 55 и старше** использует в разных местах разные пароли

Источник: Евробарометр 2017

БИБЛИОТЕКИ ПРИХОДЯТ НА ПОМОЩЬ: на инфодне, состоявшемся в ноябре, люди могли прийти в местную библиотеку с вопросами по кибербезопасности и спросить совета.

Что делает **RIA**?

- **Мы повышаем** уровень кибергигиены в Эстонии.
- **Проводим** информационные и профилактические кампании. В прошлом году в фокусе находились пожилые люди, в этом году – предприниматели.
- **Мы предлагаем** работникам публичного сектора и семейным врачам тест по кибергигиене и учебную среду DigiTest.



щественность помогать своим пожилым друзьям и родственникам, чтобы они умели безопаснее вести себя в киберпространстве.

СЛЕДУЮЩАЯ КАМПАНИЯ НАПРАВЛЕНА НА ПРЕДПРИНИМАТЕЛЕЙ

В 2020 году с информационной деятельностью мы движемся дальше, прежде всего, в направлении малых и средних предприятий. Именно на них болезненнее всего влияют перебои в работе услуг, атаки программ-вымогателей и финансовые мошенничества, организованные через компрометацию учетных записей электронной почты. Чем больше у предпринимателей будет знаний о возможных киберопасностях, тем лучше они смогут заказывать ИТ-услуги и защитить свое предприятие от киберрисков.

В то же время мы продолжаем измерение практик кибергигиены, чтобы следующие кампании были нацелены еще лучше. После осмотрИТельной кампании 2019 года мы спросили у жителей Эстонии, какие практики по кибербезопасности они соблюдают, а в 2020 году мы проведем подобное исследование среди предпринимателей.

Всё это дает лучшую картину того, как мы можем предупредить в Эстонии киберинциденты с большим влиянием.

Кампания ОсмотрИ-Тельности в числах

400 000
ПРОСМОТРОВ
в Facebook и Youtube набрал видеоклип об осмотрИТельности

16
БИБЛИОТЕК
пригласили ноября 2019 года пожилых людей спросить совета по кибербезопасности

16 МЛН
ПРОСМОТРОВ
на интернет-платформах набрал рекламный баннер осмотрИТельности

НАДЕЕМСЯ НА ЛУЧШЕЕ, готовимся к худшему

В 2015 году перед Рождеством 230 000 человек в Ивано-Франковской области (Западная Украина) остались без электричества. На этот раз причиной перебоев были не банальные причины, а, насколько известно, первая успешная кибератака на электрические системы.

В мае 2017 года государственные услуги здравоохранения Великобритании были вынуждены отменить 19 000 приемов пациентов. Причина: вследствие программы-вымогателя WannaCry в больницах вышло из строя огромное число компьютеров.

ВСЁ БОЛЬШЕ ЗАВИСИМ ОТ ИТ

Наше благополучие, безопасность и жизненно важные услуги всё больше зависят от инфотехнологии, и поэтому ее надежность и защита особенно важны. Как подтверждает случившееся в Украине и Великобритании, атака на ИТ-системы может быстро и болезненно ударить по физическому миру.

НА ЭТОТ РАЗ ПРИЧИНОЙ ПЕРЕБОЕВ БЫЛИ НЕ БАНАЛЬНЫЕ ПРИЧИНЫ, А, НАСКОЛЬКО ИЗВЕСТНО, ПЕРВАЯ УСПЕШНАЯ КИБЕРАТАКА НА ЭЛЕКТРИЧЕСКИЕ СИСТЕМЫ.

Во имя того, чтобы инфосистемы поставщиков жизненно важных и существенных услуг Эстонии были менее уязвимы атакам, чтобы знать, как вести себя при атаке, а влияния возможных инцидентов были сведены к минимуму, в RIA работает отдел защиты инфраструктуры критической информации (KIIK).

ЧТО ЭТО ТАКОЕ?

Критическая инфраструктура – это обеспечение, система или их часть, которая крайне необходима для совершения жизненно важных общественных действий. Например, для функционирования здравоохранения, безопасности, защиты, экономического и социального обеспечения людей.

Инфраструктура критической информации – это сетевые и информационные системы, от работы, надежности и безопасности которых зависит функционирование критической инфраструктуры. Если такие системы получают повреждения или уничтожаются, то это существенно влияет на всё государство.

RIA организует защиту инфраструктуры критической информации, в том числе мы составляем анализы рисков экстренной ситуации, обусловленной киберинцидентом, разрабатываем необходимые меры безопасности, организуем тестирования уровней безопасности и консультируем поставщиков жизненно важных и существенных услуг по предупреждению и решению кризисов.

Под управлением RIA регулярно составляется анализ рисков экстренной ситуации, обусловленной масштабным киберинцидентом. В нем мы оцениваем вероятность возникновения экстренной ситуации и ее последствия, а также разрабатываем меры, как избежать экстренной ситуации, или если этого не удается, то как смягчить последствия.

В 2020 году мы фокусируемся на энергетике и медицине. Начинаем учебные курсы для семейных врачей, чьи ИТ-системы должны с 2022 года соот-

В 2019 ГОДУ мы организовали самостоятельно или помогли организовать **10 УЧЕНИЙ**

ветствовать требованиям, установленным Законом о кибербезопасности. Для людей, отвечающих за кибербезопасность энергетических предприятий, мы организуем учения, чтобы они могли поупражняться в решении киберинцидента с большим влиянием.

ТЯЖЕЛО В УЧЕНИИ – ЛЕГКО В БОЮ

Организация учений является нашей повседневной работой. Здесь приведены некоторые примеры.

В марте прошлого года вместе с финскими коллегами мы упражнялись, как отразить атаку программы-вымогателя, которой подверглись энергетические предприятия. В апреле мы координировали участие Эстонии в крупнейших в мире международных учениях по киберзащите Locked Shields. Мы помогли подготовить и участвовали в майских учениях НАТО по управлению кризисом CMX2019, в сценарий которых были вписаны кибератаки. Мы принимали участие в организации учений по киберзащите руководства сил развития НАТО CyberCoalition 2019, состоявшихся в Тарту.

Помимо этого, ежегодно во время крупных весенних учений Сил обороны мы организуем учения «Кибершторм», в которых отрабатываем навыки сотрудничества гражданских и военных сил при решении киберинцидента. В 2019 году в рамках таких учений мы смоделировали и решили инциденты в энергетическом секторе. В 2020 году планируется привлечь сферу телекоммуникаций.

Помимо этого, в 2020 году пройдут европейские киберучения CyberEurope, организатором которых от Эстонии является RIA. Если в ходе прошлых учений CyberEurope в 2018 году были разыграны киберинциденты в авиации, то на этот раз в фокусе находятся учреждения здравоохранения.

Чем больше учений и чем они сложнее, тем проще будет в реальной кризисной ситуации. Хотя мы надеемся, что нам никогда не понадобится приобретенное в ходе учений, однако мы должны быть готовы к возможным критическим ситуациям, когда на учения уже не будет времени.

Что делает RIA?

- **Мы собираем информацию** по инфраструктуре критической информации и **управляем** ею.
- **Составляем обзоры** по рискам инфраструктуры критической информации.
- **Разрабатываем меры безопасности**, инструкции и материалы с примерами.
- **Консультируем поставщиков жизненно важных услуг** в вопросах предупреждения и решения кризисов.
- **Организуем** местные и международные учения.
- **Повышаем** осведомленность о кибербезопасности.

было проведено **14** учебных курсов в **2020** году запланировано **40** курсов по повышению осведомленности об информационной безопасности.

мы фокусируемся на **ЭНЕРГЕТИКЕ** и **ЗДРАВООХРАНЕНИИ**.

ВНЕШНИЕ ОТНОШЕНИЯ RIA: 150 делегаций в год

Помимо того, что RIA собирает информацию и делится ей в Эстонии, мы очень активные также во внешних отношениях. С одной стороны, мы заинтересованы вести сотрудничество с государствами-партнерами, а с другой стороны представители многих государств желают посетить RIA, чтобы получить вдохновение и информацию о том, как наше э-государство работает. Гости хотят своими глазами увидеть, как построено государство, где людям не нужно приходить в учреждения и стоять в очереди в комнатах ожидания. В большинстве стран этого еще нет.

2019 ГОД БЫЛ РЕКОРДНЫМ

В 2019 году RIA посетили 150 иностранных делегаций, что является рекордом. Наиболее экзотическими и далекими странами, откуда прибыли делегации, были Бруней, Камбоджа, Аруба, Шри-Ланка, страны Карибского бассейна, Австралия, Таиланд, Руанда, Эсватини, многие страны Латинской Америки и другие. По числу гостей в первой тройке стран были Япония, Германия и США.

Прием такого большого числа гостей стал одновременно вкладом RIA при подаче заявки в Совет безопасности ООН в кампании Эстонкой Республики, длившейся несколько лет и успешно достигшей своей кульминации.

Время от времени мы принимаем в RIA гостей очень высокого уровня. С визитом у нас побывали премьер-министры, министры и вице-министры ИКТ многих стран, а также коронованные персоны. Основной интерес гостей направлен на получение из первоисточника информации о строении и повседневном управлении э-государства. В RIA они получают обзор базовых элементов государственной инфосистемы, а также информацию о том, как защитить э-государство от кибероопасностей.

Из посещающих иностранных гостей основную часть составляют представители правительственных учреждений других стран. Многие из них находились с визитом в Эстонии уже второй или третий раз. Если в первый раз гости посещают представительский центр э-Эстонии, то в следующий раз они желают уже серьезнее углубиться в конкретную тему. Для этого они как раз и приезжают в RIA и встречаются с представителями предприятий, которые в качестве государственных партнеров принимали участие в строительстве цифровой среды. Также нас посещают студенты и частный сектор.

ЧТО ИНТЕРЕСУЕТ ГОСТЕЙ?

Для гостей наибольший интерес представляет тема обмена данными. Очевидно, что большинство стран мира ищет решение, которое позволило бы безопасно обмениваться данными между учреждениями (и частным сектором). Эстонский X-tee работает уже 18 лет и может предложить вдохновение другим странам в достижении своего решения.

По рейтингу тематик далее следуют электронная идентификация и цифровая подпись, а четвертое место занимает кибербезопасность, формирующаяся в отдельную тему.

КАКИЕ СТРАНЫ ПОСЕЩАЕМ МЫ САМИ?

Помимо приема гостей эксперты RIA также сами посещают зарубежные страны. Мы ведем переговоры, выступаем с докладами и учимся.

Ежегодно мы организуем 5-6 содержательных двухсторонних встреч с основными странами-партнерами, чтобы обсудить темы, представляющие интерес для обеих сторон. На таких встречах мы выясняем и при возможности согласовываем свои точки зрения в вопросах, которые являются темой в рабочих группах Европейского союза. RIA ведет тесное сотрудничество также с Департаментом сетевой и информационной безопасности Европейского союза ENIS.

В 2019 году специалисты RIA выступали с докладами в разных местах мира почти 25 раз: несколько раз в Австралии, Сингапуре, Америке, арабских странах и странах Европы. Это дает возможность представлять Эстонию и одновременно помогает открывать двери для частного сектора.

В то же время наши представители всегда учатся чему-то новому, слушая других и проводя встречи. При разработке и защите эстонского э-государства нужно быть в курсе решений, и здесь на пользу пойдет по возможности широкая сеть контактов.

ДАЛЕКИЕ ГОСТИ:
В сентябре 2019 года RIA посетила министр по цифровым вопросам Абу-Даби доктор Рауда Аль-Саад, которую приветствовала руководитель по международным отношениям Пирет Урб.

В 2019 году RIA посетили

150

иностранных делегаций

в 2018 году

96

ПОЧТИ

25 РАЗ

работники RIA выступали с докладами в зарубежных странах: несколько раз в Австралии, Сингапуре, Америке, арабских странах и странах Европы.

Что делает **RIA**?

- **Мы формируем** в своих внешних отношениях репутацию Эстонского цифрового государства.
- **Получаем** новые знания и контакты, которые могли бы пойти на пользу при развитии и защите нашего э-государства.
- **Организуем** двухсторонние встречи с основными государствами-партнерами.

По числу гостей в первой тройке стран были **ЯПОНИЯ**, **ГЕРМАНИЯ** и **США**.Наибольший интерес для гостей представляют темы обмена данными, электронной идентификации и кибербезопасности.

Наиболее экзотическими и далекими странами, откуда прибыли делегации, были **Бруней, Камбоджа, Аруба, Шри-Ланка, страны Карибского бассейна, Австралия, Таиланд, Руанда, Эсватини.**

МЕЖДУНАРОДНЫЕ проекты RIA

Для RIA очень важны также международные проекты, поскольку они помогают сохранять позитивный имидж Эстонии и повысить уровень кибербезопасности во всем мире. Также они дают нашим работникам хорошую возможность опробовать свои умения наставника, находить по всему миру рабочие контакты и делиться лучшими знаниями и опытом с другими странами. В настоящий момент в RIA ведется работа над тремя международными проектами: EU CyberNet, Cyber4Dev и Interreg Europe CYBER.

ЧТО ТАКОЕ EU CYBERNET?

EU CyberNet – это новая инициатива Европейского союза. Будучи крупнейшим в мире союзом, оказывающим помощь в целях развития, Европейский союз (ЕС) поставил перед собой цель сосредоточить свою помощь третьим странам на вопросах оцифровки и киберзащиты, развития сотрудничества между киберэкспертами государств-членов и развития их профессиональных навыков.

В рамках проекта создается общеевропейская сеть экспертов по кибербезопасности, которую государства-члены и институты ЕС смогут использовать для реализации проектов помощи в области кибербезопасности в третьих странах.

Почему успех таких проектов важен для ЕС? Потому что кибербезопасность в Европе образно начинается как с осведомленности каждого европейца, так и с нашей способности работать с экспертами по кибербезопасности за пределами Европы.

Весной 2019 года для создания сети Европейская Комиссия объявила международный конкурс. Победителем стало предложение международного консорциума во главе с RIA (Эстония, Германия, Люксембург и Финляндия). Команда EU CyberNet находится в структуре RIA и координирует все проекты по кибербезопасности в третьих странах, организованные Европейским союзом, а также оказывает посредничество в работе экспертов.

Что делает проект EU CyberNet значимым как для RIA, так и для Эстонии в целом, так это то, что мы играем ведущую роль в реализации этого проекта. Именно RIA, как договорный партнер DG DEVCO в Генеральном директорате по развитию Европейской Комиссии, отвечает за реализацию проекта с участием всего европейского сообщества кибербезопасности.

Ожидания институтов ЕС и государств-членов высоки, поскольку сектор нуждается в лучшей координации и более последовательном подходе. Наладить его работу – большой вызов, но мы, безусловно, способны достойно с этим справиться.

EU CyberNet

По окончании проекта сетью должно быть охвачено более 500 экспертов и 150 партнерских учреждений, начиная от государственных киберцентров и заканчивая университетами и аналитическими центрами. Мы разработали коммуникационную стратегию, создается веб-страница, объединяющая экспертов. Состоялись первые тренинги по EU CyberNet и командирование эксперта в миссию.

ПРОДОЛЖИТЕЛЬНОСТЬ ПРОЕКТА: 1 сентября 2019 г. – 31 августа 2023 г.

ОБЩИЙ БЮДЖЕТ ПРОЕКТА: 4 миллиона евро

ЧТО ТАКОЕ CYBER4DEV?

Европейский проект по оказанию помощи в развитии EU Cyber Resilience for Development Project, или Cyber4Dev, является международным проектом под руководством Эстонии, Нидерландов и Великобритании, в котором Эстония вместе со своими экспертами является самым весомым вкладчиком. Цель этого проекта – увеличить с помощью учебных программ кибербезопасность в странах Африки, Азии, Латинской Америки и Карибского региона. В ходе проекта участникам оказывается помощь в составлении и реализации стратегий по кибербезопасности, повышается работоспособность рабочих групп в работе с киберинцидентами (CERT) и поддерживается региональное и международное сотрудничество.

В 2019 году Cyber4Dev организовал в целевых

В 2019 году в рамках проекта Cyber4Dev состоялось 48 мероприятий, где участвовало в общей сложности 28 экспертов и свыше 400 лекторов. Помимо этого, было поддержано участие экспертов из 25 целевых стран на международных специальных форумах в Европе.
ПРОДОЛЖИТЕЛЬНОСТЬ ПРОЕКТА: 1 января 2018 г. – 30 июня 2021 г.
ОБЩИЙ БЮДЖЕТ ПРОЕКТА: 11 миллионов евро
ВЕБ-СТРАНИЦА ПРОЕКТА: cyber4dev.eu

странах учебные семинары и визиты для разных групп, начиная от политиков и заканчивая техниками. В ходе проекта было поддержано создание CERT в Ботсване, а также развитие возможности управления инцидентами CERT в Шри-Ланке, была оказана помощь центру кибербезопасности в Руанде в составлении первой государственной киберстратегии, были предоставлены консультации составителям закона о кибербезопасности и разработчикам eID в Шри-Ланке, проведены учебные курсы для многих групп CERT в странах Африки на тему управления инцидентами и организованы первые государственные учения по кибербезопасности на Маврикии.

В прошлом году географический охват проекта расширился: помимо стран Африки и Азии началась деятельность в Латинской Америке и на Карибских островах. У RIA уже имеется многолетний опыт сотрудничества с этим регионом благодаря Организации американских государств (OAS), которая часто приглашала экспертов из Эстонии для проведения своих учебных курсов. Опыт Эстонии в строительстве безопасного цифрового государства известен и ценится во всем мире.

ЧТО ТАКОЕ INTERREG EUROPE CYBER?

Interreg Europe CYBER – проект, финансируемый Европейским фондом регионального развития, цель которого – поддержать конкурентоспособность малых и средних предприятий в сфере кибербезопасности. В проекте участвует семь стран: Франция (ведущий партнер), Эстония, Италия, Испания, Бельгия, Словакия и Словения.

В Эстонии с этим проектом развиваются предпринимательство и инновация в сфере кибербезопасности. Для этого разрабатываются политические инструменты, ведется государственное сотрудничество и организуются международные консультации с партнерами проекта. У эстонских

ЛИЙНА АРЕНГ

руководитель проекта Cyber4Dev

Работая для Cyber4Dev, я восторгаюсь больше всего тем, насколько старательны участники наших курсов. Они полны желания учиться, задавать вопросы и принимать новые вызовы. В ходе проекта мы делимся прежде всего знаниями Эстонии и опытом Европейского союза, и я верю, что и мы сами также узнаем много нового. В целевых странах нашего проекта идет стремительный переход на цифровые технологии. Во многих сферах они продвигаются вперед большими шагами, используя новейшие цифровые платформы, экспериментируя в финансовой и мобильной технологии, используя не подключенные к центральной сети решения возобновляемой энергии и поддерживая создание отечественных предприятий.

Цель Cyber4Dev – повысить осведомленность как в обществе, так и среди политически значимых лиц, желающих с большим рвением пожинать плоды «цифровой революции». Мы помогаем им понять, насколько важно инвестировать в безопасность цифровых решений, чтобы они выдерживали потенциальные кибератаки, и чтобы государство могло скоординированно реагировать на киберинциденты и быстро после них восстанавливаться.

предприятий открывается возможность налаживать отношения со странами-партнерами и их предприятиями, а у RIA возникает лучшее понимание, как поддерживать инновацию. Цель проекта – смотреть прямо на экосистему кибербезопасности Эстонии, определить имеющихся партнеров, найти в экосистеме проблемные места и систематически ими заниматься.

В результате проекта готовятся анализы для международного расширения и сотрудничества малых и средних предприятий, и по этой же теме предлагаются консультации.

ПРОДОЛЖИТЕЛЬНОСТЬ ПРОЕКТА:
1 июня 2018 г. – 31 мая 2023 г.
ОБЩИЙ БЮДЖЕТ ПРОЕКТА: 1 864 242 евро
ВЕБ-СТРАНИЦА ПРОЕКТА: www.interregeurope.eu/CYBER

RIA: ЦИФРЫ И ЛЮДИ

RIA является государственным центром компетенции, который формирует и укрепляет основы информационного общества Эстонии: мы развиваем и управляем сосредоточенными на э-государстве инфраструктурными службами и обеспечиваем кибербезопасность страны. Вместе мы создаем и защищаем лучшее в мире цифровое общество.

Мы договорились об общих ценностях, которые считаем важными и которые используем в своем поведении и решениях:

- **мы берем на себя ответственность:** мы создаем лучшее цифровое государство, которое создает новые возможности для людей и общества, мы осознаем свою роль в организации и знаем, как наша работа влияет на конечный результат;
- **мы учимся и делимся:** в постоянно развивающемся цифровом обществе мы как в качестве организации, так и в качестве сотрудников должны быть в состоянии развиваться и быть открытыми;
- **мы работаем вместе:** для достижения результатов нам нужны единство, взаимопонимание и поддержка, а также приверженность общей цели.

КОЛЛЕКТИВ RIA в цифрах

61% работников RIA МУЖЧИНЫ ...

... и 39% ЖЕНЩИНЫ

В RIA работают люди в возрасте от 18 до 68 ЛЕТ

... 72% из них имеют высшее образование

В 2019 году работники RIA прошли в общей сложности 6426 ЧАСОВ ОБУЧЕНИЯ

2019 году средняя численность сотрудников RIA составляла 141 ЧЕЛОВЕК

Общая текучесть кадров составила 22%

СРЕДНИЙ СОТРУДНИК RIA – ЭТО 37-ЛЕТНИЙ МУЖЧИНА, ПРОРАБОТАВШИЙ В RIA 3,6 ГОДА.

По состоянию на 16.03.2020 г. средняя зарплата брутто в RIA составляла 2539 евро.

В 2019 году RIA осуществил инвестиции на сумму 4,1 млн евро

Объем управленческих расходов RIA составил 5,2 млн евро.

СТРУКТУРА Департамента государственной инфосистемы

Сотрудники RIA о RIA

ТАРМО ХАНГА

Руководитель технологического отдела

Работает в RIA более десяти лет

В RIA я научился идти на компромиссы и поддерживать здоровое отношение к жизни. У работников ИТ-индустрии, как правило, достаточно высокий уровень общего стресса, поэтому я научился справляться с ним, чтобы продолжать получать удовольствие. На работу нужно приходить счастливым, полным энтузиазма, а не с неохотой. По-прежнему ли интересно работать в RIA по прошествии десяти лет? Я оцениваю свою работу по тому, что мне не должно быть скучно, и в работе должно быть порядком вызовов. Должно складываться ощущение, что ты смог сделать что-то важное для Эстонии и мира информационных технологий. В RIA эти условия соблюдены.

СЕЙКО КУЙК

пресс-секретарь

Работает в RIA один год

В RIA интересные темы и интересные люди. Будучи сторонним наблюдателем, я и предположить не мог, насколько важную роль играет RIA в поддержании и развитии работы э-государства. Здесь имеется возможность внести свой вклад в выводе э-государства на новый уровень. Все сотрудники способствуют этому.

КЯТЛИН ПИРК

главный специалист офисного управления

Работает в RIA два года

За всё время моей работы в RIA мне ни разу не доводилось чувствовать скуку. Каждый день приносит разные задачи и вызовы, новые знакомства и знания. RIA дал мне огромный багаж опыта. Я приобрела здесь уверенность в себе и смелость заниматься новыми для себя вещами. При поддержке коллег и начальства я могу постоянно развиваться и, будучи вспомогательным звеном, вносить свой небольшой вклад в создание лучшего электронного государства.

МАРГУС АРМ

Заместитель генерального директора по государственной инфосистеме

Работает в RIA три с половиной года

Я пришел в RIA в сентябре 2016 года из частного сектора на должность руководителя сферы eID. Исходя из своего опыта работы в RIA, я могу сказать, что здесь невероятно круто. При всем моем уважении к своим предыдущим работодателям, я осмелюсь сказать, что так увлекательно и интересно мне не было ни в одном месте работы. Здесь каждый день появляются новые и захватывающие задачи, которые влияют на работу практически всей электронной Эстонии. Постоянный контакт с очень приятными, энергичными и ответственными коллегами как из RIA, так и из других учреждений вселяет желание и силы стремиться к тому, чтобы в Эстонии всем было лучше, чтобы мы оставались ведущим электронным государством.

АННИКА КЛУГЕ

руководитель проекта отдела eIDt

Работает в RIA четыре года

Мне нравится, что в RIA я могу сама выбирать время и место работы – конечно же, в разумных границах, чтобы можно было проводить собрания! Я чувствую, что мне доверяют и у меня есть право голоса в принятии решений. Здесь работают готовые к сотрудничеству и невероятно крутые люди, а работа поражает своим разнообразием. Я чувствую себя полезной.

ЛИЙНА АРЕНГ

руководитель проекта Cyber4Dev

Работает в RIA более пяти лет

На мой взгляд, RIA является самым потрясающим учреждением для работы в Эстонии. Различные подразделения RIA тесно сотрудничают друг с другом, поскольку стремятся к общей цели. Мне нравится, что в RIA люди всегда находят способы поддержать реализацию идеи, а не ищут бюрократические оправдания, чтобы воспрепятствовать этому.

МЫ ВМЕСТЕ ФОРМИРУЕМ И ЗАЩИЩАЕМ ЛУЧШЕЕ В МИРЕ ЦИФРОВОЕ ОБЩЕСТВО. ЕСЛИ ВЫ ХОТИТЕ ПРИСОЕДИНИТЬСЯ К RIA, ОТПРАВЬТЕ СВОЮ ХАРАКТЕРИСТИКУ И РЕЗЮМЕ ПО АДРЕСУ PERSONAL@RIA.EE

Подробнее: www.ria.ee/ru